IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

CLINTON PLUMBING AND HEATING OF TRENTON, INC., et al.,	:	
Plaintiffs,	:	
v.	:	**CIVIL NO. 09-2751**
STEPHEN ANTHONY CIACCIO,	:	
NICOLE MARIE CIACCO, and	:	
CAPITOL ONE BANK (USA), N.A.,	:	
Defendants.	:	

MEMORANDUM OPINION AND ORDER

RUFE, J. **October 22, 2010**

In this case, Plaintiffs Clinton Plumbing and Heating of Trenton, Inc. ("CPH") and Peter and Nancy Pelicano ("Pelicanos"), bring multiple claims against Defendants, all relating to Stephen Anthony Ciacco's alleged fraudulent scheme to make unauthorized transfers from Plaintiffs bank accounts to Ciacco's outstanding credit balance held by Defendant Capital One Bank ("Capital One"). Presently before the Court is Defendant Capital One's Motion to Dismiss Counts II, VII, and XI of the First Amended Complaint.[1] For the reasons that follow, Capital One's Motion will be GRANTED.

[1] Doc. No. 14.

I. FACTUAL AND PROCEDURAL BACKGROUND

A. Procedural Background

Plaintiff Peter Pelicano is the president and sole shareholder of Plaintiff CPH, a corporation that provides plumbing and heating services in New Jersey and Pennsylvania.[2] Defendants are Stephen Ciacco ("Ciacco"), his wife, Nicole Marie Ciacco, and Capital One, the national bank that allegedly held Ciacco's outstanding credit balance and initiated the unauthorized debits from CPH's accounts.

Plaintiffs filed an Amended Complaint in this matter on August 24, 2009.[3] The amended complaint describes a scheme by Ciacco to defraud CPH and the Pelicanos by misrepresenting himself as authorized to initiate transfers from CPH's bank account to his outstanding balance at Capital One. Capital One is alleged to have participated, albeit unwittingly, in Ciacco's scheme by carrying out the unauthorized transactions. Against all Defendants, Plaintiffs bring claims for computer fraud in violation of the Computer Fraud and Abuse Act ("CFAA"), conversion, and identity theft in violation of the New Jersey Identity Theft Statute. Plaintiffs bring claims of fraud and fraudulent transfer against Ciaccio and claims for negligence and breach of warranty against Capital One.

Defendant Capital One has moved to dismiss Plaintiffs' claims against it for computer fraud, identity theft, and breach of warranty. The Court has considered the Motion, Response in Opposition, Reply and Sur-reply, and this matter is now ready for disposition.

---

[2] First Am. Compl. ¶¶ 11–12.

[3] Doc. No. 14.

B. Factual Background

Stephen Ciaccio is the sole proprietor of Krash Enterprises ("Krash"), a computer repair and management company.[4] On November 21, 2007, Ciacco, acting through Krash, entered into a service agreement with CPH.[5] Pursuant to that contract, Ciaccio was responsible for installing and managing CPH's network servers and office management software—which included the software for managing payables and receivables.[6]

Allegedly, Ciacco soon sought greater responsibility for managing the accounts receivable software from CPH.[7] Plaintiffs claim they promoted Ciacco to comptroller of CPH because he told them he required greater access to their bank accounts in order to manage the complexity of the software and difficulties arising from its installation.[8] As comptroller, Ciacco was responsible for managing CPH's payables and receivables and was given access to CPH's bank accounts.[9] Ciacco also set up CPH's computer system so that he could remotely access CPH's account information from his home and personal computer.[10] However, Plaintiffs allege that Ciacco's authorized access

---

[4] First Am. Compl.¶ 11.

[5] First Am. Compl. at ¶ 13.

[6] First Am. Compl. at ¶ 14.

[7] First Am. Compl. at ¶ 15.

[8] First Am. Compl. at ¶ 15.

[9] First Am. Compl. at ¶ 15. During the alleged course of Ciaccio's scheme, he was responsible for administering accounts that CPH held at two different banks. At the beginning of his employment with the CPH, they held three accounts with Sun National Bank (a savings account, and two business checking accounts). First Am. Compl. at ¶ 20. Later, in July of 2008, CPH closed the Sun Trust Account (for reasons unrelated to the alleged fraud), and opened up three accounts with Roma Bank (again, a savings account, and two business checking accounts). First Am. Compl. at ¶ 25. To avoid confusion, the Court will refer to all accounts as the "bank accounts" throughout the body of this opinion.

[10] First Am. Compl. at 15. Plaintiff's complaint does not specify whether they authorized Ciacco to set up remote access to CPH's accounts from his home.

was limited to monitoring the daily status of those accounts.[11] Plaintiffs also claim the Pelicanos had sole authority to authorize payments from the CPH accounts and to authorize automatic clearing house ("ACH") debit transfers on behalf of CPH.[12]

In March of 2008, Ciacco allegedly began making unauthorized transfers from CPH's bank accounts to his personal Capital One credit card account.[13] Plaintiffs claim that Ciacco initiated the ACH debit transfers using Capital One's online credit card payment site.[14] Upon receiving Ciacco's transfer request, Capital One debited the funds from CPH's bank accounts and applied them to Ciaccio's outstanding credit balance.[15] Although the Pelicanos terminated Ciacco from his position as Comptroller in August 2008, he allegedly continued to remotely access the CPH servers and accounts until November 2008.[16]

In November 2008, the Pelicanos discovered the electronic withdrawals by Capital One. [17] They immediately cut off Mr. Ciaccio's access to their bank accounts, suspended all remote access to CPH's computers, changed the passwords for their bank accounts, and informed Capital One of the improper withdrawals.[18] Capital One responded by advising the Pelicanos that it would

[11] First Am. Compl. at ¶ 23

[12] First Am. Compl. at ¶¶ 21, 27.

[13] First Am. Compl. at ¶ 31.

[14] First Am. Compl. at ¶ 31.

[15] First Am. Compl. at ¶ 33.

[16] First Am. Compl. at ¶¶ 19, 38.

[17] First Am. Compl. at ¶38.

[18] First Am. Compl. at ¶38.

investigate the allegations.[19] Although Capital One has since provided Plaintiff with statements regarding the Capital One account, it refuses to reimburse CPH for the amounts withdrawn from their accounts.[20]

II. STANDARD OF REVIEW

A complaint can be dismissed for failure to state a claim upon which relief can be granted pursuant to Federal Rule of Civil Procedure 12(b)(6) if the plaintiff has not presented "'enough facts to raise a reasonable expectation that discovery will reveal evidence' of [a] necessary element."[21] A court must "accept all factual allegations as true, construe the complaint in the light most favorable to the plaintiff, and determine, whether under any reasonable reading of the complaint, the plaintiff may be entitled to relief."[22] However, Plaintiffs' "bald assertions" or "legal conclusions" need not be accepted as true by the court.[23] At this stage, the court does not determine whether the non-moving party will prevail, but whether it will be permitted to offer evidence in support of the claims in the complaint.[24]

This particular pleading standard, described in Federal Rule of Civil Procedure 8(a)(2) as "a short and plain statement of the claim showing that the pleader is entitled to relief"[25] has been

---

[19] First Am. Compl. ¶ 40.

[20] First Am. Compl. at ¶ 41.

[21] Phillips v. County of Allegheny, 515 F.3d 224, 234 (3d Cir. 2008).

[22] Id. at 233.

[23] In Re Burlington Coat Factory Sec. Litigation, 114 F.3d 1410, 1429-30 (3d Cir. 1997).

[24] Fay v. Muhlenberg College, No. 07-4516, 2008 WL 205227 at *4 (E.D. Pa. Jan. 23, 2008) (citing Scheuer v. Rhodes, 416 U.S. 232, 236 (1974)).

[25] FED. R. CIV. P. 8(a)(2).

addressed twice by the Supreme Court of the United States in recent years, first in Bell Atlantic Corp. v. Twombly[26] and then in Ashcroft v. Iqbal.[27] The Court in Twombly articulated a "plausibility" standard that a plaintiff must meet by its factual allegations to survive a motion to dismiss.[28] The Court described it as a level higher than suspicion or speculation.[29] The Iqbal Court clarified that "where the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged - but it has not 'show[n]' - 'that the pleader is entitled to relief.'"[30]

III. DISCUSSION

A. Count II: Computer fraud claim under 18 U.S.C. § 1030

1. Governing Law

Capital One moves to dismiss Count II of Plaintiffs Amended Complaint, wherein Plaintiffs allege that Capital One violated the Computer Fraud and Abuse Act ("CFAA").[31] In particular, Plaintiffs claim a violation of 18 U.S.C. § 1030(a)(5)(A)(iii).[32] As a preliminary matter,

---

[26] 550 U.S. 544 (2007).

[27] 129 S. Ct. 1937 (2009).

[28] Twombly, 550 U.S. at 556.

[29] Id. at 555. The decision in Twombly retired the previous standard articulated in Conley v. Gibson, 355 U.S. 41 (1957), allowing dismissal if it "appears beyond doubt that the plaintiff can prove no set of facts in support of his claim which would entitle him to relief." Conley, 355 U.S. at 45-46.

[30] Iqbal, 129 S. Ct. at 1950 (quoting FED. R. CIV. P. 8(a)(2)).

[31] 18 U.S.C. § 1030.

[32] Plaintiffs' reply attempts to constructively amend the complaint by alleging that Capital One violated §§ 1030(a)(2)(A), 1030(a)(2)(c), and 1030(a)(5)(c). See Pls.' Mem. Opp'n Def. Capital One's Mot. to Dismiss, 7 (Doc. No. 21). "Plaintiffs may not amend the complaint to add . . . a claim to their allegations in their briefs in opposition to the motion . . . ." Herbert v. Mentor, No. 04-413, 2007 WL 2893387, *5 (D.N.J. 2007) (citing Fletcher-Harlee Corp. v. Pote Concrete Contractors, Inc., 482 F.3d 247, 252–53 (3d Cir. 2007)) ("[T]o request leave to amend a complaint, the plaintiff must submit a draft amended complaint to the court. . . ."); Ranke v. Sanofi-Synthelabo, Inc.,

the Court notes that this provision of the CFAA no longer exists—the statute was amended in September 2008. The parties do not address this problem, and the First Amended Complaint and Capital One's Motion to Dismiss both apply the pre-amendment law.[33]

A comparison of the pre- and post-amendment statutes reveals that the changes did not substantively change 18 U.S.C. § 1030(a)(5)(A)(iii); instead, they mainly reorganized the pertinent parts of the statute. Each version of the statute requires Plaintiffs to allege the same five elements, explained infra, to sufficiently state a claim.[34] In addition, the majority of the alleged debit transfers at issue in this case took place prior to the amendments.[35] Therefore, because the substance of the law did not significantly change post-amendment, and because the bulk of the alleged conduct occurred prior to the amendments, the Court will analyze Plaintiffs' claim under the pre-amendment law.

2. Analysis under the CFAA

Although the CFAA is primarily a criminal statute, it provides a private cause of action in particularized circumstances. Under § 1030(g), "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action . . . if the conduct involves [one] of the

---

436 F.3d 197, 206 (3d Cir. 2006). The Court therefore disregards additional claims raised by the Plaintiffs in their Reply for the purposes of our analysis herein.

[33] Plaintiffs, in their Opposition to the Motion, cite to the new amendments.

[34] For example, the amended version of § 1030(a)(5)(A)(iii), now codified at §1030(a)(5)(C), no longer requires an aggregate loss of $5,000. However, under § 1030(g), Plaintiffs are entitled to bring a civil action only if the alleged conduct caused a loss aggregating at least $5,000. Therefore, while the statutory requirements have been rearranged, their substance remains unchanged.

[35] Plaintiffs allege that the first unauthorized ACH transfer occurred on 3/20/2008, (First Am. Compl. at ¶34), and that the last transfer occurred on 11/17/2008 (Compl. ¶ 37). Therefore, six months of the alleged conduct occurred while the pre-amendment law governed; the post-amendment law was effective for less then a month before the cessation of transfers between Plaintiffs' bank accounts and Ciacco's credit balance.

factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B)."[36] The five factors listed under subsection (a)(5)(B) specify the forms of damage or loss that are possible harmful results of violations of other parts of the statute.[37]

Here, 1030(g) does not impose any extra burden on Plaintiff because §1030(a)(5)(A)(iii) contains a parallel requirement to show one of the special forms of loss or damage listed under (a)(5)(B). Accordingly, the Court need look no further then §1030(a)(5)(A)(iii) to determine if Plaintiffs have sufficiently alleged their claim. It is a violation of §1030(a)(5)(A)(iii) to:

> (iii) intentionally access[] a protected computer[38] without authorization, and as a result of such conduct, cause[] damage; *and*
>
> (B) by conduct described in clause (I), (ii), or (iii) of subparagraph (A), cause[] . . . [one of the special forms of loss or damage set forth in subsections (i)–(v)].[39]

In short, §1030(a)(5)(A)(iii) requires Plaintiff to allege 1) intentional access; 2) of a protected computer; 3) without authorization; 4) that causes damage; ***and*** 5) loss.

---

[36] 18 U.S.C. § 1030(g).

[37] The conduct described in §1030(5)(B) includes:

> (i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value; (ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (iii) physical injury to any person; (iv) a threat to public health or safety; or (v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security.

See also P.C. Yonkers, Inc. v. Celebrations! The Party & Seasonal Superstore, L.L.C., Civ. A. No. 04-5554(JAG), 2007 WL 708978, at *4 (D.N.J. Mar. 5, 2007).

[38] The Parties do not dispute whether the computers in question were "protected."

[39] 18 U.S.C. § 1030 (emphasis added).

Plaintiffs argue that Capital One violated §1030(a)(5)(A)(iii) by intentionally accessing Plaintiffs' bank accounts through the banks' protected computers. They claim that Capital One's access was unauthorized and caused damage to CPH in the form of money withdrawn from the bank accounts, overdraft fees, returned checks, late fees, reputational damages arising from a damaged credit score, and the termination of contracts due to insufficient funds for payments. [40]

Capital One argues that Count II should be dismissed for failure to state a claim under the CFAA. The thrust of Capital One's argument is that the kind of loss and damage alleged—"wrongfully debiting . . . bank accounts at the direction of Plaintiffs' alleged dishonest employee"—does not violate the CFAA.[41] Additionally, they argue §1030(a)(5)(A)(iii) requires Plaintiff to allege an "intent to harm." Finally, they contend that Plaintiffs did not sufficiently allege Capital One acted "without authorization." The Court will address each of these arguments in turn.

a. Intent and authorization

Capital One argues that Plaintiffs must allege an intent to harm under §1030 (a)(5)(A)(iii). The Court disagrees. By the principle of *expressio unius est exclusio alterius*,[42] subsection (a)(5)(A)(iii) unambiguously excludes an intent to harm requirement. There are three subsections listed under (a)(5)(A), each of which specifies—or, in the case of (a)(5)(A)(iii), fails to specify—a different mental state associated with "damage." Subsection (i) punishes "intentional . . . damage," subsection (ii) punishes "reckless[] . . . damage," but subsection (iii) punishes "damage" alone. Congress's failure to

[40] Pls.' First Am. Compl. ¶ 53.

[41] Defendant's Mot. To Dismiss, 5-6.

[42] See United States v. Lendmesser, 378 F.3d 308, 313 n.8 (3d. Cir. 2004) ("The canon of expression *unius est exclusio alterius* means that explicit mention of one thing in a statute implies a congressional intent to exclude similar things that were not specifically mentioned.").

define a mental state under subsection (iii) indicates that Congress did not establish an intent requirement for damage under 5(A)(iii).[43] Further, the cases cited by Defendant in support of its argument analyze the intent requirements for *different subsections* of 5(A).[44] Therefore, Plaintiffs are correct: They do *not* need to allege an *intent to harm* in order to state a claim under 1030(a)(5)(A); instead they need only allege that Capital One *intentionally accessed* the protected computers without authorization. Here, Plaintiffs allege that "Capital One *intentionally accessed* computers owned by Roma Bank, Sun National Bank, and/or others, which were used to store information regarding CPH's accounts with Sun National Bank and/or Roma Bank."[45] They also allege that Capital One repeatedly accessed the accounts and initiated transfers from CPH's bank accounts.[46] Therefore, the key inquiry is whether that access was "without authorization."

Capital One argues that because it was authorized to access the relevant computers when it initiated the debits from Plaintiffs' account, it is not liable under the CFAA. To state a claim under §1030(a)(5)(A)(iii), Plaintiffs must allege that the use of the computer was either without, or exceeded, Capital One's authorization. Capital One claims that it did not access the banks' protected computers

---

[43] Accord United States v. Morris, 928 F.2d 504, 507–09 (2d Cir. 1991) (reaching the same conclusion by analyzing both the legislative history and text of an older version of the CFAA in order to conclude that the 'intentionally' standard applies only to the 'accesses' phrase of section 1030(a)(5)(a)(iii), and not to its "damages" phrase).

[44] E.g., Kalow & Springnut, LLP v. Commence Corp., 2008 WL 2557506, *3 (D.N.J. June 23, 2008) (stating that there is an intent requirement under § 1030(a)(5)(A)(i)); North Texas Preventive Imaging, LLC v. Eisenberg, 1996 WL 1359212, *4,6 (C.D. Cal. Aug. 19, 1996) (Finding an intent to harm requirement in the 1994 version of the CFAA, § 1030 (a)(5)(A), where the statute stated that "[whoever] through means of a computer used in interstate commerce . . . knowingly causes the transmission of a program, information . . . to a computer . . . if (i) the person causing the transmission intends that such transmission will [listing various resulting activities and other requirements]"). The law discussed in North Texas was subsequently amended, and now reads as is noted supra.

[45] Pls.' First Am. Compl. ¶ 50.

[46] Pls.' First Am. Compl. ¶ 31.

without authorization because it initiated the online transfers upon the request of a customer who was apparently authorized to access those accounts.[47] In response, Plaintiffs argue that because Plaintiffs were the *only* persons allowed to authorize ACH transfers on behalf of CPH, Ciaccio was incapable of granting permission for Capital One to access the accounts.

Although the CFAA specifically defines "exceeds authorized access," it does not specifically define the phrase "without authorization" or "authorization."[48] Consequently, the contours of those terms have been developed primarily in the context of employer-employee disputes over whether authorization, once given, can be lost based on subsequent bad conduct.[49] Unlike in those cases, Plaintiffs do not allege that Capital One lost or exceeded a previously granted authorization. Instead, they argue that because Ciacco lacked the authority to grant access the accounts, Capital One's belief that its access was authorized is irrelevant.

Although the precise question presented in this case has not previously been addressed within this Circuit or elsewhere, the existing case law offers some guidance. Courts that have construed "without authorization" have reached conflicting interpretations: Some courts have adopted a broad, agency-based interpretation of "authorization" which examines the subjective intent of the accesser.[50]

---

[47] Defendant's Mot. To Dismiss, 5–6.

[48] Section 1030(e)(6) defines "exceeds authorized access" as "access[ing] a computer without authorization and us[ing] such access to obtain or alter information in the computer that the accesser is not entitled to obtain or alter."

[49] See e.g., Bro-Tech Corp. v. Thermax, Inc., 651 F. Supp.2d 378, 406, n.22 (E.D. Pa. 2009) (Rufe, J.) (considering whether an employee's authorization permitted her to delete certain emails); See Consulting Professional Res., Inc. v. Concise Technologies, LLC, No. 09-1201, 2010 WL 1337723, at *4 (W.D. Pa. March 9, 2010); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000) (holding that employees' authority to access company computers ended when those employees surreptitiously became agents of defendant competitor and sent the company's proprietary information to competitor via email).

[50] Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006); Shurgard Storage, 119 F. Supp. at 1125.

Others—including this court—have adopted "the narrower view that the terms [of the CFAA] describe action that is 'tantamount to trespass in a computer.'"[51] Because this Court has adopted the narrower view, Plaintiffs need only contend that Capital One actually lacked authorization, regardless of its belief—reasonable or not—that it was authorized to access the system.

Here, Plaintiffs allege that Ciacco was not permitted to authorize ACH payments from its bank accounts. Assuming this is true—as the Court must in the current procedural posture—if Ciacco did not have the authority to access the accounts, he was therefore incapable of granting Capital One permission to do so. Although the parties dispute whether Mr. Ciacco was an "apparent customer" with the authority to approve a transaction, resolution of that dispute is inappropriate at this stage in the litigation. Therefore, Plaintiffs have sufficiently alleged that Capital One debited the bank accounts "without authorization."

b. Damage and loss

Although the CFAA defines "damage" as "any impairment to the integrity or availability of data, a system, or information,"[52] the scope of the term is unsettled.[53] Some courts construe the term narrowly, and construe "damage" as only those circumstances resulting in "some diminution in the completeness or usability of data or information on a computer system."[54] Courts advocating a broader

---

[51] See Bro-Tech Corp. v. Thermax, Inc, 651 F. Supp.2d 378, 406–09 (E.D. Pa. 2009) (Rufe, J.) (granting in part and dismissing in part Defendants' motion for summary judgment); see also Shamrock Foods v. Gast, 535 F.Supp.2d 962, 964–95 (D. Ariz. 2008) (collecting cases); Brett Senior & Assocs., P.C. v. Fitzgerald, No. 06-1412, 2007 WL 2043377, at *3 (E.D. Pa. July 13, 2007).

[52] 18 U.S.C. § 1030 (e)(8).

[53] See P.C. Yonkers, Inc., 2007 WL 708978, at *16; EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 584 (1st Cir. 2001); In re Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 521 (S.D.N.Y. 2001).

[54] Garelli Wong & Assocs, Inc. v. Nichols, 551 F. Supp. 2d 704, 709 (N.D. Ill. 2008) (quoting ResDev, LLC v. Lot Builders Ass'n Inc., No. 6:04-CV-1374, 2005 WL 1924743, at *5 n.3 (M.D. Fla. Aug.10, 2005) (concluding that CFAA liability does not arise merely by copying data); see also Motorola, Inc. v. Lemko Corp.,

interpretation have held that the mere copying or sending of confidential information constitutes damage because it causes irreparable harm to the integrity of the computer system or database.[55]

The debate over the scope of the term "damage" has mainly arisen in employer-employee claims for theft of trade secrets or use of confidential information to gain an unfair competitive edge. For instance, in Shurgard Storage, the Plaintiff collected and disseminated confidential information from his former employer.[56] There, although no data was physically changed or erased, an impairment of integrity occurred because of the "subsequent corrective measures the rightful computer owner [had to] take to prevent the infiltration and gathering of confidential information."[57] In Bro-Tech Corporation v. Thermax,[58] this Court recognized the "increasingly expansive scope of the CFAA" and also allowed an employee-employer information misappropriation claim to proceed under the CFAA.[59]

Plaintiffs do not allege that Capital One collected, copied, or disseminated any of the confidential information. Instead, they argue that the debit transfers impaired the integrity of the bank's information by changing the balance reflected in Plaintiffs' account. Before the transfers began, the computer data reflected a balance of almost $150,000; by the time they stopped, the balance

---

609 F. Supp. 2d 760, 769 (N.D. Ill. 2009).

[55] See e.g., HUB Group, Inc. v. Clancy, No. Civ. A. 05-2046, 2006 WL 208684, *2–4 (E.D. Pa. Jan. 25, 2006) (noting that emails with attachments sent to Defendant's wife regarding confidential company information constituted damage to the integrity of Plaintiff's's computer database); I.M.S. Inquiry Mgmt. Sys, Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 525 (S.D.N.Y. 2004) (noting that copying of confidential information for competitor appropriation was enough for "damage" purposes as it caused irreparable harm to the integrity of the data and the system).

[56] 119 F. Supp.2d at 1122–23.

[57] Id. at 1126–27 (W.D. Wash., 2000) (quoting S. Rep. No 104-357 at 11 (1996)).

[58] 2006 WL 516767 (E.D. Pa. 2006) (Rufe, J.).

[59] Id.

was $0. Although this argument is creative, it goes too far. In Shurgard Storage, the court construed "integrity," in the context of the statute as "necessarily contemplat[ing] maintaining the ***data*** in a protected state." There, integrity referred to confidential information—namely trade secrets—that were gathered and disseminated.[60] Here, Plaintiffs do not allege that the integrity of *data* was impaired; instead, they allege the integrity of their *bank funds* was impaired. This claim does not allege damage for the purposes of the CFAA.

Similarly, Capital One argues that Plaintiffs' allegations do not meet the statutory definition of loss. "Loss" is treated separately from "damage" in the CFAA, and is specifically defined as:

> 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 interruption of service.[61]

Various courts have interpreted "loss" to mean the remedial costs of investigating a computer for damage, remedying damage done, and costs incurred while the computer is inoperable.[62] In *Crown Coal & Coke Co. v. Compass Point Resources, LLC*, the court explained that: "According to the CFAA, lost "revenue" constitutes "loss" if it is incurred "because of interruption of service." Therefore, if defendants had lost revenue because their computers were inoperable, that would be the type of lost revenue contemplated by the statute."[63] This interpretation of "loss" has been adopted by other courts. For instance, in B&B Microscopes v. Armogida, Plaintiffs suffered a loss after they lost

---

[60] Shurgard Storage Ctrs., 119 F.Supp. at 1127.

[61] 18 U.S.C. § 1030(e)(11).

[62] E.g., Nexans Wires S.A. v. Sark-USA, Inc., 319 F. Supp. 2d 468, 474 (S.D.N.Y. 2004), aff'd, 166 Fed. App. 559 (2d Cir. 2006); Dudick, ex rel. Susquehanna Precision, Inc. v. Vaccarro, No. 06-cv-2175, 2007 WL 1847435, *6 (M.D. Pa. June 25, 2007); P.C. Yonkers, Inc., 2007 WL 708978, *5 (D.N.J. March 5, 2007).

[63] 2009 WL 1806659, *8 (W.D. Pa. June 23, 2009).

access to data and were unable to reproduce their operational system.[64] Conversely, in Advantage Ambulance Group, Inc. v. Lugo,[65] Plaintiffs' claim for *future* lost revenue because of the dissemination of its trade secrets was not "loss" under the CFAA.[66]

Here, Plaintiffs allege "loss of assets, overdraft fees, returned check fees, late fees, reputational damages arising from a damaged credit score, and termination of certain contracts due to insufficient funds for payment."[67] Like the claim in Advantage Ambulance, none of these claims allege loss *related to computer impairment or interruption of service*. These losses did not arise from investigating computer damage, remedying or responding to damage done, or costs incurred while the computer was impaired. Instead, they were the consequential damages of an overdrawn bank account. This is not the type of loss envisioned by the drafters of the CFAA. Because Plaintiffs do not set forth plausible fact allegations regarding the damage and loss elements of a CFAA claim, this claim against Capital One will be dismissed.

B. Count VII: Identity Theft under New Jersey Statute 2C: 21-17

A civil cause of action for a person harmed by a violation of the New Jersey Identity Theft Statute ("Identity Theft Statute") 2C:21-17 is found in 21-17.4, as Plaintiffs suggest[68] and as Capital One concedes.[69] First, Capital One claims the statute applies only to natural persons and not corporations. This is incorrect. "Person" is defined in two places in the Identity Theft Statute, and

[64] B&B Microscopes v. Armogida, 532 F. Supp. 2d 744 (W.D. Pa. 2007).

[65] No. 08-3300, 2009 WL 839085 (E.D. Pa. March 20, 2009).

[66] Id. at * 4.

[67] Pls.' First Am. Compl.¶ 53.

[68] Pls.' First Am. Compl. ¶ 76–81.

[69] Mot. to Dismiss at 8.

both definitions are inclusive of Capital One. Under New Jersey Statute 2C :20-1(m), which applies to the Identity Theft Statute, "person" is defined to "include[] any individual or entity or enterprise;" and under New Jersey Statute 2C 21-24, which also applies to the Identity Theft Statute, "person" is defined as "any corporation, unincorporated association or any other entity or enterprise."

However, Capital One properly challenges the substance of Plaintiffs' allegations under the New Jersey Identity theft statute. In their Response to Defendant's Motion to Dismiss, Plaintiffs claim that their allegations "fit the statutory language" of two subsections of the Identity Theft Statute:

> A person is guilty of an offense if the person . . .
>
> (2) Pretends to be a representative of some person or organization and does an act in such pretended capacity for the purpose of obtaining a benefit for himself or another or to injure or defraud another; [or]
>
> (4) Obtains any personal identifying information pertaining to another person and uses that information, or assists another person in using the information, in order to assume the identity of or represent himself as another person, without that person's authorization and with the purpose to fraudulently obtain or attempt to obtain a benefit[.]

It is apparent from the plain text of the statute that Plaintiffs have alleged neither the *actus reus* nor the *mens rea* required to state a claim under either subsection. The Identity Theft Statute is meant to punish individuals who "impersonate[] another or assume[] [a] person's identity for the purpose of obtaining a benefit for himself or for the purpose of defrauding another."[70] In an effort to fit its claim to the statute, Plaintiff alleges that Capital One, "'purport[ed]' to act on behalf of CPH." But the act of pretending requires an individual to intentionally adopt a false pretense. And here, Plaintiffs do not assert any facts consistent with the claim that Capital One ever pretended to be someone it is not.

[70] State of New Jersey v. Smith, 2009 WL 17873, *4 (N.J. Super. A.D. Jan. 2, 2009).

Moreover, subsection four is clearly aimed at combating identity theft. The *actus reus* of the crime is to "'obtain[] personal information' . . . in order to assume the identity of or represent himself as another person." Plaintiffs do not allege that Capital One obtained information; rather, they allege that Capital One *received* information. Further, even if the allegations do properly state that Capital One "obtained" information, there is no allegation that they did so for the purpose of "assum[ing] the identity or represent[ing] [its]elf as another person."

Finally, imposing liability on Capital One for Mr. Ciacco's alleged misrepresentations would misconstrue the intent of the New Jersey legislature. As noted in *Piscitelli v. Classic Residence by Hyatt*,[71] the civil remedy provided under the Identity Theft Statute is "directed against the thief."[72] It is not intended to punish third parties who are unwittingly are involved in a fraudster's scheme. It is unclear how, as Plaintiffs claim, their allegations fit the statute "like a glove." This claim is dismissed.

C. Count XI: Breach of Warranty

Plaintiffs allege that under the National Automated Clearing House Association ("NACHA") rules,[73] Capital One warranted to CPH that it would not debit accounts without authorization.[74] Therefore, when Capital One carried out the unauthorized debit transfers (Automatic Clearing House ("ACH") transactions), it breached its warranty.[75] In response, Capital One argues that Plaintiffs do

---

[71] 408 N.J. Super. 83 (N.J.Super.A.D., 2009).

[72] Id. at 115.

[73] NACHA 2010 Operating Rules ("NACHA Rules"(2010), *available at* http://www.achrulesonline.org/free_pdf.aspx.

[74] Pls.' First Am. Compl. ¶¶ 105–07

[75] Pls.' First Am. Compl. ¶ 108.

not have standing to assert a breach of warranty claim because the warranty provisions of the NACHA Rules apply only to the obligations between banks.

The NACHA Rules establish the contractual obligations between the parties to ACH transactions.[76] The ACH is a national network of banks and financial institutions which transfers funds electronically to and from bank customers' accounts.[77] In a typical transaction, the ***Originator*** is any individual that initiates entries into the ACH network.[78] Here, the originator was Ciaccio, who fraudulently initiated the ACH transfer from CPH's bank account. Ciaccio sent his request to Capital One, the ***Originating Depository Financial Institution*** ("ODFI").[79] A financial institution is an ODFI if it agrees to originate ACH entries at the request of its customers. After receiving Ciaccio's (the originator's) response, Capital One (the ODFI) sent a request for a debit transfer to the ***ACH***,[80] who processed the request and forwarded it to CPH's bank, the ***Receiving Depository Financial Institution*** ("RDFI").[81] Because CPH had entered into ACH agreements authorizing its Bank (the RDFI) to honor ACH requests to debit its account, it was categorized as a ***Receiver***.[82] A ***Receiver*** is the consumer

---

[76] The rules governing ACH transfers are promulgated by the National Automated Clearing House Association ("NACHA")—a not for profit association of financial institutions who use the ACH network. See NACHA, Executive Management, http://www.nacha.org/c/ExecMgmt.cfm (last visited September 23, 2010); see also Lary Lawrence & Bryan D. Hull, Payment Systems §15:6 (2009) (explaining the NACHA system and the structure of a typical transaction).

[77] Volden v. Innovative Financial Systems, Inc, 440 F.3d 947, 949 (2006) (explaining the structure of the ACH and the NACHA).

[78] NACHA Rules, § 14.1.48.

[79] Id. at § 14.1.47.

[80] Id. at § 14.1.1.

[81] Id. at § 14.1.60.

[82] Id. at § 14.1.58.

whose account is accessed. Therefore, the bank (the RDFI) approved Capital One's (the ODFI) debit requests and debited CPH's (the receiver's) account.

Here, an important precondition to any ACH transfer—authorization—was missing. But Capital One relied on the Ciacco's (the originator's) representation that the transfer was authorized and carried out the transaction. When this type of unauthorized ACH transfer occurs, the NACHA Rules protect *certain* parties by requiring: "[e]ach ODFI sending an entry [to] warrant[] the following to each ***RDFI***, ***ACH Operator***, and ***Associations***[83]:

> §2.2.1.1 . . . . each entry transmitted by the ODFI to an ACH Operator is in accordance with *proper* authorization provided by the Originator and that is in accordance with proper authorization provided by the Originator and the Receiver; [and]
>
> §2.2.3 Each ODFI breaching any of the preceding warranties [here, §2.2.1.1] shall indemnify each *RDFI, ACH Operator*, and *Association* from and against any and all claim, demand, loss, liability, or expense, including attorney's fees and costs, that result directly or indirectly from the breach of warranty or the debiting or crediting of the entry to the receivers account.[84]

Plaintiffs do not have standing to raise a breach of warranty claim pursuant to the NACHA Rules. Neither section creates an authorization warranty that runs to any party outside the RDFI, ACH Operator, and Associations.[85] Plaintiffs direct the Court to consider Security First Network Bank v. C.A.P.S., Inc,[86] where an Illinois federal district court considered a breach of warranty claim directly

---

[83] An "[A]ssociation means a Payment Association." NACHA Rules, §14.1.9.

[84] (emphasis added).

[85] Plaintiffs only assert a breach of warranty claim arising from a direct contractual relationship between itself and Capital One; they have not asserted any other breach of warranty claims in their complaint. Therefore, the court does not analyze whether Plaintiffs have standing to assert a breach of warranty claim under a third-party beneficiary theory. Notably, in Sinclair Oil Corp. v. Sylvan State Bank, 894 F. Supp. 1420 (D. Kansas 1995), the court rejected a receiver's attempt to assert a breach of warranty claim under a third-party beneficiary theory.

[86] No. 01-C-342, 2002 WL 485352 (N.D. Ill. 2002).

analogous to the one raised by Plaintiffs. In that case, Joseph Sykes, using the name Marvin Goldman, opened a deposit account at Security First Bank in Chicago.[87] Security First was unaware of Sykes' true identity at the time.[88] Using the Goldman alias, Sykes was able to fraudulently debit accounts held by two companies at other banks in the Chicago area and transfer the funds into his Goldman account at Security First.[89] One of the accounts debited was Consolidated Artists Payroll Service, Inc. ("CAPS"), an Illinois firm that used electronic fund transfers to provide payroll services to its customers.[90] The other account that Sykes defrauded was a Saks Fifth Avenue ("Saks") payroll account held at LaSalle Bank.[91]

Both Saks and CAPS alleged that they entered into agreements with their banks for ACH services, and that the agreements incorporated the NACHA Rules.[92] Security First argued that neither company could enforce the NACHA warranty provisions because they run only to RDFIs and ACH operators, and not to receivers. The court began by drawing a distinction between §§2.2.3 and 2.2.1.1. Although it agreed that Saks could not enforce the warranty provisions under §2.2.3 because "it [was] an agreement *to indemnify* an RDFI, ACH Operator or Association for the breach of the warranty in §2.2.1.1,"[93] it interpreted §2.2.1.1 to create a direct warranty between Saks (the receiver) and Security

---

[87] Id. at *1.

[88] Id.

[89] Id.

[90] Id.

[91] Id.

[92] Id.

[93] Id. at * 6.

First (the OFDI). Accordingly, the court allowed the breach of warranty claim to survive the Motion to Dismiss.[94]

The Court does not find the reasoning of Security First persuasive. First, the Security First court apparently ignored the clear text of the warranty provision, which limits its reach to RDFIs, ACH Operators, and Associations. Sections 2.2.1.1 and 2.2.3 fall under that limitation, so it is unclear how the Security First court interpreted §2.2.1.1 to have a broader reach then §2.2.3. Second, NACHA clarified its own rules in a 2008 Amendment entitled "Beneficiaries of the Rules," which states that:

> §1.9 Nothing in these rules is intended to, and nothing in these rules shall be implied to, give any legal or equitable right, remedy, or claim to other entity, including to any Originator, ***Receiver***, Third-Party Service Provider, or Third-Party Sender.[95]

Notably, the Security First decision predates the rule clarification offered in §1.9. In this case, Capital One was an ODFI, Plaintiffs' banks were RDFIs, and CPH was a receiver. Since CPH has receiver status, it does not have standing to bring a breach of warranty claim under NACHA.

---

[94] Id.

[95] Capital One attached NACHA Rule § 1.9, a 2008 amendment to the NACHA Rules entitled "Beneficiaries of the Rule" to its Reply to Plaintiffs' Opposition to Capital One's Motion to Dismiss the First Amended Complaint. Doc. No. 24. Plaintiffs dispute the authenticity of the document, and argue that because it was not attached to the complaint, it is improper to consider on a Motion to Dismiss. See Pl.'s Sur-Reply, Doc. No. 27. In In Re Burlington Coat Factory, then-Judge Alito noted that "[a]s a general matter, a district court ruling on a motion to dismiss may not consider matters extraneous to the pleadings" without converting the motion to Summary Judgment. 114 F.3d at 1426. Although there is an exception to the general rule if a "document [is] integral to or explicitly relied upon by Plaintiffs, consideration of extraneous documents is only appropriate if they are "undisputedly authentic." Id.

Here, Plaintiffs simultaneously contest the authenticity of the NACHA Amendment, see Pls.' Sur-Reply, while also relying on the NACHA as a basis for their breach of warranty claim, see First Am. Compl. at ¶¶ 100–104. Although Plaintiffs' breach of warranty claim is generally alleged to be "pursuant to the NACHA Rules and regulations," the complaint does not specify *which* NACHA Rules create the warranty they claim exists. Because of the generality of Plaintiffs' allegations, this Court *must* also generally review the NACHA rule. Although the attached amendment was passed *after* the conduct, NACHA specifies that is meant as a "clarification," and does not substantively change the rule. Therefore, this Court must consider the amendment in order to assess the sufficiency of Plaintiffs' allegations. Just as "Plaintiffs cannot prevent a court from looking at the texts of the documents on which its claim is based by failing to attach or explicitly cite them," Plaintiffs cannot hem in the scope of this Court's review by selectively disputing sections of the NACHA Rules. In Re Burlington Coat Factory, 114 F.3d at 1426.

IV. Conclusion

Based on the foregoing discussion, the Court finds that Plaintiff has failed to sufficiently allege that Defendant Capital One violated the CFAA, New Jersey Identity Theft Statute, or the terms of a warranty owed to Plaintiffs. Accordingly, Capital One's Motion to Dismiss is GRANTED in full.

An appropriate Order follows.