UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

EXETER TOWNSHIP, Plaintiff,	:	
v.	:	No. 5:18-cv-01723
ERIC GARDECKI, Defendant.	:	

O P I N I O N

Defendant's Motion to Dismiss for Failure to State a Claim, ECF No. 10—Granted

Joseph F. Leeson, Jr. **July 10, 2019**
United States District Judge

I. INTRODUCTION

Plaintiff Exeter Township has brought this action against its former IT administrator, Defendant Eric Gardecki. In its amended complaint, the Township asserts three claims: violation of the federal Stored Communications Act, violation of the Pennsylvania Stored Communications Act, and breach of fiduciary duty. Gardecki moves to dismiss the amended complaint for failing to state a claim upon which relief may be granted under Federal Rule of Civil Procedure 12(b)(6). For the reasons set forth below, the motion to dismiss is granted.

II. BACKGROUND[1]

Plaintiff Exeter Township filed its original complaint in April 2018 asserting claims for violations of the federal Stored Communications Act (SCA), 18 U.S.C. §§ 2701–2712, and the

[1] The background information in this section is taken from the amended complaint and is set forth as if true solely for purpose of analyzing the pending motion to dismiss. *See Phillips v. Cnty. of Allegheny*, 515 F.3d 224, 228 (3d Cir. 2008).

Pennsylvania Stored Communications Act, 18 Pa. Cons. Stat. §§ 5741–5749, trespass to chattels, conversion, and breach of fiduciary duty. Defendant Eric Gardecki moved to dismiss in June 2018 and the Court granted Gardecki's motion to dismiss on December 14, 2018, but granted the Township leave to amend three counts.

The Township filed its amended complaint on January 4, 2019. It includes three counts: (1) a claim for a violation of the Federal Stored Communications Act (Count I); (2) a claim for a violation of the Pennsylvania Stored Communications Act (Count II); and (3) a claim for a breach of fiduciary duty (Count III). Gardecki moves to dismiss the amended complaint in its entirety under Federal Rule of Civil Procedure 12(b)(6).

The Court discussed the factual background of this case previously. *See Exeter Twp. v. Gardecki*, No. 5:18-cv-01723, 2018 U.S. Dist. LEXIS 212275 (E.D. Pa. Dec. 14, 2018).[2] In its amended complaint the Township added several additional allegations clarifying the facts of the case. The Court will detail only the relevant portions of the additional factual pleadings.

The Township employed Gardecki in the position of Township Information Technology (IT) Administrator. In his position as IT Administrator, Gardecki's duties included providing general computer support services to Township employees. As a Township employee, he was only authorized to act in the Township's best interest and was not authorized to take actions that would jeopardize the safety, security, or both, of the Township and its property. Gardecki was not authorized to make or retain copies of Township's electronic data for his own personal purposes and without the express consent of the Township. He was not authorized to access the Township's cloud-based server for the purpose of creating a copy of the server.

---

[2] Opinion, ECF No. 7.

On April 12, 2016, however, Gardecki accessed the server and created a copy of it onto a hard drive. The server contained Township's highly sensitive and confidential information as well as Township's electronic data such as email messages. After his termination, Gardecki retained the copy of the server and stole two additional hard drives that contained Township's confidential information. He stored them at his home in an unsecured location for over twenty months. Gardecki allegedly did so for his own personal benefit and to assist the Township's former zoning officer who had informed Gardecki about her intent to act as a whistleblower against the Township.

As a result of Gardecki's unauthorized actions, the Township incurred more than $10,000 in damages because it was forced to retain a forensic computer expert to determine if Gardecki had deleted, destroyed, or altered the Township's electronic data stored on the server.

Now, Gardecki moves to dismiss a second time.

III. LEGAL STANDARDS

Federal Rule of Civil Procedure 12(b)(6) allows a court to dismiss a complaint for its "failure to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). The Rules generally demand "only a short and plain statement of the claim showing that the pleader is entitled to relief, in order to give the defendant fair notice of what the claim is and the grounds upon which it rests." *Connelly v. Lane Constr. Corp.*, 809 F.3d 780, 786 (3d Cir. 2016) (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (internal quotations omitted)).

"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.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 570). In rendering a decision on a motion to dismiss, this Court must "accept all factual allegations as true [and] construe the complaint in the

light most favorable to the plaintiff." *Phillips*, 515 F.3d at 233 (quoting *Pinker v. Roche Holdings Ltd.*, 292 F.3d 361, 374 n.7 (3d Cir. 2002) (internal quotations omitted)). Only if "the '[f]actual allegations . . . raise a right to relief above the speculative level'" has the plaintiff stated a plausible claim. *Id.* at 234 (quoting *Twombly*, 550 U.S. at 555). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678. However, "the tenet that a court must accept as true all of the allegations contained in a complaint is inapplicable to legal conclusions." *Id.* (explaining that determining "whether a complaint states a plausible claim for relief . . . [is] a context-specific task that requires the reviewing court to draw on its judicial experience and common sense"). The defendant bears the burden of demonstrating that a plaintiff has failed to state a claim upon which relief can be granted. *Hedges v. United States*, 404 F.3d 744, 750 (3d Cir. 2005) (citing *Kehr Packages, Inc. v. Fidelcor, Inc.*, 926 F.2d 1406, 1409 (3d Cir. 1991)).

IV. ANALYSIS

As referenced above, the Township asserts three claims against Gardecki. In Counts I and II of the amended complaint, the Township alleges that Gardecki violated the SCA and the Pennsylvania Stored Communications Act when he accessed the Township's cloud-based server to create the hard drive. In Count III, the Township asserts a claim of breach of fiduciary duty, alleging that Gardecki breached his duties to the Township as an employee when he intentionally failed to act in good faith and solely for the benefit of the Township.

Gardecki moves to dismiss the amended complaint for failing to state a claim. As discussed below, the Court will grant the motion to dismiss because the Township's amended complaint fails to state a claim under the SCA. The Court will dismiss this claim with prejudice

and dismiss the remaining state law claims without prejudice to be refiled in the proper state court. The analysis below focuses on the Township's failure to state a claim under the SCA.

A. The Township's claim under the federal Stored Communications Act[3]

In order to state a claim under the SCA, a plaintiff must allege that the defendant: (1) intentionally accessed without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeded an authorization to access that facility; and thereby obtained, altered, or prevented authorized access to a wire or electronic communication while it is in electronic storage in such system. 18 U.S.C. § 2701(a).

Gardecki makes four arguments in his brief that the Township fails to state a claim under the SCA: (1) the Township fails to allege facts that Gardecki accessed the Township's cloud-based server and the stored information contained on the server without authorization or by exceeding his authorization; (2) the information he accessed is not protected under the SCA; (3) the Township is not an electronic service provider and is not protected under the SCA; (4) the harm is not causally related to the alleged wrongdoing. *See* Mot. Dismiss Am. Compl., ECF No. 10. The Court's analysis below focuses only on Gardecki's first argument concerning his authority to access the server because the issue is dispositive.

---

[3] The previous opinion combined analysis for claims under the federal Stored Communications Act and Pennsylvania Stored Communications Act. The Court dismissed those claims on the same grounds that the complaint did not discuss Gardecki's authorization to access Township's server and the Court could not accept as true the conclusory assertions that Gardecki accessed the server without authorization or in excess of his authorization. Here, however, the Court's analysis of the SCA claim only refers to the federal Stored Communications Act claim, over which the Court has original jurisdiction. Having dismissed the only federal claim, the Court refrains from exercising supplemental jurisdiction over pendent state law claims, including the Pennsylvania Stored Communications Act claim.

In its response, the Township argues that it sufficiently alleges this element because its amended complaint includes allegations that Gardecki was only authorized to act in its best interests and that he was unauthorized to take actions that would jeopardize the safety, security, or both, of the Township and its property. Resp. to Mot. Dismiss Am. Compl. 9-10, ECF No. 12. The Township argues further that Gardecki was not authorized to access the server for the purpose of creating a copy of it. *Id.*

Many courts around the country have "struggled with what it means for a person to access without authorization or exceed an authorization to access a facility." *Cheng v. Romo*, No. 11-cv-10007, 2012 WL 6021369, at *3 (D. Mass. Nov. 28, 2012) (citing Orin Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1240 (2004)). Two diverging approaches to the meaning of "access with authorization" or "exceeding authorization to access" in the context of the SCA have emerged. The United States Court of Appeals for the Third Circuit has not addressed the meaning, but courts in the Eastern District of Pennsylvania have interpreted the language to prohibit unauthorized access of stored communications, but not unauthorized use of the communications. *See Ideal Aerosmith, Inc. v. Acutronic USA, Inc.*, No. 07-cv-1029, 2007 WL 4394447, at *7 (E.D. Pa. Dec. 13, 2007) (citing *Int'l Ass'n of Machinists and Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479, 499 (D. Md. 2005)); *Citizens Bank of Pa. v. Reimbursement Techs., Inc.*, No. 12-cv-1169, 2014 WL 2738220, at *9 (E.D. Pa. June 17, 2014) (quoting *In re Am. Airlines, Inc., Privacy Litig.*, 370 F. Supp. 2d 552, 558-59 (N.D. Tex. 2005)) (the SCA "does not prohibit unauthorized use or disclosure of information obtained from authorized access to a facility").

Under this line of precedent, a defendant who is authorized to access stored information is not liable under the SCA for misusing that information—even if he uses it in a malicious way.[4] *See Ideal*, 2007 WL 4394447, at *7 (finding that a defendant company could not be liable under the SCA for using the contents of stored communications because it had the authority to access those communications). Therefore, an employee who is authorized to access an employer's server is not liable under the SCA for accessing it for unauthorized or illegitimate purposes. *See Citizens*, 2014 WL 2738220, at *1-9 (finding no violation of the SCA when a defendant employee accessed financial information of employer's clients and sold the confidential information to a third party). This approach is consistent with Congress' intent for the SCA to provide protection against "computer hackers" as opposed to disloyal employees. *See Ideal*, 2007 WL 4394447, at *6; *Thompson v. Ross*, No. 10-cv-479, 2010 WL 3896533, at *3 (W.D. Pa. Sep. 30, 2010) (citing S. Rep. No. 99-541, at 3 (1986)) ("Congress enacted [§ 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.").

---

[4] This approach is consistent with how most courts in the United States Court of Appeals for the Third Circuit have interpreted the analogous terms under the Computer Fraud and Abuse Act (CFAA). To establish a CFAA claim, a plaintiff must show that the defendant accessed a protected computer without authorization or by exceeding authorization. While there is a circuit split, district courts in this circuit have almost entirely adopted a narrow interpretation of "authorization" and held that an employee is not liable under the CFAA unless he "hacks into" a computer or the files that he is not authorized to access. *See Carnegie*, No. 13-cv-1112, 2014 WL 896636 at *9 (W.D. Pa. Mar. 6, 2014). The Court notes, however, that in one criminal appeal, the Third Circuit Court of Appeals affirmed a conviction under the CFAA where there was evidence of a defendant accessing customers' accounts without a business purpose. *See United States v. Tolliver*, 451 F. App'x 97, 103 (3d Cir. 2011). The Third Circuit Court of Appeals' analysis of the pertinent language under the CFAA was minimal and did not address the issue at hand here. Therefore, the Court's analysis is not affected.

Courts in other districts have similarly concluded that the SCA "outlaws illegal entry, not larceny." *See Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F. Supp. 2d 817, 821 (E.D. Mich. 2000) (finding that a defendant does not violate the SCA as long as he has authorized access to information "no matter how malicious or larcenous his intended use of that access"); *In re Am. Airlines*, 370 F. Supp. 2d at 558-59 (finding that a defendant company did not violate the SCA when it disclosed plaintiffs' personal information to third party vendors without plaintiffs' consent because the SCA prevents unauthorized access, not unauthorized disclosure of information). Under this approach, an employee exceeds his authorization to access a server only when he accesses stored information without authorization (*e.g.*, using a computer he was not to use, or using someone else's password or code). *See Sherman*, 94 F. Supp. 2d at 821. Therefore, an employee who has authorized access to a server and stored information therein does not exceed his authority even when he accesses the information with malicious intent to misuse it. *See Int'l Ass'n*, 390 F. Supp. 2d at 498-99 (finding that a former employee did not exceed her authorized access to an employer's website when she obtained confidential information from the website with intent to sell it because she was "entitled to see all the information stored therein"); *see also Penrose Comput. Marketgroup, Inc. v. Camin*, 682 F. Supp. 2d 202, 211-12 (N.D.N.Y. 2010) (finding that an employee did not exceed authorization to access his company email account when he deleted his company emails containing useful information to the employer because his full authorization to access the email account included the ability to control his inbox).

On the other hand, other courts have interpreted the language more broadly and held that an employee exceeds his authorization to access an employer's server when he accesses it for non-business purposes. *See Frisco Med. Ctr, L.L.P. v. Bledsoe*, 147 F. Supp. 3d 646, 661 (E.D.

Tex. 2015) (finding that a former Information Systems Administrator "far exceeded" his authorization to access an employer's computer network because he accessed it to obtain confidential information for himself; he had signed a confidentiality agreement that limited his access for job-related duties); *Amedisys Holding, LLC v. Interim Healthcare of Atlanta, Inc.*, 793 F. Supp. 2d 1302, 1316 (N.D. Ga. 2011) (finding that a former sales representative likely exceeded his authorization to access employer's trade-secret material when he sent it to his personal email account before leaving for another job); *Lasco Foods, Inc. v. Hall & Shaw Sales, Mktg, & Consulting, LLC*, No. 08-cv-01683, 2009 WL 3523986, at *5 (E.D. Mo. Oct. 26, 2009) (finding allegations that an employee accessed his employer's confidential information to benefit his own interests and not interests of his employer sufficient to satisfy the "unauthorized" element of the SCA because the employee's authorization to access this information ceased when he breached his duty of loyalty to his employer).

Without addressing the split in interpretation or precedent from courts in the Eastern District of Pennsylvania, the Township asks the Court to adopt this second approach and interpret the language more broadly. It relies primarily on *Lasco* and argues that Gardecki exceeded his authorization to access the server when he accessed it without a legitimate business purpose. In *Lasco*, an employer alleged that it authorized two employees to access its confidential information for the limited purpose of using the information to further the business interests of the employer. 2009 WL 3523986, at *5. The employees allegedly accessed that information to benefit their own interests and not the interests of their employer. *Id*. The court in *Lasco* found that these allegations satisfied the "unauthorized" element of the SCA because the employees' authorization to access the information ceased when they breached their duty of loyalty to their employer and their employment terminated. *Id*.

The Court is not persuaded by the Township's reliance on the *Lasco* court's analysis. Instead, the Court will follow precedent from courts in this Circuit that limits the scope of the SCA to unauthorized access, but not unauthorized use. *See Ideal*, 2007 WL 4394447, at *7; *Citizens*, 2014 WL 2738220, at *9.

For example, the facts here are comparable to those in *Citizens*. In *Citizens*, a defendant employee allegedly accessed financial information of employer's clients without a legitimate business purpose and obtained the confidential information to sell it to a third party. 2014 WL 2738220, at *1. The court in *Citizens* dismissed the SCA claim because the SCA does not prohibit unauthorized use of information obtained from authorized access to a facility.[5] *Id.* at *9. Similarly, dismissal of the SCA claim is warranted here because the Township merely alleges that Gardecki lost his authorization to access the server when he accessed it for non-business purposes, not that he was unauthorized to access the server at all.[6] Am. Compl. ¶¶ 18, 20, ECF No. 9. Moreover, the Township fails to allege that Gardecki exceeded his authorized access to the server because the amended complaint fails to allege that Gardecki copied any stored information that he was not authorized to access. *See Sherman*, 94 F. Supp. 2d at 821.

Without any allegations that Gardecki accessed the server without authorization or that he accessed the stored information in excess of authorization, the Township fails to state a claim under the SCA. Consistent with the weight of authority in this Circuit and from many federal

---

[5] The court in *Citizens* dismissed the SCA claim because of three independent reasons: (1) the plaintiff was not an individual protected under the Act, (2) the plaintiff did not allege access to a stored communication, and (3) the plaintiff's allegations failed to make a proper claim of a violation of the SCA. 2014 WL 2738220, at *8–9. Only the third reason is relevant and discussed above.

[6] Indeed, it strains credibility to infer that as an IT Administrator, Gardecki was not authorized to access the server in its entirety.

courts around the country and consistent with the legislative purpose of the Act, the Court dismisses this claim with prejudice.[7] To convert actions taken by rogue employees authorized to access stored communications into actionable claims under the SCA would extend the scope of the law far beyond Congress' original intent.

B. Remaining state law claims

After dismissing Count I, the only claims that remain in this case are state law claims against Gardecki which allege violation of the Pennsylvania Stored Communications Act (Count II) and breach of fiduciary duty (Count III). A district court may exercise its discretion and decline to exercise supplemental jurisdiction if it has dismissed all claims over which it has original jurisdiction. *Growth Horizons, Inc. v. Del. Cty, Pa.*, 983 F.2d 1277, 1284 (citing 28 U.S.C. § 1367(c)); *see Gallo v. Wash. Cnty.*, No. 08-cv-0504, 2009 WL 274500, at *10-11 (W.D. Pa. Feb. 4, 2009) (using the Court's discretion to refuse to exercise supplemental jurisdiction and dismissing remaining state claims to be refiled in the proper state forum); *Atkinson v. Olde Economie Fin. Consultants, Ltd.*, No. 05-cv-772, 2006 WL 2246405, at *2 (W.D. Pa. Aug. 4, 2006) (dismissing a case without prejudice and remanding to state court for consideration of remaining state law claims after declining to exercise supplemental pendent jurisdiction over plaintiff's remaining claims because there were no claims remaining in the case with jurisdiction pursuant to federal question or diversity jurisdiction). Therefore, the Court dismisses the remaining state law claims without prejudice to be refiled in the proper state court

[7] The Court dismisses this claim with prejudice because permitting leave to amend a second time would be futile. *See Shane v. Fauver*, 213 F.3d 113, 115 (3d Cir. 2000) ("'Futility' means that the complaint, as amended, would fail to state a claim upon which relief could be granted.").

V. CONCLUSION

For the reasons stated above, Gardecki's motion to dismiss is granted. The Township's federal Stored Communications Act claim is dismissed with prejudice. The Township's Pennsylvania Stored Communications Act and breach of fiduciary duty claims are dismissed without prejudice to be refiled in the proper state court. A separate order follows.

BY THE COURT:

/s/ Joseph F. Leeson, Jr.
JOSEPH F. LEESON, JR.
United States District Judge