

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

**JEFF DEVINE and DEVINE SOLUTIONS,
INC., an Illinois corporation,**)
)
)
Plaintiffs,)

v.)

**SABIR KAPASI, HUSENI KAPASI, GREG
CARLO, and MANAGESERVE
TECHNOLOGY, INC., an Illinois
Corporation,**)
)
)
Defendants.)

No. 09 C 6164

HONORABLE DAVID H. COAR

MEMORANDUM OPINION AND ORDER

Plaintiffs Jeff Devine and his company, Devine Solutions, Inc., have filed suit under the Stored Communications Act, 18 U.S.C. § 2701, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and Illinois law, alleging that the defendants electronically trespassed upon the Devine Solutions computer network and tampered with electronic communications and other data stored there. The defendants have moved to dismiss the complaint for failure to state a claim. *See* Fed. R. Civ. P. 12(b)(6). For the reasons given below, the motion to dismiss is GRANTED in part and DENIED in part. Counts III-IV of the complaint are dismissed without prejudice.

FACTS

The relevant facts alleged in the complaint, which the court must take as true for present purposes, are as follows:

Prior to August 21, 2009, Jeff Devine and Sabir Kapasi each owned fifty percent of the common stock of a computer-services company called Geus Technology, Inc. Geus provided programming, configuration, and other technical support for clients who used a popular software

application (created by a German software company, not by Geus) known as SAP. Geus's unique support model allowed it to manage and maintain its clients' SAP applications remotely, as well as on-site at its clients' locations throughout North America. Huseni Kapasi and Greg Carlo were employees of Geus.

On August 21, 2009, after several months of contentious and protracted negotiations, Geus (through Sabir Kapasi), Sabir Kapasi, and Devine executed a stock-redemption agreement, pursuant to which Geus redeemed Devine's fifty-percent ownership stake in the company. The parties agreed to an equitable division of Geus's assets, and as memorialized in Schedule 1.2 of their agreement, some of those assets were assigned and transferred to Devine. Among those assets was a server identified as "Server DL380-GEUS05" (the "GEUS05 Server"), which had been a component of Geus's computer network. Following the close of the stock redemption, Devine incorporated the GEUS05 Server into the network owned and operated by Devine Solutions, which comprises computers, servers, and remote access equipment secured by password-protected accounts.

As part of their ownership and/or employment with Geus, Defendants Sabir Kapasi, Huseni Kapasi, and Carlo utilized confidential passwords to access the Geus computer network, including the GEUS05 Server. Until the Geus-issued passwords were terminated, Defendants could access the Devine Solutions network through the GEUS05 Server. Within a couple of hours after the closing of the stock-redemption transaction, and continuing for several days, Defendants systematically and without authorization accessed the Devine Solutions network, including the GEUS05 Server, and further accessed, transferred and deleted electronic information and files stored on the GEUS05 Server. At 9:40 p.m. on Friday, August 21, 2009 (a few hours after the closing of the stock redemption), Carlo remotely accessed the GEUS05

Server from an unknown computer (with the assigned IPA 10.203.86.152) using the “gcarlo” account and password issued by Geus. Carlo’s access was captured by a secure log maintained on the GEUS05 Server. Through the GEUS05 Server, Carlo logged into the Devine Solutions network’s document- tracking system, known as the Owl Document Management System, which also logs access and user activity. On Saturday, August 22, 2009, according to the Owl log, Sabir Kapasi used the Geus-issued “sabirk” account and password and an unknown computer (with the assigned IPA 10.203.86.156) to log into the Devine Solutions network through the GEUS05 Server and access the Owl document system. Lastly, the Owl log indicates that on August 25, 2009, Huseni Kapasi used the Geus-issued “hkapasi” account and password and an unknown computer (with the assigned IPA 10.203.86.155) to remotely access the Devine Solutions network through the GEUS05 Server; however, he was denied access to Owl.

The Owl log shows that a substantial volume of electronic information and files were deleted from the Devine Solutions network after the closing of the stock-redemption transaction. Plaintiffs’ investigation has revealed that, to date, more than 2000 files and 350 file folders containing electronically stored information and communications were deleted or otherwise transferred from the Devine Solutions network—but not by Devine or anyone working under his direction.

LEGAL STANDARD

To survive a motion to dismiss pursuant to Fed. R. Civ. P. 12(b)(6), a complaint need only contain a “short and plain statement of the claim showing that the pleader is entitled to relief,” Fed. R. Civ. P. 8(a)(2), that is, “a claim to relief that is plausible on its face.” *Bell Atlantic v. Twombly*, 550 U.S. 544, 570 (2007); *see also Ashcroft v. Iqbal*, 129 S. Ct. 1937 (2009) (*Twombly* applies to “all civil actions”). This requirement imposes two relatively low

hurdles. *First*, a complaint “must describe the claim in sufficient detail to give the defendant ‘fair notice of what the claim is and the grounds upon which it rests.’” *EEOC v. Concentra Health Servs.*, 496 F.3d 773, 776 (7th Cir. 2007) (quoting *Twombly*, 127 S. Ct. at 1964). *Second*, the allegations “must plausibly suggest that the defendant has a right to relief, raising that possibility above a ‘speculative level.’” *Concentra*, 496 F.3d at 776. If the allegations do not suggest a right to relief—if for instance, a plaintiff relies merely on conclusions, labels, or formulaic recitations of the elements of a cause of action—a Rule 12(b)(6) motion should be granted. *See Twombly*, 550 U.S. at 570.

ANALYSIS

Counts I-II: Electronic Communications Privacy Act

In Counts I-II, Plaintiffs assert a cause of action under Title II of the Electronic Communications Privacy Act, also known as the Stored Communications Act (“SCA”). *See* 18 U.S.C. §§ 2701-2712. Congress enacted the relevant provision of the SCA, *id.* § 2701, to protect privacy interests in personal and proprietary information from the mounting threat of computer hackers “deliberately gaining access to, and sometimes tampering with, electronic or wire communications” by means of electronic trespass. *See* S. Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, at 3557. Accordingly, any “aggrieved” party may bring a civil action against a defendant who “intentionally accesses without authorization” or “intentionally exceeds an authorizations to access” a “facility through which an electronic communication service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.” 18 U.S.C. § 2701(a)(1)-(2); *see* § 2707(a) (providing private right of action). An “electronic communication service” is “any service which provides to users thereof the ability to send or

receive wire or electronic communications,” i.e., electronic signals that affect interstate commerce. *Id.* § 2510(15), (12); *see* § 2711 (applying definitions in § 2510 to SCA).

The complaint alleges that Defendants “accessed, obtained, altered, transferred, and deleted Plaintiffs’ stored electronic information and communications” by gaining unauthorized access to the Devine Solutions network using Geus-issued user accounts and passwords. The complaint further alleges that the Devine Solutions network provides authorized users with the ability to transmit and receive electronic communications by on-site or remote access, through password protected accounts—including, as the defendants acknowledge, the ability to send and receive e-mail. Nevertheless, Defendants contend that Plaintiffs do not and cannot adequately plead that they provide an electronic communication service within the meaning of the SCA. This conclusion, Defendants say, follows from the facts that Plaintiffs (1) “merely provides [*sic*] technological support for customers using the SAP software; as opposed to (2) “independently” providing internet services to their customers; and (3) must purchase their own internet access just like any other consumer. In effect, Defendants argue that § 2701 does not apply because Plaintiffs are not in the business of providing an electronic communication service to the public. But that is not what § 2701 requires.

To see why, it is instructive to consider Defendants’ misplaced reliance on *Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041 (N.D. Ill. 1998) (Bucklo, J.). UOP, a chemical company, hired Andersen to perform a systems-integration project and, to that end, gave Andersen’s employees access to its internal e-mail system. *Id.* at 1042. During the course of the suit and countersuit that followed the collapse of this arrangement, UOP divulged (to the *Wall Street Journal*) the contents of e-mails that Andersen employees had sent through UOP’s system. *Id.* Andersen brought a subsequent suit, claiming that UOP violated § 2702 of the SCA, which

provides that “a person or entity providing an electronic communication service *to the public* shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.” 18 U.S.C. § 2702(a)(1) (emphases added). The court dismissed Andersen’s complaint on the grounds that UOP did not “provide[] an electronic communication service to the public” or, what comes to that same, that UOP was not “in the business of providing electronic communication services.” *Andersen Consulting*, 991 F. Supp. at 1043.

In their to-and-fro about *Andersen Consulting*, the parties completely lose sight of the language of § 2702 and its departure from the language of § 2701. Defendants attempt to wring from *Andersen Consulting* the purported holding that providing an electronic communication service *to the public* is a necessary condition of providing an electronic communication service *tout court*. Plaintiffs respond that *Andersen Consulting* is inapposite because § 2702 redresses the wrongful disclosure of electronic communications whereas § 2701 redresses wrongful access—inviting Defendants to wonder in their reply why ‘electronic communication service’ should mean different things in these two contexts. Of course it does not; the point, however, is that the court was not merely interpreting the phrase ‘electronic communication service’ when it found that UOP did not provide one to the public. Rather, it was addressing the elements of the applicable statute: § 2702 applies, by its terms, to persons and entities “providing an electronic communication service to the public.” In contrast, § 2701 applies where someone has gained unauthorized access to “a facility through which an electronic communication service is provided.” § 2701 simply does not say “to the public,” and *Andersen Consulting*—tethered as it is to the statutory elements of § 2702—provides no support for the proposition that a plaintiff

that does not provide an electronic communications service to the public fails to state a claim under § 2701.¹

To date, no court of appeals has held that § 2701 applies only where the plaintiff is “in the business” of providing an electronic communication service “to the public.” Indeed, the only court of appeals to face the question, albeit obliquely, has concluded otherwise. *See Fraser v. Nationwide Mutual Ins. Co.*, 352 F.3d 107, 115 (3d Cir. 2003) (holding that § 2701(c)(1)’s exception for electronic communications accessed with authorization from “the person or entity providing a wire or electronic communication service” applied to insurance company sued by former employee for its allegedly unauthorized access to his e-mail account). To be sure, there is some disagreement within and between the district courts as to whether § 2701 can apply to a private employer that is not “in the business” of providing an electronic communication service “to the public.”² In any event, this court concludes that it can: imposing a to-the-public requirement on § 2701 sloughs over a pointed difference between adjacent statutory provisions and renders the qualification added to § 2702 at best otiose, at worst utterly opaque. Where, as here, a plaintiff pleads that it stores electronic communications on its own systems, and that a defendant intentionally and without authorization got hold of those stored communications through the plaintiff’s electronic facilities, the plaintiff states a claim under § 2701 of the SCA.

¹ Defendants’ formulations notwithstanding, § 2701 does not require a plaintiff to be an electronic service provider; it requires that a plaintiff’s computers or workplace be a “facility through which an electronic communication service is provided.” *See Expert Janitorial, LLC v. Williams*, 2010 U.S. Dist. LEXIS 23080, at *13-14 (E.D. Tenn. March 12, 2010); *In re Intuit Privacy Litigation*, 138 F. Supp. 2d 1272, 1275 n.3 (C.D. Cal. 2001).

² *Compare, e.g., Expert Janitorial*, 2010 U.S. Dist. LEXIS 23080, at *14 (under § 2701, janitorial-services company may sue employee for unauthorized access to e-mails and other data stored on employer’s password-protected system) and *Cedar Hill Assocs., Inc. v. Paget*, 2005 U.S. Dist. LEXIS 32533, at *7-8 (N.D. Ill. Dec. 9, 2005) (Anderson, J.) (under § 2701, wealth-management company may sue employee for unauthorized access to employer-provided e-mail accounts) with *Steinbach v. Village of Forest Park*, 2009 U.S. Dist. LEXIS 59907, at *6 (N.D. Ill. July 14, 2009) (Zagel, J.) (in dicta, defendant municipality that gave plaintiff e-mail account but had to purchase internet access from third party did not provide electronic communication service for purposes of § 2701) and *In re Jet Blue Airways Corp. Privacy Litigation*, 379 F. Supp. 2d 299, 307-08 (E.D.N.Y. 2005) (defendant airline’s website was not an electronic communication service because defendant was not in the business of providing internet access).

See, e.g., Expert Janitorial, 2010 U.S. Dist. LEXIS 23080, at *14 (substantially similar allegations sufficed at motion-to-dismiss stage). Since Defendants raise no other challenges to the legal sufficiency of Counts I-II, there is no basis for dismissing them.

Counts III-IV: Computer Fraud and Abuse Act

In Counts III-IV, Plaintiffs assert a cause of action under the Computer Fraud and Abuse Act (“CFAA”), which punishes the conduct of anyone who, as relevant here: “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); or “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,” *id.* § 1030(a)(5)(A); or “intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage,” *id.* § 1030(a)(5)(B); or “intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss,” *id.* § 1030(a)(5)(C). The CFAA provides a private right of action, but only where the defendant’s alleged conduct “involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i).” *Id.* § 1030(g). There is no dispute between the parties that only one of these five subclauses is even colorably implicated by the allegations in the complaint, namely, that Defendants’ conduct must have “caused . . . loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value.” *Id.* § 1030(c)(4)(A)(i)(I). Defendants contend, however, that Plaintiffs do not and cannot allege loss that meets the statutory threshold.

The complaint alleges merely that Defendants “caused damage” by wrongfully accessing the GEUS05 Server and transmitting commands that resulted in the loss of data, but it nowhere alleges that Defendants’ alleged actions caused Plaintiffs to suffer at least \$5,000 in damages

during a 1-year period. Since the statute is clear that less than \$5,000 in damages will not suffice, Plaintiffs have failed to adequately plead a cause of action under the CFAA. *See Hayes v. Packard Bell NEC, Inc.*, 193 F. Supp. 2d 910, 912 (E.D. Tex. 2001) (dismissing claim under 18 U.S.C. § 1030 where plaintiff failed to allege at least \$5,000 in losses).

What's more, Defendants say, Plaintiffs could not possibly have sustained at least \$5,000 in losses as a result of the actions alleged in the complaint. That is because the CFAA limits compensable losses to "reasonable cost[s] to any victim . . ." *Id.* § 1030(e)(11). Since Devine Solutions was a technology company, Defendants reason, it would have an information back-up system to ensure that the costs associated with any data loss remained minimal—indeed, it would not be acting reasonably if it did not. Thus, \$5,000 could not be a "reasonable cost."

Defendants' conclusion is premature. As it stands, the complaint is silent about the scope of Plaintiffs' losses, leaving the court with no way to gauge, at least at this juncture, whether Plaintiffs could properly allege the statutory-minimum loss. Compensable losses or "reasonable cost[s]" under the CFAA include "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 damage incurred because of interruption of service." *Id.* To conclude that Plaintiffs cannot properly allege at least \$5,000 in losses, the court would have to speculate, for instance, about the possible extent of any revenue lost as a result of Defendants' alleged actions. A far better alternative is for Plaintiffs to amend their complaint, if they so choose, and attempt to cure the defects in their allegations of loss under the CFAA. Accordingly, they are granted leave to do so. Counts III-IV of the complaint are dismissed without prejudice.

Counts V-IX: State-Law Claims

In Counts V-IX, Plaintiffs assert various causes of action under Illinois law. Defendants argue that since Plaintiffs have failed to state any claim under federal law, this court lacks supplemental jurisdiction over the remaining state-law claims. But Plaintiffs have, at a minimum, stated a claim under 18 U.S.C. § 2701. Therefore, this court has supplemental jurisdiction over Plaintiffs' state-law claims. *See* 28 U.S.C. § 1367(a).

CONCLUSION

For the foregoing reasons, Defendants' motion to dismiss for failure to state a claim is GRANTED in part and DENIED in part. Counts III-IV of the complaint are dismissed without prejudice.

Enter:

/s/ David H. Coar

David H. Coar

United States District Judge

Dated: May 7, 2010