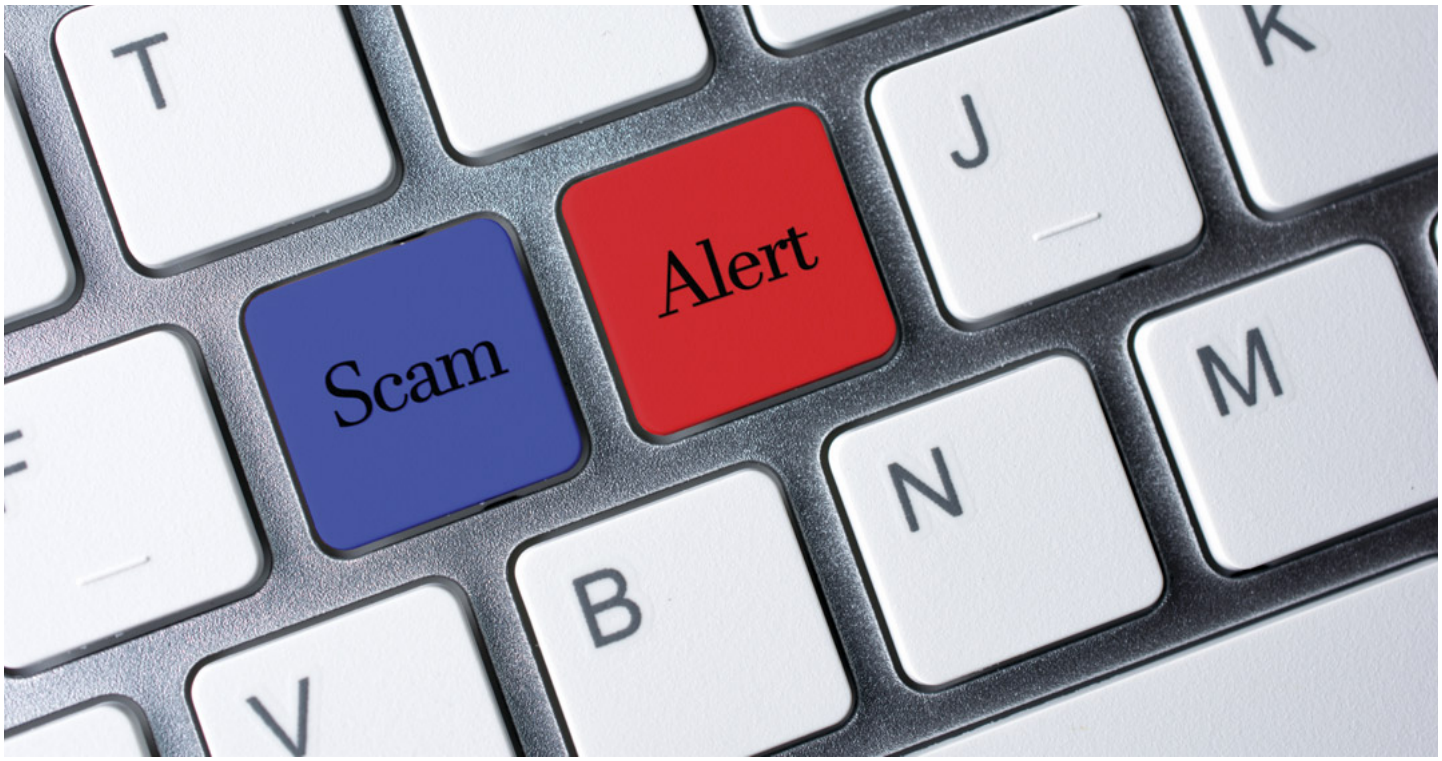
Jeffrey I. Ehrlich
THE EHRLICH LAW FIRM

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
September 2018 Issue



There but for the grace of God go you

A LOCAL PLAINTIFF'S LAWYER GETS ENSNARED IN A "BEC" SCAM

Monsters are generally not all that scary until you find one under your bed. So, if I told you that it was important for you to become familiar with "business email compromise" or BEC scams to avoid being taken in, and that you could learn much of what you needed to know from a public-service announcement posted on the FBI's website, you'd probably nod and skip to the next article.

What if I told you this, instead? An experienced plaintiff's lawyer you probably know and like – we'll call him "Bob" – had a 7-figure settlement wired to criminals in Hong Kong instead of into his client-trust account because the defense lawyer fell for a BEC scam. The defense lawyer's firm and its client then blamed Bob for the problem and tried to get a court order declaring that they were entitled to entry of a full satisfaction of judgment. Had they succeeded, Bob would have faced a large malpractice claim from his own clients. I'll spoil the ending here – Bob won. But he did not come out of the experience unscathed. Not only was the receipt of the settlement proceeds delayed for almost a year, he and his client had to deal with the expense and uncertainty of months of litigation during that period.

In this article I'll show you how the scam worked and how you can protect yourself from similar ones. By the time you are done, I bet you might even check out that FBI website.

The scam

Bob sued a major international company that makes, among other things, wheeled vehicles (we'll call it "D" for defendant.) The suit was defended by a major products-liability defense firm, which we'll call "Archer & Stream" or "A&S." The partner with day-to-day responsibility for the case at A&S was "Ralph." He was an experienced, careful lawyer. For example, he insisted that Bob's clients (the "Smiths") have their signatures on the settlement agreement notarized "because of the sums involved." The settlement that Bob, Ralph and D worked out provided that the proceeds would be paid in three parts: (1) a structure; (2) a six-figure sum that would be paid by check; and (3) a 7-figure sum that would be paid by wire transfer.

On June 1, 2017, Bob emailed Ralph the wire-transfer instructions to have the settlement proceeds wired to Bob's trust account at a local Wells Fargo branch. There is no dispute that Ralph got the instructions. But a few days later Ralph received an email that looked like it came from Bob, which said, "Ralph, the Smiths would be setting up some investments in Hong Kong. They have requested the funds to be wired there. Can you jump on this? Please let me know."

Ralph responded to the bogus email by hitting the "reply" command. As a result, Ralph's email went to the thief,

See Ehrlich, Next Page

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
September 2018 Issue

not to Bob. Ralph asked, "Are we wiring them to a different account than you designated on the form? If so I need a new form with the correct information." The thief, posing as Bob, responded by emailing Ralph new wire instructions, directing that the proceeds be wired in equal amounts to two companies: "Hong Kong Copper Trade Co Limited" and "Run Xing Trading Company Limited." Both of these were Hong Kong entities, with the wire transfers directed to accounts in Hong Kong banks.

On June 19, Ralph emailed the thief (believing he was emailing Bob) and informed him that the check had been overnighted to Bob and the wire transfers would go through the next day. The thief responded with an email that said, "Thanks Ralph. I'll keep my eyes on the eyes on the ground. Please give me a heads up when both wires hits out."

The wires went out the next day, but one was rejected by the receiving bank in Hong Kong. This type of rejection of an international wire, which is normally caused by a discrepancy between the recipient listed in the wire instructions and the account owner, is a warning sign that the bank may have considered the transfer to be fraudulent. But neither Ralph nor D detected any red flags.

On June 21, the thief – now posing as Ralph – sent Bob an email explaining that there would be a delay in receiving the wire transfer because of a death in the family of the employee at D who was responsible for handling wire transfers, who would be out of the office until July 5. On July 6, the thief sent Bob an email stating that the bereaved employee was still out of the office, and the funds would be sent by July 12, 2017. Bob was annoyed, but because the structure had funded and he had received the check as promised, he remained patient.

On June 22 the thief, posing as Bob, sent Ralph an email advising of the rejected wire transfer and requesting that the funds be re-sent to Run Xing Trading Company. Ralph responded to the thief by email, stating, "I'm in a depo, otherwise I'd call. But to confirm: (1) We initially sent the rejected wire to "Hong Kong Central Copper Trade Co Limited." (2) You want that transfer to go to "Run Xing Trading Company Limited" (3) So both Hong Kong transfers are going to the same recipient and same account? Is this different than you instructed? We have to make sure we don't transfer twice (i.e. Double Pay)." The thief responded by email saying "yes" to each question.

D waited until the rejected funds had been credited back to its account before sending the second wire. Once the funds were available again, on July 10, Ralph emailed the thief advising that the funds were now available for transfer and asking for further instructions. The thief provided new wire instructions to Ralph, directing that the funds be sent to a Hong Kong entity called "Fair Top Industrial Development (HK) Co. Limited." This transfer was successful.

The post-scam litigation

The scheme was finally discovered on July 19, after an exasperated Bob sent Ralph and his senior partner at A&S an email expressing frustration with the delays in receipt of the wired funds. That night Bob learned from Ralph that D had wired the funds to Hong Kong based on what they had thought were instructions from Bob.

At that point both sides hired their own technical experts. There were some unproductive meetings and conversations about how to resolve the situation. Both sides then lawyered up, and ultimately filed cross-motions under section 664.6 of the Code of Civil Procedure to specifically enforce the settlement. (This was how I got involved in the matter.)

D argued that it was entitled to relief because it had "performed" its part of the settlement by wiring the funds. It blamed Bob for supposedly having his email "compromised" and claimed that he bore primary responsibility for the misdirected funds.

Neither side had obtained discovery of the other side's email systems. So, both sides had to work with the evidence available to them based on emails that they had received, or paper copies of email strings produced by the other side.

D argued that the paper trail showed that Bob's email had been compromised in some way, and that the emails that Ralph received did not just *look like* they had come from Bob, they actually came from his account. But Bob's IT professional could find no evidence to support this view. That is, there was no evidence in Bob's system that showed that any of the emails that Ralph received from the thief actually came from Bob's computer. The evidence did show, however, that the thief had been able to relay "spoofed" emails (that is, emails that looked like they came from Bob, but did not) via a third-party's IP address.

In their cross-motions, both sides relied on the same case – which at the time appeared to be the single case decided by a U.S. court that resembled the situation presented most closely, *Bile v. RREMC, LLC* (E.D. Va. 2016) 2016 WL 4487864 ("Bile"). In *Bile*, the plaintiff (Bile) settled his employment-discrimination claim against Denny's. Before the settlement funded, Bile's lawyer (Ubom) received an email purporting to be from Bile, directing him to have the settlement funds wired to an account in London, held in Bile's name. Ubom telephoned Bile to confirm the authenticity of the email, and Bile informed him that it was fake.

Despite their knowledge that a third party was attempting to steal the settlement funds, neither Bile nor Ubom notified Denny's or its counsel about the attempted fraud. The thief then turned his attention to Denny's counsel, sending fake emails purporting to be from Ubom that instructed that the funds be wired into the same London account in Bile's name. Defense counsel had Denny's wire the funds to that account, which the thief controlled, and the funds were lost.

Both parties in *Bile* filed cross-motions to specifically enforce the settlement. Relying on principles derived from the law of negotiable instruments set forth in Article 3 of the Uniform Commercial Code, the *Bile* court derived the following rule: "[T]the U.C.C. requires 'ordinary care' by participants in financial transactions; the participant

See Ehrlich, Next Page

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
September 2018 Issue

who fails to exercise ordinary care is liable for any losses to which his lack of ordinary care substantially contributes."

Applying this rule, the court denied Bile's motion and granted Denny's cross-motion. The court found that Denny's counsel had acted with due care because there was nothing suspicious in the emails or the instructions he had received. By contrast, the court found that Bile and his attorney, Ubom, had been unreasonable in failing to notify defense counsel of the original fraudulent email. As the court explained:

> At the heart of this case is the simple fact that Bile's agent, Ubom, could have prevented the loss . . . by notifying opposing counsel on July 27, 2015, when he had actual knowledge of an attempted fraud . . . . As technology evolves and fraudulent schemes evolve with it, the Court has no compunction in firmly stating a rule that: where an attorney has actual knowledge that a malicious third party is targeting one of his cases with fraudulent intent, the attorney must either alert opposing counsel or must bear the losses to which his failure substantially contributed.

Bob and D urged court to apply this rule

While both parties in dispute between Bob and D urged the court to apply this rule, they disagree on the outcome its application would produce. D argued that the same reasons that allowed the court to find that the Denny's lawyer acted reasonably were applicable to Ralph's conduct here: that the fraudulent emails received by the lawyer actually came from Ubom's account; that the emails used language that mimicked the way that Ubom spoke; and that the wire request was consistent with what the parties had previously agreed to do.

Bob argued that the parallels that D claimed to see did not exist. There was no evidence that the fake emails received by Ralph came from Bob's account, and there were a host of clues that suggested that they were fake. Nor did the emails in *Bile* seek to change legitimate wire instructions that had already been received by the defense, or ask to have the funds wired into accounts that were not owned by or connected to the plaintiff.

Bob also argued that D overlooked a key lesson taught in *Bile*: that the reasonable thing for an attorney to do upon receipt of an email that may look real, but which asks for something odd, is to pick up the phone and call the sender, just as Ubom did when he received the first fake email purporting to be from his own client.

Ultimately, the trial court ruled in Bob's favor and granted his 664.6 motion and denied the cross-motion by D. D ultimately decided not to appeal that ruling and paid the funds a second time. Presumably, A&S and D then had to work out how that loss would be apportioned.

Lessons to be learned

Now that you have seen that the monster Bob faced could easily find its way under *your* bed, I want to go back to the dry public-service announcement about BEC scams. Here is the address for the FBI public service announcement: https://www.ic3.gov/media/2017/170504.aspx. I urge you to read it.

The takeaway is that the criminal organizations that carry out these BEC scams are incredibly sophisticated. They comb through public filings with the SEC and other agencies to learn about how organizations are structured, who they do business with, and which employees hold which jobs. They also use social media and phishing attacks to gather additional information. They can produce emails and websites that look authentic. They can insert malware on computers to obtain passwords and control of email accounts. And they have contacts in companies that use wire transfers, or the companies who deal with them, so that they know when a large transfer is going to be made, so they can target it.

The scammers can pose as a high-level executive asking to have a wire transfer made immediately to facilitate an important deal. They can pose as a supplier wondering why an invoice has not been paid. And, as we have seen above, they can create a "man-in-the-middle" attack in which both sides in a transaction think they are following the other side's new instructions.

On June 12, 2018, the Washington Post published an article with the headline: *It's time to stop laughing at Nigerian scammers – because they are stealing billions of dollars*. You should read it too. (https://www.washingtonpost.com/news/business/wp/2018/06/12/its-time-to-stop-laughing-at-nigerian-scammers-because-theyre-stealing-billions-of-dollars/?utm_term=.f9f79d59cc72)

The current BEC scams they run resemble the old "Nigerian Prince" scams in the same way that a 747 resembles the Wright Brother's flyer. Same idea; substantially better execution.

It is often impossible to detect the difference between an authentic email and a bogus one by how they look or even by their metadata. This means that your first line of defense must be to decide whether what is being requested in the email seems questionable for some reason. If so, question it!

If you know the person who sent the email, such as opposition counsel in a case you have litigated for the last two years, the best approach would be to pick up the phone and call them. But sometimes the sender may not be someone you know, and you may have no other means to respond than by email. If so, don't just hit "reply." If you do, and the email is spoofed (meaning it looks like it came from one sender, but actually came from someone else), hitting "reply" will respond to the spoofed email, not the "real" person you want to deal with. So instead of hitting "reply,' you should either type out the address manually or select it from your email address list. This way, you know that your email is directed to the right person. (Of course, if their email has truly been compromised, it may not matter.)

Also, avoid sending emails with subjects that are likely to attract the attention of scammers, like "Wire Instructions." (In Bob's case, Ralph had emailed him the wire-instruction form

See Ehrlich, Next Page

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
September 2018 Issue

that he wanted Bob to complete with a "wire instructions" subject line.)

Be aware of red flags

Be aware of potential red flags that require further investigation. If you receive a request to do something that is at odds with what has already been agreed to, or with how transactions are usually handled, be suspicious. For example, in Bob's case, Ralph and A&S should have been dubious of any request to change the wire instructions from Bob's client-trust account in a local bank to a bank in Hong Kong. Plaintiff's lawyers almost always insist on having settlement proceeds wired to or deposited into their client-trust accounts. This is the only way that they can assure that they can pay the liens on a case, including the lien for their fee.

And defendants should (and almost always do) insist on making payment to the plaintiff they are settling with, either directly or through the plaintiff's lawyer. If they don't, then they are at risk for being asked to pay a second time. And if they pay the funds to a third party, it looks like someone may be involved with money laundering.

Other red flags include a change in the tenor of the communications. Very few native speakers of English would say, "I'll keep my eyes on the eyes on the ground. Please give me a heads up when both wires hits out."

Red flags could also include delays in performance coupled with dubious excuses. Would a major manufacturer like D really only have one person who handles wire transfers? Possibly. But if that person was out of the office for two weeks, would all wire transfers stop until that particular employee returned? Not likely.

Consider whether the convenience of wire transfers is worth the risk. Any settlement that can be funded by wire transfer can also be funded by a check. If a check is sent to the wrong recipient, or stolen, it can be much easier to claw back the funds than if they are wired.

Likewise, as plaintiff's counsel it may be worthwhile to include specific instructions for payment of the settlement proceeds in the settlement agreement itself, together with a provision stating that any change must be in a notarized writing signed by both parties. That may not prevent defense counsel and its client from being taken in by a BEC scam, but it would make it much harder for them to blame you if they are.

Jeffrey I. Ehrlich is the principal of the Ehrlich Law Firm *and is an appellate specialist certified by the State Bar's Committee on Legal Specialization. He is an emeritus member of the CAALA Board of Governors and is the editor-in-chief of Advocate. He is also a co-author of Croskey, Heeseman, Ehrlich & Klee, California Practice Guide – Insurance Litigation (Rutter 2018). Ehrlich was twice named CAALA's Appellate Lawyer of the Year.*