

UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

Wentworth-Douglas Hospital,
Plaintiff

v.

Civil No. 10-cv-120-SM
Opinion No. 2010 DNH 128

Young & Novis Professional
Association d/b/a Piscataqua
Pathology Associates; Cheryl
C. Moore, M.D. and Glenn H.
Littell, M.D.,
Defendants

O R D E R

Wentworth-Douglas Hospital brought suit against several physicians and their professional association under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (Counts I-III) and New Hampshire common law (Count IV). The hospital says that it declined to renew a contract with defendants to provide pathology services, whereupon defendants appropriated and erased important computer data belonging to the hospital. Before the court is defendants' motion to dismiss. Plaintiff objects. For the reasons given, defendants' motion is denied.

The Legal Standard

A motion to dismiss for "failure to state a claim upon which relief can be granted," FED. R. CIV. P. 12(b)(6), requires the court to conduct a limited inquiry, focusing not on "whether a

plaintiff will ultimately prevail but whether the claimant is entitled to offer evidence to support the claims." Scheuer v. Rhodes, 416 U.S. 232, 236 (1974). That is, the complaint "must contain 'enough facts to raise a reasonable expectation that discovery will reveal evidence' supporting the claims." Fantini v. Salem State Coll., 557 F.3d 22, 26 (1st Cir. 2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 556 (2007)). When considering a motion to dismiss under Rule 12(b)(6), a trial court "assume[s] the truth of all well-plead facts and give[s] the plaintiff[s] the benefit of all reasonable inferences therefrom." Vernet v. Serrano-Torres, 566 F.3d 254, 258 (1st Cir. 2009) (quoting Ruiz v. Bally Total Fitness Holding Corp., 496 F.3d 1, 5 (1st Cir. 2007)).

"To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." Sutcliffe v. Epping Sch. Dist., 584 F.3d 314, 325 (1st Cir. 2009) (quoting Ashcroft v. Iqbal, 129 S. Ct. 1937, 1949 (2009)). On the other hand, a Rule 12(b)(6) motion should be granted if "the facts, evaluated in [a] plaintiff-friendly manner, [do not] contain enough meat to support a reasonable expectation that an actionable claim may exist." Andrew Robinson Int'l, Inc. v. Hartford Fire Ins. Co., 547 F.3d 48, 51 (1st Cir. 2008) (citations omitted).

Background

For over eighteen years, Young & Novis Professional Association ("Young & Novis"), doing business as Piscataqua Pathology Associates, provided pathology services to Wentworth-Douglas Hospital under a series of contracts. At all times relevant to this complaint, defendants Cheryl Moore, M.D., and Glenn Littell, M.D., were owners and employees of Young & Novis, Dr. Moore served as Medical Director of the Wentworth-Douglas Laboratory, which included the Pathology Department, and Dr. Littell was a member of the Wentworth-Douglas medical staff.

In late 2009, Wentworth-Douglas informed Drs. Moore and Littell that the hospital's agreement with Young & Novis, scheduled to expire on February 28, 2010, would not be renewed. Between February 1 and February 28, Drs. Moore and Littell downloaded electronic data from the Wentworth-Douglas computer network, using two desktop computers and one laptop computer in the Pathology Department, and removable storage devices. Those data included "specimen/slide photos; autopsy images; charts with patient specific information; College of American Pathologist Reviews; Quality Assurance information; documents, templates, forms and folders utilized by employees of the pathology department to process specimens; individual employee subfolders; and records related to complaints against Dr. Moore and Dr.

Littell." (Compl. ¶ 56.) On February 28, Drs. Moore and Littell installed software called "DriveScrubber 3" on all three Pathology Department computers. That software deleted data from the hard drives of those computers (the C Drives), and also deleted data from the H Drive, the K Drive, and the P Drive used by the Wentworth-Douglas computer network.¹ Wentworth-Douglas's written policy on security and confidentiality of information, described in a document titled "IM-09," expressly prohibits the attachment of external hardware to, the installation of software on, and the deletion of files from the computer systems.

On February 28, approximately twenty minutes after Dr. Littell's last access to the hospital system's K Drive, a Wentworth-Douglas employee attempted to access the K Drive, but was unable to do so. The pathologists who succeeded Young & Novis had no access to information stored on the K Drive for approximately one week. After losing access to the K Drive, and discovering a DriveScrubber 3 CD in the CD tray of the Pathology Department laptop, Wentworth-Douglas engaged the services of a forensic expert to conduct a damage assessment and restore its computer system.

¹ The H Drive consists of user-specific network drives. The K Drive is the pathology network shared drive. The P Drive is the "PowerPath network shared drive," which is the system used for the tracking and reporting of pathology specimens.

Based upon the foregoing factual allegations, the hospital claims that defendants violated 18 U.S.C. § 1030(a)(2)(C) (Count I), § 1030(a)(5)(A) (Count II), and § 1030(b) (Count III), and that defendants are liable for common law conversion (Count IV).

Discussion

Defendants move to dismiss the federal claims (Counts I-III) for failure to state a cause of action, and ask the court to decline to exercise supplemental jurisdiction over the state conversion claim (Count IV).

A. Count I

The Computer Fraud and Abuse Act provides a private right of action for compensatory damages and equitable relief to any person who suffers damage or loss because another "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). "[T]he term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). Plaintiff's theory is that by connecting removable storage devices to three Wentworth-Douglas computers and downloading data to those devices, defendants

obtained information from those computers in a manner that exceeded their authorized access, because the hospital's IM-09 policy prohibited them from connecting external hardware to Wentworth-Douglas computers.

Defendants argue that Count I should be dismissed because the hospital has not alleged any conduct on their part that is proscribed by 18 U.S.C. § 1030(a)(2)(C). Specifically, defendants contend that the complaint does not allege that they were not authorized to access Wentworth-Douglas's computers and fails to allege, with adequate particularity, that they accessed the hospital's computers in a way that exceeded their authorization to do so. The crux of defendants' argument is that while Wentworth-Douglas alleges that their rights of access to the hospital's computers were governed by the IM-09 policy, the version of IM-09 attached to the complaint is outdated,² and that, in any event, their rights of access were governed by their contractual agreement with Wentworth-Douglas, not by the hospital's IM-09 policy.

² The hospital acknowledges that the version of the IM-09 policy attached to its complaint was superseded by a new version in January of 2010, but points out, accurately, that the specific provisions on which it relied in its complaint were carried over, intact, into the new version.

Defendants' argument addresses matters beyond the scope of a motion to dismiss, the purpose of which is simply to test the legal sufficiency of the complaint. See Scheuer, 416 U.S. at 236. Here, Wentworth-Douglas has alleged that defendants were subject to a hospital-wide policy that limited their access to hospital computer systems by proscribing certain acts, that defendants committed one of those proscribed acts, i.e., connecting external hardware to hospital computers, and that by committing the proscribed act, defendants obtained information to which they were not entitled. Defendants are of course free to argue, in a motion for summary judgment, for example, that they were not subject to the IM-09 policy. But, taking the well-pleaded allegations of the complaint as true, as the court must at this point, the hospital has stated a cognizable legal claim upon which relief can be granted under 18 U.S.C. § 1030(a)(2)(C).

B. Count II

The Computer Fraud and Abuse Act provides a private right of action for compensatory damages and equitable relief to any person who suffers damage or loss because another "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer." 18 U.S.C. § 1030(a)(5)(A). The hospital says that defendants

damaged three Wentworth-Douglas computers, and the hospital's computer network, by installing DriveScrubber 3 software and/or issuing commands that deleted information from the C Drives of those three computers as well as the H, K, and P Drives of the hospital's computer network.

Defendants argue that Count II should be dismissed because the hospital has not alleged that they accessed a protected computer without authorization. Defendants incorrectly suggest that a person who has authorization to access a computer cannot violate 18 U.S.C. § 1030(a)(5)(A).

To begin, the cases on which defendants rely for the proposition that unauthorized access is an element of a claim under § 1030(a)(5)(A) were both decided under an earlier version of the statute that, unlike the current version, did include a requirement of unauthorized access. See United States v. Morris, 928 F.2d 504, 506 (2d Cir. 1991); United States v. Sablan, 92 F.3d 865, 867 (9th Cir. 1996). The current version of the statute has no such requirement: "[T]o successfully plead a civil violation under the [Computer Fraud and Abuse Act], the plaintiff must allege facts that could establish three elements: 1) the knowing 'transmission' of a 'program, information, code, or command;' 2) the transmission is 'to a protected computer;' and

3) the transmission causes intentional 'damage without authorization.' " Hayes v. Packard Bell, NEC, Inc., 193 F. Supp. 2d 910, 912 (E.D. Tex. 2001) (quoting 18 U.S.C. § 1030(a)(5)(A)); see also Thurmond v. Compaq Computer Corp., 171 F. Supp. 2d 667, 675 (E.D. Tex. 2001) (same); Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 174 F. Supp. 2d 890, 898 (N.D. Iowa 2001) ("the elements of a civil claim under [§ 1030(a)(5)(A)] are as follows: (1) the person or entity must intentionally cause the transmission of a program, information, code, or command; (2) the computer must be a 'protected computer;' (3) the transmission must be without authorization; and (4) the transmission must cause damage."). Unauthorized damage and/or unauthorized transmission are elements of a cause of action under § 1030(a)(5)(A); unauthorized access to the protected computer is not.

In Lloyd v. United States, the district court rejected an argument by a habeas corpus petitioner, convicted under the criminal provisions of § 1030, who contended that his counsel was ineffective for failing to argue "that because he was authorized as an employee to access the computer, the government did not prove that the transmission was 'without authorization,' as required under § 1030." Lloyd, No. Civ.03-813(WHW), 2005 WL 2009890, at *8 (D.N.J. Aug. 16, 2005). As the court explained:

"Contrary to Petitioner's contention, the term 'without authorization' modifies the element of intentionally causing damage to a computer. To read the statute as Petitioner does requires twisting the statutory language and violates common sense." Id. The reasoning of Lloyd applies here with equal force.

In sum, that the hospital did not allege that defendants lacked authorization to access the Pathology Department computers does not warrant dismissal of Count II. The hospital adequately alleged that defendants knowingly transmitted a program or commands to the Wentworth-Douglas computer system that caused unauthorized damage, in the form of erasure of files. That is enough to state a claim under § 1030(a)(5)(A).

C. Damages Threshold

Defendants also argue that the court lacks subject matter jurisdiction because Wentworth-Douglas has not alleged a loss of at least \$5,000. Under 18 U.S.C. § 1030(g), a civil action under the Computer Fraud and Abuse Act "may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)." Those factors include: "(I) loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value; [and] (II) the

modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals." 18 U.S.C. § 1030(c)(4)(a)(i).

The statute further provides that

the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of the interruption of service.

18 U.S.C. § 1030(e)(11).

In Counts I, II, and III, the hospital alleges that it suffered damage or loss of at least \$5,000. Defendants argue that the complaint's allegations of loss are too conclusory, and that much or all of what the hospital claims as losses are actually costs of litigation that do not count toward the aggregate loss envisioned by the statute. See Wilson v. Moreau, 440 F. Supp. 2d 81, 110 (D.R.I. 2006) (holding "that, as a matter of law, the costs of litigation cannot be counted towards the \$5,000 statutory threshold").

The hospital has adequately alleged conduct involving the factors identified in 18 U.S.C. §§ 1030(c)(4)(A)(i)(I) and (II). It alleged that the Pathology Department was without access to

the K Drive for approximately one week. That is sufficient to establish a claim for "modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals," 18 U.S.C. § 1030(c)(4)(A)(i)(**II**), resulting from the conduct alleged in Counts II and III. Relevant to all three counts, the hospital has also alleged that it had to retain a forensic expert to conduct a damage assessment and restore its computer system. Given the computer system described, the aggregate loss of at least \$5,000 required by 18 U.S.C. § 1030(c)(4)(A)(i)(**I**) has been adequately pled. Defendants, of course, are free to conduct discovery regarding the claimed losses, and to move for summary judgment should the hospital be unable to produce evidence sufficient to establish that element of its claim. But, at this stage of the litigation, the hospital has adequately alleged an aggregate loss of at least \$5,000.

D. Count III

In Count III, brought under 18 U.S.C. § 1030(b), the hospital charges defendants with conspiring to commit an offense under § 1030(a). Defendants argue that Count III should be dismissed because the hospital has not stated claims under §§ 1030(a)(2)(C) and 1030(a)(5)(A). But, as plaintiff is entitled to proceed on Counts I and II (and because conspiratorial success

is not a prerequisite to a claim for conspiracy), defendants' motion to dismiss Count III is necessarily denied.

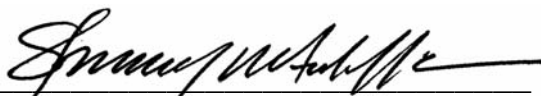
E. Count IV

Defendants ask the court to decline to exercise supplemental jurisdiction over the common law claim for conversion (Count IV), but the federal claims have not been dismissed, so it is appropriate to continue to exercise supplemental jurisdiction over the state claim.

Conclusion

For the reasons given, defendants' motion to dismiss (document no. 16) is denied.

SO ORDERED.



Steven J. McAuliffe
Chief Judge

July 28, 2010

cc: William E. Christie, Esq.
Charles W. Grau, Esq.