MEALEY'S®

Emerging Insurance Disputes

Can Human Error Really Constitute Insured Computer Fraud? A Circuit Split On Coverage For Spoofing Claims Will Spur More Litigation

by
Laura Foggan
and
Stephanie V. Corrao

Crowell & Moring
Washington, D.C.

A commentary article reprinted from the August 2, 2018 issue of Mealey's Emerging Insurance Disputes

LexisNexis®

Commentary

Can Human Error Really Constitute Insured Computer Fraud? A Circuit Split On Coverage For Spoofing Claims Will Spur More Litigation

By
Laura Foggan
and
Stephanie V. Corrao

[Editor's Note: Laura Fogganis a partner in Crowell & Moring's Washington, D.C. office, and chair of the firm's Insurance/Reinsurance Group. Stephanie V. Corrao is a Washington, D.C.-based associate in the firm's Insurance and Reinsurance Group, where she represents insurers and reinsurers on a range of matters, from providing pre-dispute advice and legal analysis of specific contract provisions and coverage issues to working to resolve complex disputes before courts and arbitrators. Any commentary or opinions do not reflect the opinions of LexisNexis®, Mealey Publications™. Copyright © 2018 by Laura Foggan and Stephanie Corrao. Responses are welcome.]

A fraudster, posing as a company's CEO, sends an email to the company's accounting department and tricks an employee into transferring company funds to an offshore bank account. By the time the ruse is discovered, the money is long gone. Does the company's crime policy cover the loss resulting from this business email compromise ("BEC") claim, also known as a "spoofing" attack?

In the courts, the answer to that question under widely-used computer fraud coverage terms is decidedly uncertain. While coverage for spoofing claims has been a hot issue this summer — prompting two federal circuit court rulings, courts remain split on the issues and the case law continues to develop.[1] Multiple courts have concluded that computer fraud coverage is intended to apply solely to "unauthorized" attacks on a policyholder's computer system. What is surprising is that, in recent, prominent rulings, two courts did not recognize and enforce fundamental limits on computer fraud coverage — and thus extended insurers' liability beyond instances where an unauthorized user causes a computer to act in a manner resulting in loss (such as through hacking or the use of malicious code or other alteration of electronic data in a computer system).

In rulings this July, the United States Courts of Appeal in the Second and Sixth Circuits found that computer fraud coverage included loss resulting from human error — where an "authorized" user, who has been tricked by spoofing, purposefully transfers funds out of the policyholder's account.[2] These decisions, which throw into doubt the confines of computer fraud coverage, are far from the last word. There is a closely-watched case pending now before the Eleventh Circuit, and there is a sharp conflict between the circuits under existing law.[3]

Courts are wrestling with a number of questions in determining whether "spoofing" claims are covered under "computer fraud" provisions of crime policies. For instance, how much "computer use" is enough — does the fraudster's use of e-mail alone make it *computer* fraud? Is the deceived employee's *authorized* use of the company computer system a "*fraudulent*" entry into the computer system? Did the fraudster's actions *proximately cause* the company's loss, or were the voluntary actions of authorized company employees, or of a vendor or customer, an *intervening cause*? For the loss to "*result directly from*" the fraudulent conduct, as most policies require, must the loss also be "immediate"? Is there an exclusion for loss resulting, directly (or indirectly), from an "authorized" user's entry of electronic data into the company's computer system? And, do variations in crime policy language drive different outcomes?[4] These are the questions underlying the split of authority on the scope of coverage afforded by computer fraud provisions.

Is Unauthorized Access Required?

Probably the most fundamental question in the debate over the breadth of computer fraud coverage is whether the coverage applies only to computer "hacking" or to something more. The New York Court of Appeals and the United States Court of Appeals for the Ninth Circuit have both held that crime fraud coverage applies only to *unauthorized* access to a computer system, and not where fraudulent content is submitted to the computer system by *authorized* users.[5] Many observers believe this is the key limit to the coverage, and thus it is flatly wrong to allow coverage for "spoofing" or BEC claims.

In *Universal Am. Corp. v. Nat'l Union Fire Ins. Co.*,[6] New York's highest court held that the crime fraud provision of an insurance bond did not provide coverage for losses resulting from amounts paid through the policyholder's computerized billing system for fraudulent health care claims for unperformed services. The policy included a rider covering "computer systems fraud" which covered "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 the Insured's proprietary Computer System. . . ." The court below concluded the unambiguous language of the policy did not cover fraudulent content entered by authorized users, but rather "wrongful acts in manipulation of the computer system, i.e., by hackers," and the New York Court of Appeals affirmed. Specifically, the Court held that the phrase "fraudulent entry . . . of Electronic Data" unambiguously applied only to "unauthorized access" to the computer system and not to content submitted to the computer system by "*authorized* users."[7] It explained that "fraudulent" refers to deceit and dishonesty and modifies "entry" or "change" of electronic data or computer program, meaning it qualifies the act of entering or changing data or a computer program. "The intentional word placement of 'fraudulent' before 'entry' and 'change' manifests the parties' intent to provide coverage for a violation of the integrity of the computer system through deceitful and dishonest access," the Court said.

The Court found that other language in the policy confirmed that the rider sought to address unauthorized access. It stated that the headings "Computer Systems," and "Computer Systems Fraud" clarified that the focus is on the computer system qua computer system. It also cited an exclusion for coverage losses resulting directly or indirectly from fraudulent instruments "which are used as source documentation in the preparation of Electronic Data, or manually keyed into a data terminal." The Court noted that, if the parties had intended to cover fraudulent content, such as the billing fraud at issue, then there would be no reason to exclude fraudulent content contained in documents used to prepare electronic data, or manually keyed into a data terminal. The New York high court thus concluded that the computer fraud coverage was limited to "losses resulting from a dishonest entry or change of electronic data or computer program, constituting what the parties agree would be 'hacking' of the computer system."[8]

The Ninth Circuit similarly held in *Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.*, that computer fraud coverage requires an *unauthorized* transfer of funds.[9] There, the policyholder hired a firm to submit its payroll taxes to the IRS, but the firm failed to do so. The policyholder then sought to recover the transfer of funds from its bank account to the payroll firm's bank account. The policy defined Computer Fraud as "[t]he use of any computer to fraudulently cause a transfer" The Court held that the phrase "fraudulently cause a transfer" required an unauthorized transfer of funds, and concluded that because the transfer of funds from the policyholder to the accounting firm was authorized, the transfer was not "fraudulently caused" and no coverage applied.[10] The Ninth Circuit reasoned: "Because computers are used in almost every business transaction, 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."[11] As the Court explained, reading the computer fraud coverage as protection against *all* fraud is not what was intended, and not what Pestmaster could reasonably have expected this provision to cover.

The Ninth Circuit specifically addressed whether an *unauthorized* entry is necessary for coverage in the context of a spoofing attack in *Taylor & Lieberman v. Federal Ins. Co.*[12] There, an accounting firm sought coverage for loss resulting from wire transfers the firm made to a fraudster that had taken over a client's email account. The Ninth Circuit denied coverage, resolving that the mere sending of an email, without more, does not constitute an "unauthorized entry" into the policyholder's computer system for purposes of computer fraud coverage.[13] In addition, the Court held that, under a common sense reading of the policy, email instructions on how to complete the wire transfer were not the type of "unauthorized introduction of instructions" that "propagate themselves" through a computer system which the policy was designed to cover — "like the introduction of malicious computer code."[14]

In yet another spoofing case, the Ninth Circuit held earlier this year in *Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am.*[15] that, under Washington law, there was no coverage for an employee's authorized entry of data to change wiring information in execution of a wire transfer of company funds. The policy excluded 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."[16] The Court found that the employees had the authority to enter the company's computer system when they input the wiring information and, thus, their conduct fit "squarely within the Exclusion."[17]

All of these decisions recognize a key concept: computer fraud insurance is not intended to cover loss resulting from human error, which, by definition, is what generates the loss in spoofing claims. In spoofing claims, authorized users mistakenly comply with a fraudulent request to transfer company funds. Whether the employee's failure to identify the fraud is due to negligence, poor training, or inadequate safety protocols within the company, none of these things are covered by computer fraud insurance.[18] Quite simply, computer fraud coverage does not respond to all instances of fraud. It addresses the risk that an unauthorized party will hack into the company's computer system, causing the computer to do something, without the need for additional human intervention, resulting in a loss.

However clear the limits of computer fraud coverage may appear, this summer they were muddied by two prominent decisions. In July, in *American Tooling Center, Inc. v. Travelers Cas. & Sur. Co. of America*,[19] the Sixth Circuit refused to find that computer fraud is limited to "hacking and similar behaviors in which a nefarious party somehow gains access to and/or controls the insured's computer[.]"[20] In that case, the fraudster masqueraded as a legitimate vendor of the policyholder. The policy defined "Computer Fraud" to mean "[t]he use of any computer to fraudulently cause a transfer" of money.[21] Based on that language, the Court held that the fraud did not have to "cause the computer to do anything" in order to constitute "computer fraud."[22] The policy also expressly excluded 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."[23] However, the Sixth Circuit determined that the exclusion did not apply to the manual entry of banking details by an authorized employee because it found the fraudulent bank routing information constituted "instructions or directions to a Computer System," which was excluded from the policy's definition of "Electronic Data."[24] The Court did not discuss how its interpretation of the policy language comported with the intent of computer fraud coverage.[25]

Also in July, the Second Circuit addressed coverage for a spoofing claim in *Medidata Solutions, Inc. v. Federal Insurance Co.*[26] There, a fraudster, posing as the policyholder's president, used an altered e-mail address to convince the company's finance department to wire money to an account for a purported corporate acquisition.[27] Importantly, Medidata's email services were provided through Google's Gmail platform, and the fraudster's messages to Gmail embedded a computer code that caused Google to change the "From" field in the spoofed email from the fraudster's actual email address to the email address of the company president.[28] Thus, as the court found, the fraudsters crafted a computer-based attack that manipulated Medidata's email system, which the parties did not dispute constituted a "computer system" within the meaning of the policy. As the Second Circuit explained, the fraudster's alteration of the "From" field in the spoofed emails constituted a "fraudulent . . . entry of Data" into a computer system, and the fraudster's insertion of computer code in its messages through Google's Gmail system constituted a "'change to Data elements or program logic of' a Computer System."[29] In short, the fraudster had infiltrated the company's computer system by embedding code into the messages sent to Gmail which triggered Google's population of the email with false information concerning the identity of the sender.[30] The Second Circuit thus rejected the insurer's arguments and distinguished cases where spoofing losses only incidentally involved the use of computers, because the fraudulent instructions were sent via email and the company processed payments using computers (as opposed to on paper).[31] Here, the Court found that the fraud implicated the "the computer system qua computer system" and entailed "a violation of the integrity of the computer system through deceitful and dishonest access."[32] Even if fraudulent alteration of the policyholder's computer system was at issue, however, the incident required Medidata employees to transfer funds in accordance with the fraudulent instructions in the emails that tricked them through use of the malicious code. Even though employee actions were necessary to effectuate the transfer of funds, the Court found that the loss was "directly" caused by the computer fraud, an issue that is discussed further below.

Direct Loss/Proximate Causation

Another key issue in the cases discussing the scope of computer fraud coverage is causation — whether the computer fraud proximately caused the policyholder's loss, or whether the circumstances of the loss meet policy language often expressly requiring that computer fraud result in a "direct loss" to the policyholder. In spoofing cases, this manifests itself in questions about whether employees' conduct in effectuating the transfer of funds constitutes an intervening cause or makes the loss an indirect result of computer fraud. The decisions are split on this element of the coverage, as well.

In *Apache Corp. v. Great American Ins. Co.*,[33] for example, the Fifth Circuit, applying Texas law, held that there was no coverage under a crime fraud policy for a spoofing claim because the policyholder's loss did not "result directly from" the falsified email as the policy required. In that case, fraudsters sent an email from an incorrect website address instructing the insured to use a new bank account to make payments to a vendor.[34] Employees in the payroll department obliged, paying approximately $7 million for false invoices.[35] The Fifth Circuit found that the transfer of funds was made by authorized employees only because, after receiving the fraudulent email request, the employees "failed to investigate accurately" the new, but false information.[36] The court found no coverage, concluding that the spoofing email "was part of the scheme but merely incidental to authorized transfer of money."[37]

In another causation case, the Eleventh Circuit held in *Interactive Communications Int'l, Inc. v. Great American Ins. Co.*,[38] that a computer fraud provision did not cover loss resulting from more than $11 million in fraudulent credit card redemptions. There, the policy provided coverage for "loss of... money... resulting directly from the use of any computer to fraudulently cause a transfer."[39] The Court first held that the term "resulting directly meant that one thing results "directly from another if it follows straight away, immediately, and without any intervention or interruption."[40] The Court then found that, while the fraudsters' use of the company's computerized interactive-telephone system constituted sufficient "use of a computer," the company's loss did not "result[] directly from" that use, as required by the policy.[41] Rather, the loss to the company was "temporally remote" (weeks or months might pass before the redemption was used), and several steps "intervened" or "interrupted" the chain of events between the duplicate redemption and the company's disbursement of funds to pay a merchant for purchases made by a cardholder using the fraudulently obtained funds.[42]

Again, other courts have reached contrary conclusions, including the Second Circuit in its recent decision in *Medidata*. There, the Court reasoned that because the chain of events "was initiated by the spoofed emails" and "unfolded rapidly following their receipt," the spoofing attack was the proximate cause of Medidata's losses — even though Medidata employees themselves had to take action to effectuate the transfer. The Court did not address the series of steps required for verification of the transfer, the importance of two phone calls in convincing the employees that the request was legitimate, or the fact that following the second attempt, an employee did in fact find the email "suspicious." Rather, the Court summarily concluded: "we do not see the [employees'] actions as sufficient to sever the causal relationship."[43]

Likewise, in *American Tooling Center, Inc. v. Travelers Cas. & Sur. Co. of America*,[44] the Sixth Circuit, applying Michigan law, held that the vendor-impersonation spoofing scheme resulted in a "direct loss" to the company, and that the loss was "directly caused by" the alleged computer fraud. There, the policy stated that the insurer would "pay the Insured for the Insured's direct loss of. . . Money. . . directly caused by Computer Fraud."[45] Company employees had received a series of emails, purportedly from its Chinese vendor, claiming that the vendor had changed its bank accounts and that payments should be wired to these new accounts.[46] The Court first concluded that the transfer of money constituted a "direct loss," without deciding whether direct means "immediate only," or simply "proximate," because under either definition, it believed the loss was "direct."[47] It viewed the loss as immediate once the money was transferred, and further found no "intervening event."[48] The Court reasoned that while the company employees conducted a series of internal actions following the spoofing email, those actions were "all induced by the fraudulent email" and, therefore, direct causation was established.[49] The Court did not consider the steps taken by the company employees themselves in reviewing the false invoices, obtaining internal approvals, and failing to identify the fraud prior to transferring the funds, as an intervening cause.[50]

The "direct loss" issue has also been teed up for the Eleventh Circuit in a pending appeal in *Principle Solutions Group, LLC v. Ironshore Indemn., Inc.*[51] There, the fraudster, posing as a company executive, convinced the company's controller to wire funds from the company account for purposes of a corporate acquisition.[52] This was followed by another email and a phone call from someone posing to be the company's outside counsel for corporate acquisitions.[53] The policy provided for coverage of "loss resulting directly from a 'fraudulent instruction' directing a 'financial institution' " to transfer of funds out of the policyholder's account.[54] Applying Georgia law, the district court found coverage based on its conclusion that the policy was ambiguous as to whether coverage applies when there are "intervening events" between the spoofing email and the loss. On appeal, the insurer argues that applying the plain and ordinary meaning of the language in the insuring agreement, the loss did not result "directly from" the alleged fraudulent instruction because there were numerous intervening events between the initial spoofing email and the wire transfer. The parties have completed briefing of the appeal and now await a decision from the Eleventh Circuit.

Conclusion

Although "computer fraud" insurance should not encompass loss caused by human error such as spoofing claims, the courts now are split on several key questions as to the scope of "computer fraud" coverage. Several cases recognize that computer fraud coverage is designed to insure against a particular risk — the risk that an unauthorized "hacker" will infiltrate the policyholder's computer. Other decisions do not reflect this concept, instead expanding this coverage to include loss resulting from the unfortunate actions of a mistaken employee, who, though bamboozled, is *authorized to* access the company computer.

The divergence in the case law reflects a fundamental misunderstanding by some courts of the boundaries of computer fraud coverage. As to the issues of what constitutes "computer fraud" and when a loss directly results, we expect that litigation will continue given the unsettled and divided state of the law. In the coming months, we will all learn more about courts' views on whether computer fraud coverage somehow encompasses loss caused by authorized users who are tricked by spoofing.

Endnotes

1. *Compare Medidata Solutions, Inc. v. Fed. Ins. Co.*, No. 17-2492-cv, 2018 U.S. App. LEXIS 18376, 2018 WL 3339245 (2d Cir. July 6, 2018) ("*Medidata I*") and *Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am.*, No. 17-2014, 2018 U.S. App. LEXIS 19208, 2018 WL 3404708 (6th Cir. July 13, 2018) ("*Am. Tooling*") *with Apache Corp. v. Great Am. Ins. Co.*, 662 F. App'x 252 (5th Cir. 2016) and *Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.*, 656 F. App'x 332 (9th Cir. 2016) ("*Pestmaster*").

2. *Medidata I,* 2018 U.S. App. LEXIS 18376, 2018 WL 3339245; *Am. Tooling,* 2018 U.S. App. LEXIS 19208, 2018 WL 3404708.

3. *See Principle Solutions Grp., LLC v. Ironshore Indemn., Inc.*, No. 1:15-CV-4130-RWS, 2016 WL 4618761 (N.D.Ga. Aug. 30, 2016) ("*Principle Solutions*"), *on appeal sub nom. PSG Parent, Inc. v. Ironshore Indem., Inc.*, No. 17-11703-FF (11th Cir. 2018).

4. The policy language defining "Computer Fraud" varies. For example, some policies cover "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 the Insured's proprietary Computer System. . ." *E.g., Universal Am. Corp. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa.*, 25 N.Y.3d 675, 679 (N.Y. Ct. App. 2015). Another policy may more broadly define "Computer Fraud" to mean "[t]he use of any computer to fraudulently cause a transfer of Money. . . 1. to a person. . . outside the Premises. . .," but may also contain a specific exclusion for Electronic Data input by "a natural person having the authority to enter the Insured's Computer System[.]" *Am. Tooling,* 2018 U.S. App. LEXIS 19208, 2018 WL 3404708, at *4, *6. Other policies separately provide coverage for "funds transfer fraud" with respect to "[l]oss resulting directly from a 'fraudulent instruction' directing a 'financial institution' to debit your 'transfer account' and transfer. . . 'money' . . . from that account[,]" where the "fraudulent instruction" must be issued by "someone else[,] *without [the policyholder's] knowledge or consent*." *Principle Solutions,* 2016 WL 4618761, at *2 (emphasis added).

5. *Universal Am. Corp.*, 25 N.Y.3d at 683; *Pestmaster*, 656 F. App'x at 333.

6. *Universal Am. Corp.*, 25 N.Y.3d at 679-80.

7. *Id.* at 680-81.

8. *Id.*

9. *Pestmaster*, 656 F. App'x at 333.

10. *Id.*

11. *Id.*

12. 681 F. App'x 627 (9th Cir. 2017).

13. *Id.* at 629.

14. *Id.*

15. 719 F. App'x 701 (9th Cir. 2018).

16. *Id.* at 702.

17. *Id.*

18. *Compare S. Cal. Counseling Ctr v. Great Am. Ins. Co.*, 667 F. App'x 623, 623 (9th Cir. 2016), where policy contained an exclusion for loss resulting from the dishonest acts of "authorized representatives." There, a payroll-services agent had misappropriated funds of the policyholder. The Court explained that the function of the exclusion is "to place the onus of vetting the individuals and entities whom the insured engages to stand in its shoes — and thus the risk of loss stemming from their conduct — squarely on the insured." *Id.* at 624.

19. *Am. Tooling,* 2018 U.S. App. LEXIS 19208, 2018 WL 3404708.

20. *Id.* at *4. *See also Owens , Schine & Nicola, P.C. v. Travelers Cas. & Sur. Co. of Am.*, No. CV-09-5024601-S, 2011 WL 3200296, at *9 (Conn. Super. Ct. June 24, 2011) (in spoofing case, policy was found to be "ambiguous as to the amount of computer usage necessary to constitute computer fraud"), *vacated*, 2012 WL 12246940 (Conn. Super. Ct. Apr. 18, 2012).

21. *Am. Tooling,* 2018 U.S. App. LEXIS 19208, 2018 WL 3404708, at *4.

22. *Id.*

23. *Id.* at *6.

24. *Id.* Specifically, the policy provided that "Electronic Data" includes "facts or information converted to a form: (1) usable in a Computer System; (2) that does not provide instructions or directions to a Computer System; or (3) that is stored on electronic processing media for use by a Computer Program." *Id.*

25. The Court here was interpreting the same type of policy exclusion at issue in *Aqua Star*, which the Ninth Circuit held unambiguously precluded coverage on analogous facts. *See Aqua Star*, 719 F. App'x at 702.

26. *Medidata I*, 2018 U.S. App. LEXIS 18376, 2018 U.S. App. LEXIS 18376, 2018 WL 3339245.

27. *Id.* at *1.

28. *See Medidata Solutions, Inc. v. Fed. Ins. Inc.*, 268 F. Supp. 3d 471, 477 (S.D.N.Y. 2017), *aff'd*, No. 17-2492-cv, 2018 U.S. App. LEXIS 18376, 2018 WL 3339245 (2d Cir. July 6, 2018). The policy defined

"Computer Fraud" as "the unlawful taking or the fraudulently induced transfer of Money, Securities or Property resulting from a Computer Violation." A "Computer Violation," in turn, "included: the *fraudulent*: (a) entry of Data into . . . a Computer System; [and] (b) change to Data elements or program logic of a Computer System, which is kept in machine readable format . . . directed against an Organization." *Id.* at 474. The Policy defined "Data" broadly to include any "representation of information." *Id.*

29. *Medidata I,* 2018 U.S. App. LEXIS 18376, 2018 WL 3339245, at *1.

30. *Id.*

31. *Id.* at *2. The lower court had explicitly rejected the argument that coverage under the policy was limited to computer hacking. *Medidata,* 268 F. Supp. 3d at 477-78.

32. *Medidata I,* 2018 U.S. App. LEXIS 18376, 2018 WL 3339245, at *2, *citing Universal*, 25 N.Y.3d at 681.

33. *Apache,* 662 F. App'x 252.

34. *Id.*, at 253-54.

35. *Id.*

36. *Id.* at 259.

37. *Id.*

38. No. 17-11712, 2018 WL 2149769 (11th Cir. May 10, 2018).

39. *Id.* at *2.

40. *Id.* at *4.

41. *Id.* at *5.

42. *Id.*

43. *Medidata I,* 2018 U.S. App. LEXIS 18376, 2018 WL 3339245, at *2.

44. *Am. Tooling,* 2018 U.S. App. LEXIS 19208, 2018 WL 3404708.

45. *Id.* at *2.

46. *Id.* at *1.

47. *Id.* at *3.

48. *Id.* at *5.

49. *Id.*

50. *Id.* In *State Bank of Bellingham v. BankInsure, Inc.,* 823 F.3d 456 (8th Cir. 2016), the Eighth Circuit, applying Minnesota law, held that a hacker's insertion of malware into a bank computer that enabled it to make unauthorized wire transfers was the proximate cause of the illegal transfer of money. There, the hacker was able to insert the malware when a bank employee left her computer running at the end of a work day. That Court held that the illegal wire transfer was not the foreseeable and natural consequence of the bank employee's failure to follow proper security protocols.

51. *Principle Solutions Grp., LLC v. Ironshore Indemn., Inc.*, No. 1:15-CV-4130-RWS, 2016 WL 4618761 (N.D.Ga. Aug. 30, 2016), *on appeal sub nom. PSG Parent, Inc. v. Ironshore Indem., Inc.*, No. 17-11703-FF (11th Cir. 2018).

52. *Id.* at *1.

53. *Id.*

54. *Id.* at *4. ■

MEALEY'S: EMERGING INSURANCE DISPUTES
edited by Jennifer Hans
The Report is produced twice monthly by

LexisNexis®

1600 John F. Kennedy Blvd., Suite 1655, Philadelphia, PA 19103, USA
Telephone: (215)564-1788 1-800-MEALEYS (1-800-632-5397)
Email: mealeyinfo@lexisnexis.com
Web site: http://www.lexisnexis.com/mealeys
ISSN 1087-139X