



1 of 5 DOCUMENTS

[**1] Universal American Corp., Appellant, v National Union Fire Insurance Company of Pittsburgh, PA., Respondent.

No. 95

COURT OF APPEALS OF NEW YORK

2015 N.Y. LEXIS 1434; 2015 NY Slip Op 05516

June 25, 2015, Decided

NOTICE:

THE LEXIS PAGINATION OF THIS DOCUMENT IS SUBJECT TO CHANGE PENDING RELEASE OF THE FINAL PUBLISHED VERSION. THIS OPINION IS UNCORRECTED AND SUBJECT TO REVISION BEFORE PUBLICATION IN THE OFFICIAL REPORTS.

PRIOR HISTORY: *Universal Am. Corp. v. National Union Fire Ins. Co. of Pittsburgh, PA.*, 110 A.D.3d 434, 972 N.Y.S.2d 241, 2013 N.Y. App. Div. LEXIS 6278 (N.Y. App. Div. 1st Dep't, 2013)

DISPOSITION: Order affirmed, with costs.

COUNSEL: [*1] Richard H. Dolan, for appellant.

Barbara A. Lukeman, for respondent.

United Policyholders, amicus curiae.

JUDGES: Opinion by Judge Rivera. Judges Read, Pigott, Abdus-Salaam, Stein and Fahey concur. Chief Judge Lippman took no part.

OPINION BY: RIVERA

OPINION

RIVERA, J.:

On this appeal we consider whether an insuring agreement for computer systems fraud that applies to "a fraudulent entry of Electronic Data or Computer Program" encompasses losses caused by an authorized user's submission of fraudulent information into the insured's

computer system. We conclude that the agreement is unambiguous and "fraudulent entry" refers [**2] to unauthorized access into plaintiff's computer system, and not to content submitted by authorized users. Therefore, we affirm the order of the Appellate Division.

Plaintiff, Universal American Corp. ("Universal"), is a health insurance company that offers, as relevant to this appeal, a choice of federal government-regulated alternatives to Medicare, known as "Medicare Advantage Private Fee-For-Service" plans ("Medicare Advantage")¹. These plans allow Medicare-eligible individuals to purchase health insurance from private insurance companies, and those companies are, in turn, eventually reimbursed [*2] by the U.S. Department of Health and Human Services's Centers for Medicare and Medicaid Services, for health care services provided to the plans' members. Universal has a computerized billing system that allows health care providers to submit claims directly to the system. According to Universal, the great majority of claims submitted are processed, approved, and paid automatically, without manual review.

1 Medicare, a hospital, medical, and prescription drug insurance program, is administered by the Centers for Medicare & Medicaid Services within the United States Department of Health and Human Services (*see* 42 USC § 1395 *et seq.*).

The matter before us involves Universal's demand for indemnification to cover losses resulting from health care claims for unprovided services, paid through Universal's computer system. At issue is the coverage available to Universal pursuant to rider #3 ("Rider") of a financial institution bond ("bond"), issued by defendant National Union Fire Insurance Company of Pittsburgh, PA ("National Union"). The bond insured Universal

against various losses, inclusive of certain losses resulting from dishonest and fraudulent acts. The Rider amended the bond to provide indemnification specifically [*3] for computer systems fraud, and states, in part

COMPUTER SYSTEMS

It is agreed that:

1. the attached bond is amended by adding an Insuring Agreement as follows:

COMPUTER SYSTEMS FRAUD

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

...

provided that the entry or change causes

(a) Property to be transferred, paid or delivered,

(b) an account of the insured, or of its customer, to be added, deleted, debited or credited, or

(c) an unauthorized account or a fictitious account to be debited or credited"

The Rider, and the basic bond coverage, carry a \$10 million limit and a \$250,000 deductible for each "single loss," which, as defined in the Rider, includes "the fraudulent acts of one individual," or of "unidentified individuals but arising from the same method of operation." Universal's annual premium during the relevant policy period was \$170,500.

A few months after obtaining coverage, Universal suffered over \$18 million in losses for payment of fraudulent claims for services never actually performed under its Medicare Advantage plans. When Universal [*4] sought payment from National Union for its post-deductible losses, National Union denied coverage on the ground that the Rider did not encompass losses for Medicare fraud, which National Union described as losses from payment for claims submitted by health care providers.

Universal then commenced an action for damages and declaratory relief against National Union. Thereafter, Universal moved pursuant to CPLR 3212 for partial summary judgment, and an order declaring the losses to be covered under the policy. National Union cross-moved for summary judgment. Supreme Court denied Universal's motion, granted National Union's motion, and dismissed the complaint (38 Misc 3d 859, 959

N.Y.S.2d 849 [Sup Ct 2013]), concluding that the Rider is not ambiguous and does not extend to fraudulent claims entered into Universal's system by authorized users. The court determined, instead, that the intended coverage is for an unauthorized entry into the computer system by a hacker or through a computer virus.

The Appellate Division unanimously modified the summary judgment order, on the law, to declare the policy does not cover the loss, and otherwise affirmed. The court concluded the unambiguous language of the policy does not cover fraudulent content entered [*5] by authorized users, but rather "wrongful acts in manipulation of the computer system, i.e., by hackers" (110 AD3d 434, 434, 972 N.Y.S.2d 241 [1st Dept 2013]). We granted Universal leave to appeal (23 NY3d 904, 990 N.Y.S.2d 161, 13 N.E.3d 661 [2014]), and now affirm.

An insurance agreement is subject to principles of contract interpretation. "As with the construction of contracts generally, 'unambiguous provisions of an insurance contract [*3] must be given their plain and ordinary meaning, and the interpretation of such provisions is a question of law for the court'" (*Vigilant Ins. Co. v Bear Stearns Companies, Inc.*, 10 NY3d 170, 177, 884 N.E.2d 1044, 855 N.Y.S.2d 45 [2008], quoting *White v Continental Cas. Co.*, 9 NY3d 264, 267, 878 N.E.2d 1019, 848 N.Y.S.2d 603 [2007]). "Ambiguity in a contract arises when the contract, read as a whole, fails to disclose its purpose and the parties' intent" (*Ellington v EMI Music, Inc.*, 24 NY3d 239, 244, 997 N.Y.S.2d 339, 21 N.E.3d 1000 [2014], citing *Brooke Group v JCH Syndicate* 488, 87 NY2d 530, 534, 663 N.E.2d 635, 640 N.Y.S.2d 479 [1996]), or where its terms are subject to more than one reasonable interpretation (see *Dean v Tower Ins. Co. of New York*, 19 NY3d 704, 708, 979 N.E.2d 1143, 955 N.Y.S.2d 817 [2012], quoting *Seaboard Sur. Co. v Gillette Co.*, 64 NY2d 304, 311, 476 N.E.2d 272, 486 N.Y.S.2d 873 [1984]; *Chimart Assoc. v Paul*, 66 NY2d 570, 573, 489 N.E.2d 231, 498 N.Y.S.2d 344 [1986] [ambiguity exists if "the agreement on its face is reasonably susceptible of more than one interpretation"]; see also *Greenfield v Philles Records*, 98 NY2d 562, 569-570, 780 N.E.2d 166, 750 N.Y.S.2d 565 [2002]). However, parties cannot create ambiguity from whole cloth where none exists, because provisions "are not ambiguous merely because the parties interpret them differently" (*Mount Vernon Fire Ins. Co. v Creative Hous. Ltd.*, 88 NY2d 347, 352, 668 N.E.2d 404, 645 N.Y.S.2d 433 [1996]). Rather, "[t]he test to determine whether an insurance contract is ambiguous focuses on the reasonable expectations of the average insured upon reading the policy, . . . and employing common speech" (*Mostow v State Farm Ins. Companies*, 88 NY2d 321, 326-27, 668 N.E.2d 392, 645 N.Y.S.2d 421 [1996] [internal [*6] citations omitted]; see also *Cragg v Allstate Indem.*

Corp., 17 NY3d 118, 122, 950 N.E.2d 500, 926 N.Y.S.2d 867 [2011] ["Insurance contracts must be interpreted according to common speech and consistent with the reasonable expectations of the average insured"]).

Turning to the language of the Rider, we conclude that it unambiguously applies to losses incurred from unauthorized access to Universal's computer system, and not to losses resulting from fraudulent content submitted to the computer system by authorized users. The term "fraudulent" is not defined in the Rider, but it refers to deceit and dishonesty (*see* Merriam Webster's Collegiate Dictionary [10th ed 1993]). While the Rider also does not define the terms "entry" and "change," the common definition of the former includes "the act of entering" or "the right or privilege of entering, access," and the latter means "to make different, alter" (*id.*). In the Rider, "fraudulent" modifies "entry" or "change" of electronic data or computer program, meaning it qualifies the act of entering or changing data or a computer program. Thus, the Rider covers 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. The [*7] Rider's reference to "fraudulent" does not also qualify what is actually acted upon, namely the "electronic data" or "computer program" itself. 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.

Other language in the Rider confirms that the Rider seeks to address unauthorized access. First, the Rider is captioned "Computer Systems," and the specific language at issue is found under the subtitle "Computer Systems Fraud." These headings clarify that the Rider's [*4] focus is on the computer system qua computer system. Second, under "EXCLUSIONS," the Rider exempts from 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." If the parties intended to cover fraudulent content, such as the billing fraud involved here, 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.

Nonetheless, Universal [*8] argues that in the context of the Rider, "fraudulent entry" means "fraudulent input" because a loss due to a fraudulent entry by necessity can only result from the input of fraudulent information. This would render superfluous the word "a" before "fraudulent," and the word "of" before "electronic data or computer program." Universal's proposed interpretation is easily achieved by providing coverage for a "loss resulting directly from fraudulent data." Of course,

that is not what the Rider says. Moreover, Universal's reading ignores the other language contained in the Rider and its categorical application to "Computer Systems" and "Computer Systems Fraud."

We are also unpersuaded by Universal's reliance on *Owens, Schine & Nicola, P.C. v Travelers Cas. and Sur. Co. of Am.* (2010 Conn. Super. LEXIS 2386, 2010 WL 4226958, at *1 [Conn Super Ct Sept. 20, 2010] judgment vacated, 2012 Conn. Super. LEXIS 5053, 2012 WL 12246940 [Conn Super Ct Apr. 18, 2012] [memorandum of decision vacated by stipulation of the parties]), in support of its argument that the heading "computer systems fraud" can reasonably be interpreted to encompass fraud committed through a computer, meaning fraud that is not limited to computer hacking incidents. The *Owens* decision is of little assistance to Universal's cause. In *Owens*, the policy provision was far broader, and contained an internally applicable definition of "Computer Fraud" as, "The [*9] use of any computer to fraudulently cause a transfer of Money, Securities or Other Property from inside the Premises or Banking Premises: 1. to a person (other than a Messenger) outside the Premises or Banking Premises; or 2. to a place outside the Premises or Banking Premises" (2010 Conn. Super. LEXIS 2386, [WL] at *4). The insurer argued that "computer fraud" within the meaning of the policy required manipulation of the computer system, i.e., hacking. It further argued that there was no actual computer fraud because the use of emails and a computer to create a fraudulent check, as part of a scheme to steal funds from the insured, did not cause the physical transfer of money out of the insured's account. Instead, the loss resulted from the insured's wiring of the funds out of the account. The court found the phrase "use of any computer" to be ambiguous as to "the amount of computer usage necessary to constitute computer fraud" (2010 Conn. Super. LEXIS 2386, [WL] at *7). Thus, *Owens* was concerned with whether the computer had been utilized sufficiently to constitute computer fraud as contemplated by the parties, based on their reasonable understanding of the policy's terms.

Here, it is undisputed that use of Universal's computer is absolutely essential to trigger [*10] coverage for a loss, and that its computers were indeed used in a manner that resulted in payment of claims for health care services that were never provided. Thus, unlike in *Owens*, the [*5] question is not how much computer use is required under the policy, but whether the use involved here is the type actually covered by the Rider.

We conclude that the "reasonable expectations of the average insured upon reading the policy" (*Mostow*, 88 NY2d at 326-27) are that the Rider applies to losses resulting directly from fraudulent access, not to losses from the content submitted by authorized users. Accordingly,

the order of the Appellate Division should be affirmed,
with costs.

* * * *

Order affirmed, with costs. Opinion by Judge Rivera. Judges Read, Pigott, Abdus-Salaam, Stein and Fahey concur. Chief Judge Lippman took no part.

Decided June 25, 2015