INSURANCE COVERAGE
SECTION OF LITIGATION
Fall 2017, Vol. 27 No. 4

# Insurance Coverage for Business Email Compromise Losses

Gregory Wright and Gillian Giannetti – December 1, 2017

Numerous courts have recently addressed disputes between policyholders and insurers related to insurance coverage for so-called business email compromise (BEC) losses. There are various forms of BEC schemes, but in many, a criminal uses "fake" or fraudulent emails, social engineering, hacking, or other manipulation of the policyholder's computer system through malware to fraudulently induce the policyholder to wire funds to a bank account controlled by the criminal. The Federal Bureau of Investigation (FBI) has described this issue as a $5 billion scam.[1]

This article provides an overview of BEC schemes and the types of policies and bonds that might apply, and then discusses recent case law addressing coverage disputes related to these losses. In many cases, policyholders may have strong arguments for coverage for BEC losses under a variety of policies, including commercial crime policies, crime-related coverage parts included in package policies offering multiple lines of coverage, and financial institution bonds, all of which may include coverage parts for so-called "computer fraud" or "funds transfer fraud." In addition, certain insurers are now offering endorsements to crime policies that more specifically focus on BEC-related risks.

A growing number of courts across the country have considered BEC coverage claims, reaching mixed results. As discussed below, courts have considered two major defenses: (1) whether any involvement of a deceived employee of the policyholder defeats coverage and (2) whether any proof of "hacking" is required to trigger coverage. Going forward, it is likely that the courts also will focus on factual issues and expert testimony related to the criminal's scheme. These cases are reviewed below.

## Background

**The nature of BEC schemes.** BEC schemes vary widely, but often a criminal induces the policyholder to wire money to an account the criminal controls. Once the fraud is discovered, it is often too late for the policyholder to stop the payment or recover the funds. The FBI has issued an alert that describes many types of BEC schemes, the following among them:

· The Bogus Invoice Scheme: The criminal purports to be a long-standing business partner and sends an email asking the policyholder to wire funds for an

outstanding invoice to a new account that appears legitimate but is controlled by the criminal.

· Business Executive Fraud: The criminal spoofs or hacks the email account of an executive of the policyholder (or an attorney purportedly working with an executive) and requests payment to an account controlled by the criminal. A request for a wire transfer is sent from the spoofed or hacked account to an employee of the policyholder who is responsible for processing such payments.

· Hacked Employee Email Account: The criminal hacks or spoofs an employee's email account and then sends emails to outside vendors directing the vendor to make payments owed to the policyholder to an account controlled by the criminal (rather than the policyholder's account).[2]

BEC scams continue to grow in number, evolve, and target businesses of all sizes. As of May 2017, the FBI had identified total BEC-related losses in excess of $5 billion. Between January 2015 and December 2016, there was a 2,370 percent increase in identified losses.[3]

Notably, many BEC schemes do not originate with the email requesting payment to the criminal's account; instead, the schemes are preceded by a period of monitoring by the criminal in which the criminal investigates the target, the target's process for paying invoices, the people in charge of paying invoices, and the status of projects requiring future payments. The FBI alert states that criminals typically "monitor and study their selected victims . . . prior to initiating the BEC scam."[4]The criminals often conduct extensive research to identify active projects, learn jargon and product names, send phishing emails to get feelers in the door, and create phony websites to lend credibility to their emails.[5] Criminals may seek information through social-engineering techniques (e.g., impersonating company officials, attorneys, or vendors) and by "cyber hacking."[6] For example, the criminal may send a phishing email to the target from a seemingly legitimate source that contains a malicious link.[7] By clicking on the link, the victim downloads malware, allowing the criminal to access the victim's data, including passwords and financial account information.[8] Certain BEC schemes have involved the criminal sending emails to targets that contain keylogging software that sends information from the target's computer back to the criminal.[9] The FBI has noted that, after introducing malware, "[u]ndetected [criminals] may spend weeks or months studying the organization's vendors, billing systems, and the CEO's style of email communication and even his or her travel schedule."[10] Criminals also may attempt to spoof company email by manipulating the policyholder's computer system or via other techniques.[11] In other words, when the criminal sends an email to the policyholder, the criminal may introduce code that tricks the policyholder's computer system into adding the policyholder's normal graphics and contact information to the criminal's email, which makes it appear that someone who works for the policyholder actually sent the email.

Using the information and the techniques described above, criminals then attempt to make their emails requesting payment appear as authentic as possible (e.g., criminals send emails to the person in charge of making payments at the time an anticipated payment to a known vendor is due).

**Policies that potentially afford coverage for BEC-related losses.** Various types of policies may afford coverage for BEC-related losses, including commercial crime policies, package policies that include crime or computer fraud coverage, and financial institution bonds. Such policies and bonds often include crime-related or computer-fraud-related coverage grants that are similar in concept but often vary in their specific terms.

For example, some crime policies include a "computer and funds transfer" coverage part that generally affords coverage for "Loss resulting directly from a 'fraudulent instruction' directing a 'financial institution' to debit your 'transfer account' and transfer . . . money . . . from that account."[12] Similarly, certain bonds include "computer system fraud" coverage that generally affords coverage for "Loss resulting directly from a fraudulent . . . entry of Electronic Data . . . or change of Electronic Data . . . within any Computer System operated by the Insured, . . . provided the entry . . . causes an account of the Insured or of its customer to be . . . debited."[13]

In addition to language requiring that loss result *directly* from the type of conduct triggering coverage, certain crime policies and bonds include exclusions that potentially apply to loss caused by an employee of the policyholder.

Alternatively, some crime policies afford coverage for "computer fraud," which is defined to include the use of any computer to fraudulently cause the transfer of money. Some crime policies also may include so-called "fraudulent instruction" coverage, which potentially covers losses arising from fraudulent instructions that result in a financial institution debiting the policyholder's account.

In response to the growing risk of BEC schemes, some insurers have started to offer new policy forms or riders that expressly address this risk, perhaps subject to a negotiated sublimit.[14]

**Cases Addressing Coverage for BEC-Related Claims**

The case law related to coverage for BEC-related losses is relatively sparse but is developing rapidly. Courts have considered various issues, including causation-based coverage defenses, as well as various hacking-based defenses. While courts have reached mixed results, the law is still developing and policyholders may have strong arguments for coverage for BEC-related losses, even when the policies at issue do not expressly mention BEC-type claims or events.

**Causation defense: Does employee involvement defeat coverage?** Certain crime policies and bonds require that any loss "result directly" from the "computer fraud" or "fraudulent instructions" at issue. Citing this "resulting directly" language,

insurers have contested coverage when an employee of the policyholder arranges for the wire to be sent, even though the employee did so after being deceived by the criminal. The insurers argue that the criminal's conduct was not the "direct" cause of the loss due to the acts of deceived employees. As discussed below, courts have reached mixed results on this issue.

**1. Courts rejecting the causation defense.** Several courts have rejected the causation defense on the grounds that it would render coverage illusory and have held that coverage exists if the criminal's action is the proximate cause of the loss or started the chain of events leading to the payment.

First, in *Principle Solutions Group, LLC v. Ironshore Indemnity, Inc.*,[15] a criminal emailed the policyholder's controller, purporting to be a managing director of the policyholder, and directed the controller to work with an outside attorney with respect to a pending acquisition. The criminal's email directed the controller to "ensure that the wire goes out today."[16] The controller also received an email and phone call from a person purporting to be the outside attorney. After attempting to confirm the request, the controller arranged for the funds to be wired.

After discovering the fraud, the policyholder sought coverage under a commercial crime policy, which covered "Loss resulting directly from a 'fraudulent instruction' directing a 'financial institution' to debit your 'transfer account' and transfer, pay or deliver 'money' . . . from that account."[17] The insurer denied coverage, arguing that the loss did not result "directly" from the criminal's email (purportedly from the managing director) because "(1) additional information for the wire was conveyed to [the policyholder] by [the outside attorney] after the initial email, and (2) [the policyholder's] employees set up and approved the wire transfer."[18]

The court granted the policyholder's motion for summary judgment, holding that the policy language was ambiguous and should be construed in the light most favorable to the insured.[19] The court rejected the insurer's argument that the involvement of deceived employees defeated coverage, reasoning that "[i]f some employee interaction between the fraud and the loss was sufficient" to defeat coverage, "the provision would be rendered 'almost pointless' and would result in illusory coverage."[20] The insurer has appealed the district court's opinion to the Eleventh Circuit.[21]

Second, the Southern District of New York recently rejected this causation defense in *Medidata Solutions, Inc. v. Federal Insurance Co.*[22] In that case, a policyholder employee received emails purportedly from a company executive that were actually from a criminal. Based on such emails and other communications, a wire of $4.7 million was made to the criminal's bank account. The insurer denied coverage under the policy's funds transfer clause, arguing that the wire transfer was voluntary and made with Medidata's knowledge and consent. The court rejected this defense:

> [I]t is undisputed that a third party masked themselves as an authorized representative, and directed Medidata's accounts payable employee to initiate the

> electronic bank transfer. It is also undisputed that the accounts payable personnel would not have initiated the wire transfer, but for, the third parties' manipulation of the emails. The fact that the accounts payable employee willingly pressed the send button on the bank transfer does not transform the bank wire into a valid transaction.[23]

Similarly, in ruling for the policyholder under the computer fraud coverage part, the court reasoned that, even though there were intervening steps, "[t]he chain of events began with an accounts payable employee receiving a spoofed email from a person posing as Medidata's president. . . . Medidata employees only initiated the transfer as a direct cause of the thief sending spoofed emails posing as Medidata's president."[24] *Medidata* currently is on appeal in the Second Circuit.[25]

Third, the Eighth Circuit rejected this defense in *State Bank of Bellingham v. BancInsure, Inc.*[26] In that case, a policyholder bank sought coverage under a financial institution's bond after a third party caused funds to be wired from the policyholder's bank account.[27] Specifically, an employee of the policyholder completed a transfer of funds in accordance with the policyholder's security protocol, including the use of security tokens, but mistakenly left the security tokens in the computer overnight. The next day, it was discovered that unauthorized transfers had been made from the policyholder's account. On further investigation, it was discovered that a virus had infected the policyholder's computer and permitted the criminal to access the computer and make the fraudulent transfers.

Notably, *Bellingham* involved a criminal directly causing the transfer of funds, rather than tricking an employee to transfer funds. Nevertheless, the insurer denied coverage based on an exclusion for "loss caused by an Employee," arguing that alleged acts or omissions of employees (e.g., leaving the tokens in the computer overnight in violation of company policies, failing to update antivirus software) resulted in a loss of coverage.[28]

Applying Minnesota law, the Eighth Circuit rejected the insurer's argument.[29] The court applied Minnesota's concurrent causation rule, which it summarized as follows: "[W]here an excluded peril 'contributed to the loss,' an insured may recover if a covered peril is . . . 'the efficient and proximate cause' of the loss. . . . An 'efficient and proximate cause,' in other words, is an 'overriding cause.'"[30]

Based on the facts, the *Bellingham* court held that the "overriding cause" of the policyholder's loss was the criminal activity of the third party—not the actions of the employee.[31] According to the court, "[e]ven if the employees' negligent actions 'played an essential role' in the loss and those actions created a risk of intrusion into Bellingham's computer system by a malicious and larcenous virus, the intrusion and the ensuing loss of bank funds was not 'certain' or 'inevitable.'"[32]

Fourth, a Connecticut court similarly rejected this causation defense in *Owens, Schine & Nicola, P.C. v. Travelers Casualty & Surety Co. of America*.[33] In that case, the policyholder law firm was the victim of an elaborate scheme by a criminal

posing as a new client of the firm on a debt collection matter. The criminal arranged for a fake, physical "check" to be sent to the law firm from the purported debtor to settle the claim. The criminal asked the law firm to deposit the "fake" check into its IOLTA account and then wire funds in the same amount to the criminal's account. The criminal arranged the scheme such that the law firm wired the funds after it deposited the fake check but before it learned that the check was invalid.

The policyholder sought coverage under a crime insurance policy covering loss arising from computer fraud, which was defined in part as "[t]he use of any computer to fraudulently cause a transfer of Money."[34] The insurer denied coverage on several grounds, including causation.[35] The insurer argued that, even though the criminal had sent emails related to the payment, "the transfer of the money occurred when [the policyholder] contacted [its bank] in person, by telephone and in writing to direct the transfer of the money."[36] The *Owens* court rejected this defense, reasoning that the use of the computer here (the emails from the criminal) "proximately caused" the policyholder's loss and that such emails "set the chain of events in motion that led to the entire loss."[37]

**2. Rulings favoring insurers on causation issues.** Insurers have in some cases relied on a Fifth Circuit opinion, *Apache Corp. v. Great American Insurance Co.*,[38] as well as certain cases that cite that Fifth Circuit opinion, to support causation defenses. As discussed below, however, *Apache* has been described as "unpersuasive" by at least one other court.

In *Apache*, a criminal sent emails to and telephoned the policyholder, directing the policyholder to change the bank account information of the policyholder's vendor. The policyholder then made payment of legitimate invoices from the vendor to the criminal's bank account.

The policyholder sought coverage under the computer fraud provision in a crime policy that covered in part "loss of . . . money . . . resulting directly from the use of any computer to fraudulently cause a transfer of that property."[39] The insurer denied coverage, arguing that "loss did not result directly from the use of a computer nor did the use of a computer cause the transfer of funds."[40]

Reversing the district court, the Fifth Circuit ruled in favor of the insurer, but the basis for its conclusion is not clear.[41] Ultimately, the *Apache* court appears to have given some credit to the insurer's causation argument, based on the fact that the fraud involved a multistep process (i.e., a call, then an email, followed by the policyholder's investigation and steps to verify, followed by payment to the wrong account). The court stated:

> The email was part of the scheme; but, the email was merely incidental to the occurrence of the authorized transfer of money. To interpret the computer-fraud provision as reaching any fraudulent scheme in which an email communication was part of the process would . . . convert the computer-fraud provision to one for general fraud.[42]

The *Apache* ruling—which the Southern District of New York recently described as "unpersuasive"[43]—is questionable for many reasons, not the least of which is that the court mischaracterized the claim as predicated on the payment of "legitimate invoices," when the policyholder was actually seeking coverage due to the "computer usage" (emails from the criminal) that resulted in the payment to the wrong account. Further, while the court purportedly based its opinion on Texas's "preference" doctrine (e.g., a preference to follow opinions in other states when there is "cross-jurisdictional uniformity" on a disputed issue), the court cited only a few cases (none from a state high court) and ignored pro-policyholder cases on this issue. In addition, the court ignored Texas law on causation issues, which focuses on whether the conduct was the proximate cause, not the sole cause of the loss.[44]

Despite its flaws, the *Apache* decision has been relied on by courts in at least two other cases that ruled in favor of insurers on causation issues. In one of those cases, *American Tooling Center, Inc. v. Travelers Casualty & Surety Co. of America*,[45] policyholder employees authorized payments to a criminal's account based on spoofed emails. Citing *Apache*, the court ruled in favor of the insurer, reasoning that "given the intervening events between the receipt of the fraudulent emails and the (authorized) transfer of funds, it cannot be said that [the policyholder] suffered a 'direct' loss 'directly caused' by the use of any computer."[46] In addition, in *InComm Holdings, Inc. v. Great American Insurance Co.*,[47] the district court cited *Apache* and questionably reasoned that the loss was not caused by the actions of the criminals, but because the policyholder purportedly "failed to investigate" and because of the policyholder's "decision to wire the funds to [the bank]."[48] Both cases are on appeal.[49]

**Hacking defense: Courts have reached mixed results.** Another coverage defense that has been litigated in the BEC context is whether policies or bonds cover only "hacking" incidents. Insurers have argued in some cases that a mere email from a criminal requesting payment does not trigger coverage; rather, coverage should be restricted to situations in which the criminal hacks the policyholder's system and directly initiates the wire transfer or otherwise interferes with the policyholder's computer system. Courts have considered various related issues: (1) whether hacking is required at all; (2) whether other types of unauthorized access or use trigger coverage; and (3) proof of hacking or other unauthorized use.

**1. Is hacking required?** Courts have reached mixed results on whether hacking is required to trigger coverage and, if so, what exactly is required. Policyholders have argued that the policies at issue do not impose a hacking restriction and that courts should not read in this extra-contractual defense. Conversely, insurers frequently cite *Universal American Corp. v. National Union Fire Insurance Co. of Pittsburgh, Pa.*[50] In that case, the policyholder (a health insurer) sought coverage under a bond for over $18 million in losses resulting from its payment of fraudulent Medicare claims. The policyholder had a computerized billing system that allowed health care providers to submit claims directly to the system, and most claims were paid automatically, without manual review. Certain health care providers submitted

claims for services that were never performed, and the policyholder sought coverage for losses associated with payments on such claims.

The bond at issue provided computer systems fraud coverage for "Loss resulting directly from a fraudulent . . . entry of Electronic Data . . . or . . . change of Electronic Data . . . within the Insured's proprietary Computer System . . . provided that the entry or change causes . . . an account of the insured . . . to be added, deleted, debited or credited."[51] The insurer denied coverage, arguing that the policy "did not encompass losses for Medicare fraud, which [the insurer] described as losses from payment for claims submitted by health care providers."[52]

The *Universal American* court ruled for the insurer, reasoning that "the rider covers losses resulting from a dishonest entry or change of electronic data or a computer program, constituting what the parties agree would be 'hacking' of the computer system."[53] The *Universal American* court rejected the policyholder's argument that coverage extended to "losses from [fraudulent data] submitted by authorized users."[54]

Insurers also have cited *Taylor & Lieberman v. Federal Insurance Co.*[55] In that case, the policyholder sought coverage under a crime policy for sums that the policyholder wired to a criminal after receiving fraudulent emails. The policyholder argued that it was entitled to coverage under the computer fraud coverage part because the criminal's fraudulent emails constituted both (1) "an unauthorized . . . 'entry into' its computer system" and (2) "'introduction of instructions' that 'propogate[d] [sic] themselves' through its computer system."[56] The Ninth Circuit rejected these arguments. First, the court held that "there is no support for the [policyholder's] contention that sending an email, without more, constitutes an unauthorized entry into the recipient's computer system."[57] Second, the court held that the criminal's emails instructing the policyholder to make payments "are not the type of instructions that the policy was designed to cover, like the introduction of malicious computer code."[58]

In contrast, certain courts have ruled that there is no hacking requirement or that the insurers have misconstrued the reference to "hacking" in *Universal American*, or both. For example, in *Owens* (discussed above), the court rejected the insurer's argument that "for a computer fraud to exist, the transfer must occur by way of a 'computer hacking' incident, such as the manipulation of numbers or events through the use of a computer."[59] The court concluded that "the policy is ambiguous as to the amount of computer usage necessary to constitute computer fraud. This ambiguity is resolved in favor of the plaintiff. A 'computer hacking incident' is not required."[60]

Other courts have rejected the insurers' argument that *Universal American* imposes a broad hacking requirement under New York law. For example, in *Medidata*, the Southern District of New York held that

> [the insurer's] reading of *Universal* is overbroad. . . . It is true that the Court of Appeals in *Universal* peppered its opinion with references to hacking as the example for a covered violation. But a hacking is one of many methods a thief can use, and "is an everyday term for unauthorized access to a computer system." Thus, *Universal* is more appropriately read as finding coverage for fraud where the perpetrator violates the integrity of a computer system through unauthorized access and denying coverage for fraud caused by the submission of fraudulent data by authorized users.[61]

**2. Does unauthorized use or conduct by an unauthorized user trigger coverage?** Courts also have addressed related questions on what "use" of a computer system is required and by whom. For example, courts have considered whether use by an unauthorized user is sufficient to trigger coverage. In *Universal American*, in ruling for the insurer, the court focused on the fact that *authorized* users entered fraudulent data into the policyholder's computer system. *Universal American* arguably did not consider or rule out other potential scenarios that could trigger coverage, such as claims based on the conduct of an unauthorized user that did not involve breaking firewalls or introducing viruses.

Notably, in *Medidata*, the Southern District of New York cited with approval the trial court opinion in *Universal American*, stating that "an examination of the trial court's analysis in *Universal* . . . 'indicates that coverage is for an unauthorized entry into the system, e.g., by an unauthorized user.'"[62]

In considering whether conduct of an authorized user could ever trigger coverage, it is notable that some insurers have included exclusions that potentially apply to loss arising from the input of data by an authorized user. If an insurer does not expressly exclude this risk, the policyholder may argue that the court should not write this restriction into the policy.

To illustrate, in *Aqua Star (USA) Corp. v. Travelers Casualty & Surety Co. of America*,[63] the district court ruled in favor of the insurer based on an exclusion for "loss resulting *directly or indirectly* from the input of Electronic Data by a natural person *having the authority* to enter the Insured's Computer System."[64] In *Aqua Star*, a criminal monitored emails between the policyholder and a vendor and then sent spoofed emails purportedly from the vendor asking the policyholder to change the bank account information for wire transfers. The policyholder's employee updated records with the false account information and used the information for wire transfers.

The insurer argued that there was no coverage because the "entry" had been made by an employee authorized to use the computer system. The policyholder argued that the exclusion applied only when a fraud is perpetrated by an authorized user, such as a customer or employee, but did not apply when an employee made changes to billing information based on emails received from criminals who had no authority with respect to the policyholder's computer system.

The *Aqua Star* court agreed with the insurer, stating that the entry of data by the employee "was an intermediate step in the chain of events that led [the policyholder] to transfer funds to the hacker's bank accounts. . . . Because an *indirect* cause of the loss was the entry of Electronic Data into [the policyholder]'s Computer System by someone with authority to enter the system," the exclusion applied.[65] This limited holding is based on the broad scope of this particular exclusion, which applied not only to loss "resulting directly" from entry of data by an authorized person, but also to loss "resulting indirectly" from such entry. This case remains on appeal in the Ninth Circuit.[66]

Further, courts have considered whether coverage could be available for losses arising from unauthorized activities of authorized users. In *Pestmaster Services, Inc. v. Travelers Casualty & Surety Co. of America*,[67] the policyholder hired a vendor who was responsible for paying payroll taxes to the Internal Revenue Service (IRS) on behalf of the policyholder. The vendor would send invoices to the policyholder for approval, and once the invoices were approved, the vendor had the standing authority to initiate a transfer from the policyholder's bank account to the vendor's account for eventual payment to the IRS. After withdrawing the funds from the policyholder's account, however, the vendor used the policyholder's funds for its own purposes, leaving the policyholder's debt to the IRS unpaid. The vendor also made other transfers that were not authorized, e.g., for amounts larger than the amounts on approved invoices.[68] Thus, although the vendor was authorized to access the policyholder's system and make payments, it was not authorized to make payments for the amounts transferred.

The policyholder sought coverage under various coverage parts in a crime policy, including a fund transfer provision and a computer fraud provision.[69] With respect to the fund transfer provision, the Ninth Circuit held that this provision "does not cover authorized or valid electronic transactions . . . even though they are . . . associated with a fraudulent scheme."[70]

The computer fraud provision covered "[t]he use of any computer to fraudulently cause a transfer."[71] The Ninth Circuit interpreted the phrase "fraudulently cause a transfer" to require an unauthorized transfer of funds. The court held that "[w]hen [the vendor] transferred funds pursuant to authorization from [the policyholder], the transfer was not fraudulently caused."[72] The court reasoned that "reading this provision to cover all transfers that involve both a computer and fraud at some point in the transaction would convert this Crime Policy into a 'General Fraud' Policy," which "is not what was intended by this provision."[73] Notably, however, the Ninth Circuit reversed the district court's ruling and remanded for further proceedings with respect to the coverage for the unauthorized transfers made by the authorized vendor, which arguably suggests the potential for coverage for losses arising from unauthorized acts by authorized users (e.g., for amounts greater than approved invoices).[74]

**3. Proof of hacking or other relevant use.** To date, many opinions have focused primarily on legal issues (Does employee involvement defeat causation? Is hacking

required?). Going forward, coverage disputes may focus more on factual issues and expert testimony related to the technical details of the criminal's scheme at issue. Thus, even if a court imposes some hacking or use requirement, coverage will then turn on the facts of the case, and policyholders and insurers may turn to experts to testify as to the technical details of the criminal's scheme.

The recent opinion in *Medidata* (discussed above) is illustrative. In *Medidata*, a policyholder employee wired funds to a criminal's bank account after receiving emails purportedly from a company executive. The insurer denied coverage on the ground that the "impostor *did not* hack Medidata's computers, implant those computers with a virus, breach any firewalls or otherwise manipulate Medidata's computers."[75]

The court denied the parties' initial competing motions for summary judgment without prejudice on the legal issue of whether the policy required some sort of "hacking" and ordered the parties to conduct expert discovery related to "the method in which the perpetrator sent its emails to plaintiff and discussing what changes, if any, were made to plaintiff's computer system when the emails were received."[76] Following expert discovery, the parties renewed their motions for summary judgment, focusing on the technical aspects of the criminal scheme. On these revised motions, the district court granted summary judgment in favor of the policyholder.[77]

As discussed above, the *Medidata* court rejected the insurer's broad hacking defense as a matter of law, reasoning that "hacking is one of many methods a thief can use, and 'is an everyday term for unauthorized access to a computer system.'"[78] The court then turned to the facts, in part the criminal's use of computer code that tricked the computer system into adding the Medidata's president's email address and photo to the criminal's emails. The court described the criminal's conduct as follows:

> It is undisputed that the theft occurred by way of email spoofing. To that end, the thief constructed messages in Internet Message Format ("IMF") which the parties compare to a physical letter containing a return address. The IMF message was transmitted to Gmail in an electronic envelope called a Simple Mail Transfer Protocol ("SMTP"). Much like a physical envelope, the SMTP Envelope contained a recipient and a return address. To mask the true origin of the spoofed emails, the thief embedded a computer code. The computer code caused the SMTP Envelope and the IMF Letter to display different email addresses in the "From" field. The spoofed emails showed the thief's true email address in the SMTP "From" field, and Medidata's president's email address in the IMF "From" field. When Gmail received the spoofed emails, the system compared the address in the IMF "From" field with a list of contacts and populated Medidata's name and picture. The recipients of the Gmail messages only saw the information in the IMF "From" field.[79]

The court held that this "fraud on Medidata falls within the kind of 'deceitful and dishonest' access imagined by the New York Court of Appeals" and therefore granted summary judgment to the policyholder.[80]

*Medidata* is instructive in how courts may analyze BEC claims in the future in cases that focus on factual and expert issues related to the specific conduct at issue.

**Conclusion**

While courts have reached mixed results to date, policyholders may have strong arguments in favor of coverage for many BEC losses. Even if insurers prevail on issues of contract interpretation, coverage disputes ultimately may turn on factual issues or expert testimony concerning the technical aspects of the criminal's scheme (or both). In sum, policyholders should evaluate their existing coverage and consider seeking additional coverage during policy renewals. In addition, when faced with a BEC loss, policyholders should take steps to preserve their rights under relevant insurance policies.

Gregory Wright is a partner and Gillian Giannetti is an associate at K&L Gates LLP in Washington, D.C.

[1] *See* Fed. Bureau of Investigation, Alert No. I-050417-PSA, Business E-Mail Compromise: E-mail Account Compromise—The 5 Billion Dollar Scam [hereinafter FBI Alert No. I-050417-PSA].
[2] *See* FBI Alert No. I-050417-PSA.
[3] *See* FBI Alert No. I-050417-PSA.
[4] *See* FBI Alert No. I-050417-PSA.
[5] *See* Richard Wickliffe, "Gone Phishing: CEO Fraud Snags Millions for Fraudsters," *PropertyCasualty360*, Sept. 1, 2016.
[6] *See* Antony Ireland, "Covering Fraudulent Impersonation," *Risk & Ins.*, July 22, 2015.
[7] *See* FBI Alert No. I-050417-PSA.
[8] *See* FBI Alert No. I-050417-PSA.
[9] *See* Trend Micro, Billion-Dollar Scams: The Numbers Behind Business Email Compromise (June 9, 2016).
[10] *See* Fed. Bureau of Investigation, Business E-Mail Compromise Timeline (Feb. 27, 2017).
[11] *See* FBI Alert No. I-050417-PSA.
[12] See the commercial crime policy at issue in Principle Solutions Group, LLC v. Ironshore Indemnity, Inc., No. 1:15-CV-4130-RWS, slip op. at 4 (N.D. Ga. Aug. 30, 2016).
[13] See the financial institutions bond at issue in State Bank of Bellingham v. BancInsure, Inc., 823 F.3d 456, 458 & n.2 (8th Cir. 2016).
[14] For example, Hartford has offered a "Deception Fraud Endorsement" for its crime insurance forms, which Hartford describes as "[c]ritical coverage to help your business prevail against crimes of deception and trickery." *See* Hartford, Crime

Insurance—Deception Fraud Coverage, at 1 (Aug. 2015). Beazley also reportedly has offered a fraudulent instruction endorsement for its commercial crime policy that affords coverage, potentially subject to a sublimit, against the "transfer of funds as a result of fraudulent instructions from a person purporting to be a vendor, client, or authorized employee." *See* "Beazley Introduces Fraudulent Instruction Insurance," *Ins J.*, June 25, 2015; Beazley, Fidelity & Crime.

[15] *Principle Sols. Grp., LLC v. Ironshore Indem., Inc.*, No. 1:15-CV-4130-RWS, slip op. (N.D. Ga. Aug. 30, 2016), *appeal filed*, No. 17-11703 (11th Cir. Apr. 13, 2017), *appeal stayed*, No. 17-11703 (11th Cir. May 15, 2017).

[16] Principle Solutions, No. 1:15-CV-4130-RWS, slip op. at 2.

[17] Principle Solutions, No. 1:15-CV-4130-RWS, slip op. at 4.

[18] Principle Solutions, No. 1:15-CV-4130-RWS, slip op. at 11–12.

[19] Principle Solutions, No. 1:15-CV-4130-RWS, slip op. at 12.

[20] Principle Solutions, No. 1:15-CV-4130-RWS, slip op. at 12–13 (citation omitted).

[21] Notice of Appeal, *Principle Solutions*, No. 1:15-CV-4130-RWS (N.D. Ga. Apr. 13, 2017), ECF No. 77. On May 15, 2017, the Eleventh Circuit granted a joint motion to stay the appellate proceedings pending the district court's resolution of a pending "Motion to Amend Judgment" filed by the policyholder on April 18, 2017.

[22] Medidata Sols., Inc. v. Fed. Ins. Co., No. 15-cv-907 (ALC), 2017 U.S. Dist. LEXIS 122210 (S.D.N.Y. July 21, 2017), *appeal filed*, No. 17-2492 (2d Cir. Aug. 11, 2017).

[23] Medidata, 2017 U.S. Dist. LEXIS 122210, at *22.

[24] Medidata, 2017 U.S. Dist. LEXIS 122210, at *18.

[25] Notice of Appeal, *Medidata*, No. 17-2492 (2d Cir. Aug. 11, 2017).

[26] State Bank of Bellingham v. BancInsure, Inc., 823 F.3d 456 (8th Cir. 2016).

[27] The bond at issue in *Bellingham* afforded coverage in part for "Loss resulting directly from a fraudulent (1) entry of Electronic Data or Computer Program into, or (2) change of Electronic Data or Computer Program within any Computer System operated by the Insured, . . . provided the entry or change causes . . . an account of the Insured or of its customer to be added, deleted, debited or credited." Bellingham, 823 F.3d at 458 & n.2.

[28] Bellingham, 823 F.3d at 458 & n.3.

[29] Bellingham, 823 F.3d at 461.

[30] Bellingham, 823 F.3d at 461 (citation omitted).

[31] Bellingham, 823 F.3d at 461.

[32] Bellingham, 823 F.3d at 461.

[33] Owens, Schine & Nicola, P.C. v. Travelers Cas. & Sur. Co. of Am., No. CV095024601, 2010 Conn. Super. LEXIS 2386 (Conn. Super. Ct. Sept. 20, 2010), *vacated by stipulation of parties*, 2012 Conn. Super. LEXIS 5053 (Conn. Super. Ct. Apr. 18, 2012). While the *Owens* opinion was vacated by stipulation of the parties, policyholders should still consider *Owens* when evaluating their potential claims, as the vacated opinion has been considered by other courts (see discussion of the *Universal American* and *Apache* cases below).

[34] Owens, 2010 Conn. Super. LEXIS 2386, at *9.

[35] Owens, 2010 Conn. Super. LEXIS 2386, at *5.

[36] Owens, 2010 Conn. Super. LEXIS 2386, at *18–19.
[37] Owens, 2010 Conn. Super. LEXIS 2386, at *22–23.
[38] Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252 (5th Cir. 2016) (per curiam).
[39] Apache, 662 F. App'x at 254.
[40] Apache, 662 F. App'x at 254.
[41] *See generally* Apache, 662 F. App'x 252.
[42] Apache, 662 F. App'x at 258 (citation omitted).
[43] Medidata Sols., Inc. v. Fed. Ins. Co., No. 15-cv-907 (ALC), 2017 U.S. Dist. LEXIS 122210, at *18 (S.D.N.Y. July 21, 2017).
[44] Appellee's Petition for Panel Rehearing at 13–14, *Apache*, No. 15-20499 (5th Cir. Nov. 11, 2016).
[45] Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., No. 5:16-cv-12108-JCP, 2017 U.S. Dist. LEXIS 120473 (E.D. Mich. Aug. 1, 2017), *appeal filed*, No. 17-2014 (6th Cir. Aug. 29, 2017).
[46] American Tooling Center, 2017 U.S. Dist. LEXIS 120473, at *5. Notably, the court distinguished *Owens* based on differences between Michigan law (at issue in *American Tooling*) and Connecticut law (at issue in *Owens*) on the meaning of "direct." Michigan courts had interpreted the term "direct" to mean "immediate," whereas Connecticut courts had interpreted the term "direct" to mean "proximate." *See* American Tooling Center, 2017 U.S. Dist. LEXIS 120473, at *5. Thus, *American Tooling* should be limited to cases governed by Michigan law or similar law.
[47] InComm Holdings, Inc. v. Great Am. Ins. Co., No. 1:15-cv-2671-WSD, 2017 U.S. Dist. LEXIS 38132 (N.D. Ga. Mar. 16, 2017), *appeal filed*, *Interactive Commc'ns Int'l v. Great Am. Ins. Co.*, No. 17-11712 (11th Cir. Apr. 17, 2017).
[48] InComm Holdings, 2017 U.S. Dist. LEXIS 38132, at *32. An appeal of this ruling is currently pending before the Eleventh Circuit. *See* Notice of Appeal, *Interactive Commc'ns Int'l v. Great Am. Ins. Co.*, No. 17-11712 (11th Cir. Apr. 17, 2017).
[49] Notice of Appeal, *Am. Tooling Ctr. v. Travelers Cas. & Sur. Co. of Am.*, No. 17-2014 (6th Cir. Aug. 29, 2017); Notice of Appeal, *Interactive Commc'ns Int'l v. Great Am. Ins. Co.* (*InCommHoldings*), No. 17-11712 (11th Cir. Apr. 17, 2017).
[50] Universal Am. Corp. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa., 37 N.E.3d 78 (N.Y. 2015).
[51] Universal Americ*an* Corp., 37 N.E.3d at 79.
[52] Universal Americ*an* Corp., 37 N.E.3d at 80.
[53] Universal Americ*an* Corp., 37 N.E.3d at 80.
[54] Universal American Corp., 37 N.E.3d at 82.
[55] Taylor & Lieberman v. Fed. Ins. Co., 681 F. App'x 627 (9th Cir. 2017).
[56] Taylor & Lieberman, 681 F. App'x at 629.
[57] Taylor & Lieberman, 681 F. App'x at 629.
[58] Taylor & Lieberman, 681 F. App'x at 629. The Ninth Circuit also held that the "forgery" and "funds transfer fraud" coverage parts did not apply. *See generally* Taylor & Lieberman, 681 F. App'x 627.

[59] Owens, Schine & Nicola, P.C. v. Travelers Cas. & Sur. Co. of Am., No. CV095024601, 2010 Conn. Super. LEXIS 2386, at *13 (Conn. Super. Ct. Sept. 20, 2010), *vacated by stipulation of parties*, 2012 Conn. Super. LEXIS 2386 (Conn. Super. Ct. Apr. 18, 2012).
[60] Owens, 2010 Conn. Super. LEXIS 2386, at *19.
[61] Medidata Sols., Inc. v. Fed. Ins. Co., No. 15-cv-907 (ALC), 2017 U.S. Dist. LEXIS 122210, at *14–15 (S.D.N.Y. July 21, 2017) (citation omitted).
[62] Medidata, 2017 U.S. Dist. LEXIS 122210, at *15.
[63] Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am., No. C14-1368RSL, 2016 U.S. Dist. LEXIS 88985 (W.D. Wash. July 8, 2016), *appeal filed*, No. 16-35614 (9th Cir. Aug. 1, 2016).
[64] Aqua Star, 2016 U.S. Dist. LEXIS 88985, at *5 (emphasis added).
[65] Aqua Star, 2016 U.S. Dist. LEXIS 88985, at *7–8 (emphasis added).
[66] Notice of Appeal, *Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am.*, No. 16-35614 (9th Cir. Aug. 1, 2016).
[67] Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am., 656 F. App'x 332 (9th Cir. 2016).
[68] *See, e.g.*, Plaintiff's Memorandum of Points and Authorities in Opposition to Motion for Summary Judgment Or, in the Alternative, Partial Summary Judgment at 3, *Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.*, No. CV 13-5039 JFW (MRWx) (C.D. Cal. June 12, 2014) ("On May 23, 2011, not only the $21,508.68 was transferred, but also [the vendor] took another $8,080.79. On May 27, 2011, it took another $3,911.10. These amounts, totaling $11,991.89 appear nowhere on the May 19, 2011 invoice or any other document.").
[69] Pestmaster, 656 F. App'x at 333.
[70] Pestmaster, 656 F. App'x at 333 (quoting Pestmaster, No. CV 13-5039 JFW (MRWx), 2014 U.S. Dist. LEXIS 108416, at *16 (C.D. Cal. July 17, 2014)).
[71] Pestmaster, 656 F. App'x at 333.
[72] Pestmaster, 656 F. App'x at 333.
[73] Pestmaster, 656 F. App'x at 333.
[74] Pestmaster, 656 F. App'x at 333. The case subsequently settled. *See* Notice of Settlement, *Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.*, No. CV 13-5039-JFW (MRWx) (C.D. Cal. Oct. 13, 2016), ECF No. 101.
[75] Defendant's Memorandum of Law in Support re: Motion for Summary Judgment at 1, *Medidata Solutions, Inc. v. Fed. Ins. Co.*, No. 15-cv-907 (ALC) (S.D.N.Y. Aug. 13, 2015), ECF No. 34.
[76] *Medidata*, No. 15-cv-907 (ALC), slip. op. (S.D.N.Y. Mar. 10, 2016), ECF No. 64.
[77] Medidata, No. 15-cv-907 (ALC), 2017 U.S. Dist. LEXIS 122210, at *1.
[78] Medidata, 2017 U.S. Dist. LEXIS 122210, at *15 (citation omitted).
[79] Medidata, 2017 U.S. Dist. LEXIS 122210, at *13–14.
[80] Medidata, 2017 U.S. Dist. LEXIS 122210, at *13 (quoting Universal Am. Corp. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa., 37 N.E.3d 78, 81 (N.Y. 2015)).