Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

A Framework For Assessing Liability In Business Email Scams

By **Kelce Wilson** (March 3, 2020, 4:20 PM EST)

Kelce Wilson

Business email compromise is a type of scam that targets individuals and businesses who use wire transfers for payments, such as by providing fraudulent instructions over email that result in a payor's wiring money to a bank account that does not belong to the proper payee. That is, the individual or business who owed money (the payor) did pay, but the money went to a scammer instead of the individual or business to whom the money was owed (the payee).

Examples include requesting that a payment be made by wire transfer in lieu of a check, changing the bank account to which money is to be wired and, in some situations, identifying the bank account in the first instructions. There are multiple classes of BEC scams of which to be aware. These include misdirected wire transfers, bogus invoices and internal fraudulent requests, often ostensibly from company leadership, and some that steal data rather than money.

According to Federal Bureau of Investigation data, the number of BEC-related incidents and the amount of losses is increasing. In 2017, the FBI's Internet Crime Complaint Center received 15,690 complaints with reported losses of $676 million [1]. By 2018, the numbers climbed to 20,373 complaints with reported losses of $1.3 billion [2]. In 2019, the numbers climbed even higher to 23,775 complaints with reported losses of $1.8 billion [3].

This is a greater than 50% increase in the number of complaints in only two years, with the financial losses more than doubling. More information is available from the FBI.[4]. BEC is a rapidly growing threat, so if you have not yet heard about it, or already know someone who has been victimized, it is likely that you soon will.

Many contracts do not specify responses to BEC events, although hopefully that is changing, and guidance from the legal system, such as via case law, is sparse regarding assignment of liability. Under what circumstances must the payor pay twice, under what circumstances does the payee lose the funds, and are there any circumstances in which the payor owes the payee a reduced amount?

Based on my own experience, which is admittedly not a scientific study, it appears as if the party with the greater bargaining power is the one that prevails, independently of whether it was the payor or the payee, and independently of who (if anyone) was hacked.

For example, if a large multibillion-dollar business is tricked into paying the scammer, rather than paying a small business that has already provided products or services, the larger business may just refuse to pay, thereby depriving the small business owner of a significant percentage of expected earnings. Meanwhile, if an individual is tricked and fails to pay a business, the business may refuse to provide the product or service or turn the individual over to a debt collector that will motivate the individual to pay twice.

If settling liability always in favor of the party with greater bargaining power does not seem palatable, a framework for analyzing the degree of each party's failure may be preferable for assigning degrees of liability.

A framework is proposed below, identifying six primary scenarios and the mistakes made (or not) by each party. The scenarios will be better understood, however, after explanations of why the scam is so easy, in some of the scenarios, and steps that may thwart a scammer's BEC attempt.

Why It Is So Easy and How to Avoid It

Scammers may use detailed transaction information, if they are able to obtain it, in order to make the fraudulent email appear to be coming from the payee. In some scenarios, BEC does involve actually hacking into the payor's or payee's email.

However, in many situations, no hacking is required at all. This is because the "from" field in most email apps is misleadingly named. The "from" field can be easily changed by the sender to display nearly anything, allowing nearly trivial spoofing of the apparent sender's name.

For example, a hacker with the email address hacker@hacker_email_server.com can edit an outgoing email so that, when you open it, you see a name that you recognize, such as John Banker. If you do not look any further than the name that you recognize, it is possible to miss the incorrect email address following the name, e.g., JohnBanker<hacker@hacker_email_server.com>. Of course, you would need sufficient familiarity with the proper email address to become suspicious, even if you did see it.

The easiest prevention against a BEC scam is to not follow instructions received only over email regarding a bank or account number to which you should wire money. Instead, there should be at least two separate paths used to communicate payment instructions and changes to payment instructions.

So, if the payor receives an email with payment instructions, either original instructions or a change to a prior account, the payor should call the payee to verify the instructions using a phone number that the payor already had (i.e., not a phone number provided in the email with the payment instructions). Hopefully, the payor will recognize the voice of the other person and will have previously used that same phone number in order to have confidence that it is valid. For large amounts of money, a physical letter may be warranted.

Using the second channel for payment instruction verification works for both the spoofed email "from" field situations and also situations in which the payee's email actually is hacked in order to send the fraudulent instructions (so that there is no mismatch identifiable in the email address). If the payor identifies a spoofed email, and obviously declines to follow the fraudulent instructions, alerting the payee may still have value.

The scammer may also be targeting the payee's other accounts, and alerting the payee enables it to

alert its other payors to be watchful. If the email "from" field is not spoofed, the payee is then alerted that at least one account of its email system has been hacked.

A Suggested Checklist for Some Prevention Steps

1. If you are an individual, do not follow instructions for wire transfers that you receive in an email. Pick up the phone and call the people whom you are to pay, using a phone number you already have (not one from the email), and speak with a person whose voice you recognize. If you don't know anyone there, that's not a good position in which to have put yourself. Be proactive about speaking with people with whom you do business or expect to do business.

2. Consider using digitally signed email and secure document delivery systems. Most information technology staff members will be familiar with these. If you are an individual, then ask your bank what systems it uses.

3. Update your contracts and purchase orders to require that verification of payment instructions and changes be made over a separate channel than the one over which the payment instructions were received. For example, if the instructions came over email, make a phone call. If the instructions came over then phone, call back and/or send an email.

4. Businesses should train their employees to do follow those contract clauses, and regularly test the employees, to ascertain whether the training is effective.

5. The recipient of the instructions should initiate the verification, using contact information already known to him or her. If feasible, verify in person.

6. The payor and payee should exchange contact information for each other over multiple channels (e.g., email, phone and physical address).

7. The payor and payee should have enough familiarity with each other, prior to any fraudulent payment instruction changes becoming a possibility, that they can recognize each other.

8. Update your contracts to identify BEC remediation steps, possibly using the scenarios identified below to allocate liability in order to calculate the amount of a second payment (if any).

9. Create an email rule to flag email communications for which the reply to email address is different than the from name or email address that is displayed.

10. If feasible, two different people should look at all payment instructions, in case the initial recipient missed a clue that the instructions might be a BEC attempt.

11. Businesses should register as many domain names as possible that are slightly different from the actual domain name, so that scammers/hackers cannot use an email with an easily missed misspelling, e.g., substituting the number "1" for a lower case letter "l".

12. Minimize public dissemination of organizational and personal information, when feasible, in order to prevent scammers/hackers from using the correct job titles or other convincing details in the fraudulent emails.

13. If you are the payee, either shortly before or immediately after making a wire transfer, contact the payee (using prior-known contact information) to request confirmation of receipt of the payment. If you do not receive timely confirmation, follow up. If the payment was not received by the proper party, there may be a problem to address.

Six Primary Scenarios

Six common scenarios are enumerated, and a real-world scenario may be a combination of more than one. The scenarios reflect that there are two primary things of value and five primary acts that may indicate negligence. The two primary things of value are (1) email account access and (2) transaction information.

The five primary acts are (1) permitting hacking of an email account, (2) permitting hacking of a computer holding transaction information, (3) improperly leaking transaction information into the public domain, (4) lacking proper vigilance to identify that the name and email address in a received email do not match, and (5) failing to confirm the instructions via a separate channel.

By assessing which party made which mistakes, it may be possible to form a reasoned opinion regarding comparative negligence. Not all acts should necessarily have equal weight for determining negligence.

First, though, an important point is worth mentioning. During a prior career, working as an engineer in a military cybersecurity testing project,[5] it became apparent to me that being hacked is not necessarily proof of having been negligent. This is because businesses must necessarily make compromises in order for their employees to be able to use data processing systems, and no system that is useable by employees can be impervious to hacking.

A determined hacker, with the proper resources, can break into even reasonably well-protected systems. Also, some real-world situations may be so complex that assessment becomes challenging, far beyond using these model scenarios.

Scenario 1

The payee is hacked for email account access. In this case, the payee has at least one fault, permitting hacking of an email account. This is in addition to other possible payee faults.

Scenario 2

The email is spoofed, rather than the payee's email account being hacked. In this case, the payor has at least one fault, lacking proper vigilance to identify that the name and email address in a received email do not match. This is in addition to other possible payor faults.

Scenario 3

The payee is hacked for transaction information. In this case, the payee has at least one fault, permitting hacking of a computer holding transaction information. This is in addition to other possible payee faults.

Scenario 4

The payee is not hacked for transaction information, but does improperly leak transaction information

into the public domain, where it is found by the scammer. In this case, the payee has at least one fault, which is in addition to other possible payee faults.

Scenario 5

The payor is hacked for transaction information. In this case, the payor has at least one fault, permitting hacking of a computer holding transaction information. This is in addition to other possible payor faults.

Scenario 6

The payor is not hacked for transaction information, but does improperly leak transaction information into the public domain, where it is found by the scammer. In this case, the payor has at least one fault, which is in addition to other possible payor faults.

In all six scenarios, the payor has at least one fault, failing to confirm the instructions via a separate channel. The degree of negligence for this failure may be affected by the payor's technical sophistication and experience in financial transactions.

For example, an unsophisticated consumer should likely be attributed a lower level of negligence than a large business' employee who has a job function of regularly paying suppliers via wire transfers. Upon analyzing the six scenarios, a count of faults may be possible for both the payor and payee. Hopefully, this provides a defensible basis for assigning liability among the payor and payee, and will replace resolving liability based upon which party has more power.

What to Do If It Happens to You

It is a good practice, after making any wire transfer, to find out whether you are involved in a BEC event. It is critical that you act quickly. If you are the payor:

1. Contact the bank you used to make the outgoing wire transfer, and alert it that there may have been a fraud. Ask for the funds to be returned. In some cases, it may be possible to recover some of the money, although the likelihood of recovery drops precipitously after the first 24 hours.

2. Then, without delay, contact the FBI through the IC3.[6]

3. Have your IT staff carefully examine the email containing the payment instructions to identify from where it was sent. Note that law enforcement may request a copy also.

    a. If the instruction email was sent from the payee's email server, then inform the payee of a suspected breach of their email system. Work with the payee to identify a new communication method, possibly one using a code word or other secret.

    b. If the instruction email was sent with a spoofed email address, then your employee training is ineffective. That needs to be addressed now.

If you are the payee:

1. Alert the payor, if he or she does not already know.

2. Contact the bank at which you are expecting to receive the incoming wire transfer, and alert it that there may have been a fraud or the funds may have been misplaces. Ask for an immediate alert if the funds arrive or are located.

3. Work with the payor to provide complete information to the FBI's IC3. See [6] for where to make the report.

4. Learn the details of the email containing the payment instructions, such as sender, time and date, subject line, recipients and names of attachment.

5. Have your IT staff carefully examine your email system to ascertain whether your email system was used.

a. If the instruction email was sent from your email server, then you may have experienced a breach. You may have a larger set of problems. Hopefully, your IT staff has a decent incident response plan in place. It's time to break it out and start using it.

b. If the instruction email was sent with a spoofed email address, then suggest that the payee become familiar with the prevention steps checklist above. And did your contract specify how the payment instructions were to be verified?

Additional steps for both the payor and payee:

1. Go to the prevention steps checklist above, and figure out what went wrong and what you can do better in the future.

2. Check your insurance for possible coverage of the loss.

3. Review your contract to determine what is requires regarding a second payment and continued delivery of products and/or services.

4. Consider reviewing and updating the following items to reduce the likelihood of another occurrence or, if there is another incident, you will have a clear plan and expectations:

a. Your employees' training and testing for prevention;

b. Your insurance coverage; and

c. Your contracts.

Kelce S. Wilson, Ph.D., is a member of Grable Martin Fulton PLLC.

[1] Federal Bureau of Investigation, "2017 Internet Crime Report," 2017, available at https://pdf.ic3.gov/2017_IC3Report.pdf.

[2] Federal Bureau of Investigation, “2018 Internet Crime Report,” 2018, available at https://pdf.ic3.gov/2018_IC3Report.pdf.

[3] Federal Bureau of Investigation, “2019 Internet Crime Report,” 2019, available at https://pdf.ic3.gov/2019_IC3Report.pdf.

[4] Federal Bureau of Investigation, “Business E-Mail Compromise the 12 Billion Dollar Scam,” Public Service Announcement I-071218-PSA, July12,2018, available at https://www.ic3.gov/media/2018/180712.aspx.

[5] K. S. Wilson and M. A. Kiy, “Some Fundamental Cybersecurity Concepts,” IEEE Access, vol. 2, pp. 116-124, 2014.

[6] The FBI Internet Crime Complain Center (IC3) has a crime report portal, for BEC and other internet-related crimes, at https://www.ic3.gov/complaint/default.aspx/.