Dillon Eustace

# Business Email Compromise - Who is Liable?

November 2024

## What is Business Email Compromise?

Business email compromise (**BEC**) is an increasingly prevalent cyber threat whereby fraudulent actors manipulate email correspondence in order to deceive individuals into taking unauthorised actions, typically involving the transfer of funds. These fraudulent actors often intercept email correspondence between parties and mislead one party into making payment to a fraudulent account. BEC attacks can lead to substantial financial losses and while there are certain protections and mechanisms available for the recovery of the funds, victims may be left with no other option than to seek to attach liability to someone other than the perpetrator of the fraud to recover their loss.

## Obligation to Protect

There are a number of legislative provisions in this jurisdiction that regulate cyber security. The primary legislation covering data protection and privacy is the General Data Protection Regulation[1] (the **GDPR**) as supplemented by the Data Protection Act 2018 (the **DPA**) with the Data Protection Commission (**DPC**) being the competent authority for its regulation and enforcement.

The GDPR and the DPA require data controllers to take appropriate security measures to protect against attacks on data under their control and to report breaches to the DPC within 72 hours[2].

BEC attacks often result in data breaches, exposing personal

1 General Data Protection Regulation (EU) 2016/679)
2 Section 86 Data Protection Act 2018

and sensitive information. The DPC investigates such incidents to ascertain if organizations have taken appropriate measures to safeguard this data. Non-compliance with data protection laws in Ireland can lead to significant fines and penalties.

For parties that have been affected by BEC and possibly transferred funds to a fraudulent third party it is imperative that they contact their transferring financial institution and the authorities immediately in an attempt to recover the misdirected funds. Often the fraudulent actors will have moved the money quickly through multiple accounts and into a jurisdiction where it cannot be recovered.

If funds are not recoverable through these channels, victims of BEC may be left with no other option but to seek to issue civil proceedings in contract or tort to try to recover their loss and avoid having to make the same payment twice.

## Contractual Position

Most commercial contracts do not anticipate the complexities of BEC, however there may be certain terms in place that may be decisive with regard to liability.

For example, a contract may stipulate the terms or conditions of how a payment is to be made, and what actually constitutes payment for the purpose of discharging a payor's obligation. If a contract states that payment should be made to an account to be nominated by the payee, but that payee has been hacked and an incorrect account number provided, it could be arguable that the payor has discharged their obligation to pay, even if it was made to a fraudulent third party.

## Duty of Care

In addition to contractual obligations, a victim may also seek to bring proceedings in tort on the basis that a creditor owed them a duty of care.

If a business has failed to take appropriate steps with regard to its cyber security measures, and that failure has led to the security breach, it may be held liable for the loss suffered as a result of a BEC attack, where the other party to the transaction successfully argues that they breached their duty of care.

The individual facts of each case will be paramount in any such claim. For instance, a lot will depend on which party to the transaction has actually been compromised and if that party has taken all reasonable precautions with regard to cyber security.

There is also recent authority in the US[3] that has seen a recipient credit union held liable for BEC losses, not because they were a party to the contract, but for allowing the fraudulent third party to hold and operate an account with it. The case involved the payment of fraudulent invoices to an account held by the fraudulent actor at the credit union. While the credit union was not a party to the transaction, they were found to have owed a duty of care to the victim and were held liable for losses of over $500,000.

## Case Law

There is limited case law on BEC in this jurisdiction and so it is necessary to look to other common law jurisdictions for guidance as to the approach that might be taken by the Irish courts.

In the UK case of *Sell Your Car With Us Ltd v Sareen* [4] the plaintiff brought an injunction to stop a winding up petition brought by the defendant. The defendant had sold a car through the plaintiff's company and was owed money in respect of the sale. A fraudulent third party intercepted the defendant's emails and instructed the plaintiff to send the money to a different account. The plaintiff argued that the defendant was obligated to exercise reasonable care in respect of the security of his own email account. However, the Court found that the plaintiff alone was responsible for sending the funds to an unauthorised account. A deciding factor in the case was that the plaintiff's terms and conditions contained a specific protocol for customers changing their email contact details that had not been engaged by the defendant and the plaintiff had not noticed the small difference in the email address provided by the fraudulent third party.

The recent case from the South African Court of Appeal of *Hawarden v ENS*[5] is of particular note for law firms.

The case involved a leading South African law firm that was found liable in the High Court in 2023 when the plaintiff,

3 Studco Building Systems US, LLC v. 1st Advantage Federal Credit Union, No. 2:2020cv00417 (E.D. Va. 2020)
4 Sell Your Car With Us Ltd v Sareen [2019] BCC 1211
5 Edward Nathan Sonnenberg Inc v Judith Mary Hawarden (421/2023) [2024] ZASCA 90 (10 June 2024)

a purchaser in a conveyance, inadvertently paid purchase monies to a fraudulent account following the manipulation of their emails. The bank details had been sent to the plaintiff by email containing a PDF document. This email was intercepted due to a breach of the plaintiff's own email account and the account details manipulated.

The High Court initially found the defendant law firm liable for the loss, citing negligence for their failure to warn the plaintiff about the risks of BEC and alerting her about the necessary safety precautions. It was further held that even though the plaintiff was not a client of the firm they owed her a duty of care and that as expert conveyancers they were better placed to be aware of the risks of BEC. The court disagreed with the law firm's argument that the plaintiff had a duty to protect herself.

The decision was subsequently overturned on appeal with the court stating that the decision was too far reaching and highlighted a number of key points in making their decision:

1. The plaintiff was not a client of the firm and had no contractual relationship with her.

2. The plaintiff had the means and knowledge to verify the bank details and had been warned previously by her estate agent before paying the booking deposit; a warning that she heeded before.

3. The decision of the High Court could lead to indeterminate liability for businesses in circumstances where email fraud may be beyond their control.

## Conclusion

From the limited caselaw available to date it would appear that the courts are unlikely to absolve a party from a contractual requirement to pay a creditor following a BEC attack. It does appear, however, that such cases will be taken on their merits and that this is not an absolute principle.

It is of vital importance for every business to take all reasonable and practical steps towards avoiding BEC attacks by:

1. Ensuring compliance with all legislative obligations and taking reasonable care with regard to cyber security.

2. Updating their contractual terms and conditions with express exemption clauses with regard to such liability.

3. Continuous review of their funds transfer procedures such as encryption of payment details and requiring phone confirmation of bank details.

4. Ensuring that there is express warning given to payors in respect of BEC.

In BEC cases, both parties are innocent victims of the fraudulent party, and the courts will be cognisant of this in determining which party was best placed to avoid the fraud. It is imperative therefore for businesses to protect themselves by taking appropriate steps, as above, to minimise their exposure.

## CONTACT US

### Our Offices

**Dublin**
33 Sir John Rogerson's Quay
Dublin 2
Ireland
Tel: +353 1 667 0022

**Cayman Islands**
Landmark Square
West Bay Road, PO Box 775
Grand Cayman KY1-9006
Cayman Islands
Tel: +1 345 949 0022

**New York**
33 Irving Place
New York
NY 10003
United States
Tel: +1 646 770 6080

**Tokyo**
12th Floor,
Yurakucho Itocia Building
2-7-1 Yurakucho, Chiyoda-ku
Tokyo 100-0006,
Japan
Tel: +813 6860 4885

## CONTACT POINTS

For more details on how we can help you, to request copies of most recent newsletters, briefings or articles, or simply to be included on our mailing list going forward, please contact any of the team members below.


**Shane Harron**
**Partner | Dublin**
E shane.harron@dilloneustace.ie
T + 353 1 667 0022