Not for Publication

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

ESSGEEKAY CORPORATION d/b/a AMERICAN PRESCRIPTION SURGICAL CENTER, **Plaintiff,** **v.** **TD BANK, N.A.,** **Defendant.**	**Civil Action No. 18-3663 (ES) (CLW)** **OPINION**

SALAS, DISTRICT JUDGE

Before the Court is Defendant TD Bank, N.A.'s ("TD") motion to dismiss Plaintiff Essgeekay Corporation's ("Plaintiff") Complaint under Federal Rule of Civil Procedure 12(b)(6). (D.E. No. 3). The Court has jurisdiction pursuant to 28 U.S.C. § 1332. Having considered the parties' submissions, the Court decides this matter without oral argument. *See* Fed. R. Civ. P. 78(b). As set forth below, the Court DENIES TD's motion to dismiss as to Count I and GRANTS TD's motion to dismiss as to Count II and Count III.

I. BACKGROUND[1]

Plaintiff is a pharmacy located in Fort Lee, New Jersey, represented by Sreedhar Vajinepalli and Kalpesh Dave. (D.E. No. 1-1, Complaint ("Compl.") ¶¶ 5 & 9). In February of 2009, Vajinepalli and Dave opened a TD business checking account on behalf of Plaintiff, over which they had sole control. (*Id*. at ¶¶ 8–9). Upon opening the account, TD provided each Vajinepalli and Dave independent login credentials to access the online banking system—credentials that they did not share

[1] The Court must accept Plaintiff's factual allegations as true for purposes of resolving the pending motion to dismiss. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009); *Bistrian v. Levi*, 696 F.3d 352, 358 n.1 (3d Cir. 2012).

with each other or anyone else. (*Id*. ¶¶ 10–12). As an additional security protocol, Vajinepalli and Dave selected individualized security questions and provided confidential responses. (*Id*. ¶¶ 11–12).

As a matter of business, each month Vajinepalli arranged five to six wire transfers to pay various pharmacy wholesalers operating in New York and New Jersey. (*Id*. ¶¶ 13–14). Plaintiff alleges that "wire transfers were not generally made for any other purpose" and Dave was not involved in the wire transfers and never initiated a transfer from his online account. (*Id*. ¶¶ 13–14). Whenever Vajinepalli attempted to login to the online account from an unfamiliar computer, TD would lock the account and require him to call the bank and "provide identifying corporate information . . . as well as the answers to his specific security questions." (*Id*.).

Sometime after June 7, 2016, Vajinepalli logged into the online account with his personal username and noticed three unauthorized wire transfers to bank accounts in California, Oklahoma, and Texas. (*Id*. ¶¶ 16–17). The transfers totaled approximately $176,000. (*Id*. ¶ 16). Plaintiff alleges that none of these transfers were consistent with either the identity or location of the usual payees involved in prior wire transfers. (*Id*.). Soon after, Vajinepalli discovered that the transfers were initiated from Dave's online account without Dave's approval, rather than Vajinepalli's account, as was the usual process. (*Id*. ¶¶ 15 & 17). Upon discovery of the transfers, Dave attempted to login to his account, but was unable to because security procedures had locked him out. (*Id*. ¶ 17).

When Dave called TD to report the issue, the representative informed him that TD had locked his account because TD suspected fraudulent activity. (*Id.* ¶ 18). TD did not, however, explain the basis of this suspicion. (*Id.* ¶ 25). TD claimed that before processing the transfers, it attempted to contact Dave by phone and email to obtain approval for the transfers. (*Id.* ¶¶ 26–27). TD "ultimately authorized the transfers" even though TD "never received such approval from Dave for any of the transfers." (*Id.* ¶ 27). Dave asked TD representatives to disclose the contact information they had used to contact him, but TD did not provide the information. (*Id.* ¶ 26).

On June 13, 2016, Vajinepalli visited the Parsippany branch of TD seeking answers about the fraudulent transfers. (*Id*. ¶ 20). However, TD representatives informed Vajinepalli that the Bank required "a police report before TD . . . could take action with respect to recovering the funds." (*Id*. ¶ 19). Vajinepalli immediately filed a report with the Parsippany-Troy Hills Police department, but Plaintiff alleges that even then, TD failed to effectuate a reversal of the fraudulent transfers and failed to provide Plaintiff with any additional information about the transfers or TD's purported investigation. (*Id*. ¶¶ 20–22). This prompted Dave to call TD two to three times a day to seek more information, but each time he was transferred from one department to another without ever receiving the requested information. (*Id.* ¶ 23).

Four days later, on June 17, 2016, TD assigned the case to a corporate security representative and attempted to reverse the transfers, but was unable to do so as the transferee(s) had already removed the funds. (*Id*. ¶¶ 24, 28 & 30–31). On June 20, 2016, TD informed Plaintiff by phone that the funds were lost, and that they would be unable to process the reversal. (*Id*. ¶¶ 30–31). Plaintiff filed this action in the Superior Court of New Jersey and TD subsequently removed the case to this Court. (*See* D.E. No. 1).

II. LEGAL STANDARD

To withstand 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 *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)).[2] "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." *Id.* "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.*

[2] Unless otherwise indicated, all citations and internal quotation marks are omitted, and all emphasis is added.

"When reviewing a motion to dismiss, [a]ll allegations in the complaint must be accepted as true, and the plaintiff must be given the benefit of every favorable inference to be drawn therefrom." *Malleus v. George*, 641 F.3d 560, 563 (3d Cir. 2011). But the court is not required to accept as true "legal conclusions," and "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Iqbal*, 556 U.S. at 678.

Finally, "[i]n deciding a Rule 12(b)(6) motion, a court must consider only the complaint, exhibits attached to the complaint, matters of the public record, as well as undisputedly authentic documents if the complainant's claims are based upon these documents." *Mayer v. Belichick*, 605 F.3d 223, 230 (3d Cir. 2010); *see also Buck v. Hampton Twp. Sch. Dist.*, 452 F.3d 256, 260 (3d Cir. 2006); *In re Burlington Coat Factory Securities Litigation*, 114 F.3d 1410, 1426 (3d Cir. 1997).

III. ANALYSIS

The parties make a number of arguments in favor of their respective positions. The Court addresses only arguments relevant to the disposition of TD's motion. As outlined below, the Court denies TD's motion as to Count I because Plaintiff has pleaded sufficient facts to state a claim for violation of the New Jersey Uniform Commercial Code ("UCC") provisions codified at N.J.S.A. § 12A:4A-202 and N.J.S.A. § 12A:4A-203. However, the Court dismisses Counts II and III because these common law claims are displaced by the New Jersey UCC.

A. Count I: Violation of N.J.S.A. § 12A:4A-202 and N.J.S.A. § 12A:4A-203

TD argues the Court should dismiss Count I as a matter of law because Plaintiff admits that TD had security procedures in place, which were effective in the past, and which were followed for the alleged fraudulent transfers. (D.E. No. 4 ("Def. Mov. Br.") at 6).[3] As a result, TD avers that

[3] TD attaches as an exhibit to its motion an account agreement allegedly binding Plaintiff. (*See* D.E. No. 3-2; Def. Mov. Br. at 2–3, 6 & 12). However, Plaintiff did not attach or otherwise referred to any such agreement in its Complaint, and Plaintiff disputes that the exhibit is the agreement it entered with TD when Plaintiff opened the account. (D.E. No. 13 ("Pl. Opp.") 12). Therefore, the Court does not rely on Defendant's exhibit or any of the arguments that rely or quote language from it. *Cf. Mayer*, 605 F.3d at 230.

under the New Jersey UCC the risk of loss shifted to Plaintiff and TD is not liable for the loss. (Def. Mov. Br. at 7).

Plaintiff counters that it has sufficiently alleged that that TD's security procedures were not "commercially reasonable" as required by N.J.S.A. § 12A:4A-202. (Pl. Opp. at 9). Particularly, Plaintiff argues that while the determination of commercial reasonableness is a question of law, it requires consideration of fact-sensitive inquiries which are not appropriate at the motion to dismiss stage. (*Id.* at 10). Additionally, Plaintiff argues that even if TD's security measures were commercially reasonable, Plaintiff has sufficiently alleged that the bank failed prove that "it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer. . . ." (*Id.* at 14).

N.J.S.A. § 12A:4A-202(2) provides that the customer will be liable for an alleged fraudulent transfer if the bank and customer have agreed upon "a security procedure to verify the authenticity of payment orders" that is commercially reasonable and "the bank proves that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer. . . ." Whether a bank's security procedure is commercially reasonable is an issue of law for the Court to determine. N.J.S.A. § 12:4A-202(3). The comments to Article 4A-203 illustrate a desire to define commercial reasonableness based on the facts of each case. *See* N.J.S.A. § 12A:4A-203 cmt. 4. There is very little jurisprudence discussing commercially reasonable security procedures in the context of UCC Section 202. Therefore, the Court is guided primarily by the language of N.J.S.A. § 12A:4A-202 and standard industry practice.

According to the official comments the purpose of the statute, as it pertains to electronic transfers, is to authenticate the identity of the individual who sends the payment order as well as to prevent mistakes. N.J.S.A. § 12A:4A-203 cmt. 4. The Federal Financial Institutions Examinations

Council ("FFIEC")[4] issued specific guidance to banks for adopting security measures to avoid fraudulent transfers. *See* FFIEC, *Authentication in an Internet Banking Environment* (Oct. 12, 2005), *available at* https://www.ffiec.gov/pdf/authentication_guidance.pdf (hereinafter "FFIEC Guidelines"). The FFIEC Guidelines were intended to aid financial institutions in "evaluating and implementing authentication systems and practices whether they are provided internally or by a service provider." *Id.* at 1. The FFIEC recommends that modern banking security procedures involve two-factor authentication selected from three types of factors: (i) something the user knows (*e.g.*, PIN or security question answer); (ii) something the user has (*e.g.*, card or device); (iii) and something the user is (*e.g.*, biometrics). *Id.* at 3. Several sister courts in jurisdictions that have adopted very similar language to New Jersey's UCC section 202 have applied the FFIEC Guidelines when determining the commercial reasonableness of a bank's security procedures. *See, e.g., Choice Escrow and Land Title, LLC v. BancorpSouth Bank*, 754 F.3d 611, 619– 20 (8th Cir. 2014); *Patco Const. Co., Inc. v. People's United Bank*, 684 F.3d 197, 201 (1st Cir. 2012).

As a threshold matter, the Court disagrees with Plaintiff's argument that the determination of commercial reasonableness is not appropriate at the motion to dismiss stage. While under the statute the determination of commercial reasonableness will depend on the facts of each case, N.J.S.A. § 12A:4A-203 cmt. 4, that does not prevent the Court from making a legal determination based on the facts as alleged by the Complaint. After all, the legal question at the motion to dismiss stage is whether, taking all the facts as alleged by Plaintiff to be true, the Complaint shows that Plaintiff has stated a claim for which relief can be granted. *See Iqbal*, 556 U.S. at 678. Answering that question at this stage does not require the Court to look beyond the facts alleged in the Complaint and the documents that are integral to the Complaint.

[4] The FFIEC is an interagency body created by Congressional statute and charged with "establish[ing] uniform principles and standards and report forms for the examination of financial institutions which shall be applied by the Federal financial institutions regulatory agencies." 12 U.S.C. § 3305(a).

Here, Plaintiff concedes that TD had various security procedures in place and that these procedures effectively barred access to the online accounts on previous occasions. (*See* Pl. Opp. at 4). Plaintiff describes at least three protocols implemented by TD for the purpose of securing the account. First, both representatives for Plaintiff were "provided with independent login information to access the online banking system." (Compl. ¶ 10). Second, Vajinepalli and Dave selected independent security questions and answers that were to be used to identify themselves for the purpose of accessing the account. (*Id.* ¶ 11). Both the login information and security questions constitute "something the user knows." *See* FFIEC Guidelines at 3. Third, Plaintiff's account was configured to lock out a user if a login was attempted from an unrecognized computer, requiring Plaintiff's representatives to call TD and provide corporate information and security question answers to regain access. (Compl. ¶ 14). The unfamiliar device lockout constitutes "something the user has," i.e. a familiar computer. *See* FFIEC Guidelines at 3. Accordingly, the Court finds for purposes of the current motion that, as alleged by the Complaint, TD's implemented two-factor authentication procedure is commercially reasonable.

The risk of a fraudulent payment order remains with TD, however, unless TD "proves that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer. . . ." N.J.S.A § 12A:4A-202(2). This is a question of fact. N.J.S.A. § 12A:4A-203 cmt. 4. The code defines good faith as "honesty in fact and the observance of reasonable commercial standards of fair dealing." N.J.S.A. § 12A:1-201(20). "This two-pronged definition has both a subjective component—honesty in fact—and an objective component—the observance of reasonable commercial standards of fair dealing." *BancorpSouth Bank*, 754 F.3d at 622. The subjective prong concerns whether the bank accepted the payment order honestly. *See id.* at 623. The objective prong concerns whether the bank accepted the payment order in accordance with the security procedures "in a way that reflects the parties' reasonable expectations

as to how those procedures will operate." *Id.* Thus, Defendant must show that its employees accepted and executed the payment orders in a way that comported with Plaintiff's "reasonable expectations, as established by reasonable commercial standards of fair dealing." *Id.*[5]

Plaintiff notes that on previous occasions when Vajinepalli attempted to access the account from an unfamiliar computer, the bank's security procedures blocked access to the account before any transfers were made. (Compl. ¶ 14; Pl. Opp. at 13–14). Therefore, this effective response is the foundation upon which Plaintiff's expectations rest. Plaintiff claims that TD failed to act with this previously-demonstrated effectiveness. (Pl. Opp. at 13–14). To support this claim, Plaintiff asserts among other things that an unauthorized user was able to access the account using Dave's information "from a different computer" and made several large transfers, and TD failed to promptly recognize this activity and lock the account as it had previously done. (Compl. ¶ 15). At its core, Plaintiff essentially argues that the unfamiliar device lockout procedure failed to stop an individual from logging into the account on an unfamiliar device.

TD argues that the "Complaint admits that the transfers initiated from Dave's user login" and that the security procedure verified the transfers. (Def. Mov. Br. at 7). As such, TD argues that the "only reasonable inference to draw from [these] allegations is that" someone used Dave's login information on his own "known" computer to initiate the transfers; i.e. that this was an "inside job." (*Id.*). But this ignores that at the motion to dismiss stage the Court must draw all reasonable inferences in favor of Plaintiff. *See Malleus*, 641 F.3d at 563. Additionally, TD's argument ignores that TD apparently attempted to contact Dave to confirm the transfers, and ultimately locked Dave's account, because TD *suspected* that the activity was fraudulent. (Def. Mov. Br. at 3; Compl. ¶ 18 & 26–27).

[5] Though "there may be some evidentiary overlap" between evaluating the commercial reasonableness of the security procedure and the bank's compliance, "the commercial reasonableness inquiry concerns the *adequacy* of a bank's security procedures, [whereas] the objective good faith inquiry" concerns the manner in which the bank complied or acted in accordance with the implemented security procedure. *BancorpSouth Bank*, 754 F.3d at 623.

Thus, taking the Complaint's factual allegations as true and drawing all reasonable inferences in favor of Plaintiff, as the Court must do, the inference can be drawn that TD failed to prevent an unauthorized individual from accessing the account on an unknown computer, and that TD permitted these transfers to go through *despite* being unable to confirm their authenticity with Dave and *despite* suspicions that they were fraudulent. (*See* Compl. ¶ 18 & 26–27). As such, Plaintiff has sufficiently pleaded that TD failed to accept the payment orders in good faith and in compliance with the security procedure. Therefore, the Court finds that Plaintiff's Article 4A-202 claim is sufficiently well-pled and denies TD's motion to dismiss Count I.[6]

B. Common Law Clams

TD argues that New Jersey's adoption of the above UCC provisions displaces the common law negligence claim in Count II and the fiduciary duty claim in Count III. (Def. Mov. Br. at 8). Plaintiff counters that upon creation of the account, TD "assumed a duty to use reasonable care to keep Plaintiff's [a]ccount information private and secure," and that by investigating the transfers TD "assumed a duty to assist Plaintiff in the recovery of the funds stolen from its Account." (Compl. ¶¶ 42–43; *see also* Pl. Opp. at 18). In reply, TD avers that "the facts pled support displacement of the common law claims by the UCC" and that in any event, Plaintiff's does not allege any facts supporting creating a special relationship. (D.E. No. 14 at 7).

---

[6] Even assuming the transfers were valid under Article 4A-202, the Court finds that Plaintiff has sufficiently pleaded facts to support its claim under Article 4A-203. Article 4A-203 provides an exception to Article 4A-202 in which the customer may shift the loss to the bank upon proof that he is not responsible for compromising of the confidential access information. N.J.S.A. § 12A:4A-203 cmt. 5. New Jersey law places the burden of "safeguard[ing] confidential security information and access to transmitting facilities" on the customer. *Id.* at cmt. 4. The parties agree that the alleged fraudulent transfers were initiated using Dave's confidential login credentials. (Compl. ¶ 15). Thus, it appears that Plaintiff failed to meet its burden of safeguarding Dave's login credentials. But, as the exception allows, Plaintiff is permitted to rebut this apparent failure with evidence that it or its agents are not responsible for the disclosure of login credentials. N.J.S.A. § 12A:4A-203(b).

A showing that the credentials were not obtained from the customer will shift the loss to the bank. *Id.* at cmt. 5. Plaintiff avers that Dave's security credentials were not disclosed to anyone, and that even Vajinepalli did not know Dave's login information or security question responses. (Compl. ¶ 12). Thus, for purposes of the present motion, the Court must draw the reasonable inference that Plaintiff was not at fault for the compromising of the confidential login information. As such, the Court finds that the Article 4A-203 claim is sufficiently pled for purposes of the present motion.

The Official Comment to N.J.S.A. 12A:4A–102 "provides that Article 4A comprehensively governs the rights and remedies of parties affected by funds transfers." *ADS Ass'n Grp., Inc. v. Oritani Sav. Bank*, 99 A.3d 345, 359 (N.J. 2014) (citing N.J.S.A. § 12A:4A-102 cmt. 1 ("Consequently, resort to principles of law or equity outside of Article 4A is not appropriate to create rights, duties and liabilities inconsistent with those stated in this Article.")). "[T]he UCC displaces the common law where reliance on the common law would thwart the purposes of the UCC." *Psak, Graziano & Whitelaw v. Fleet Nat. Bank*, 915 A.2d 42, 45 (N.J. Super. Ct. 2007). "Only in very rare instances should a court upset the legislative scheme of loss allocation and permit a common law cause of action." *City Check Cashing, Inc. v. Mfrs. Hanover Trust Co.*, 764 A.2d 411, 416 (N.J. 2001) (quoting *Bank Polska Kasa Opieki v. Pamrapo Sav. Bank*, 909 F. Supp. 948, 956 (D.N.J. 1995)). Thus, "unless the facts establish a special relationship between the parties created by agreement, undertaking or contact, that gives rise to a duty, the sole remedies available are those provided in the [UCC]." *City Check Cashing, Inc. v. Mfrs. Hanover Trust Co.*, 764 A.2d 411, 416 (N.J. 2001).

Under New Jersey law, "[t]he standard deposit agreement between a bank and a depositor does not create a special relationship." *Estate of Paley v. Bank of Am.*, No. A-4391-07T3, 2011 WL 1598974, at *12 (N.J. Super. Ct. App. Div. Apr. 29, 2011) (citing *Globe Motor Car Co. v. First Fid. Bank*, 641 A.2d 1136 (Super. Ct. Law Div. 1993), *aff'd*, 677 A.2d 794 (Super. Ct. App. Div. 1996)). Additionally, the relationship between a bank and a depositor is that of a creditor-debtor. *Estate of Paley v. Bank of Am.*, No. A-4391-07T3, 2011 WL 1598974, at * 12 (N.J. Super. Ct. App. Div. Apr. 29, 2011) (citing *Klemm v. Labor Coop. Nat'l Bank*, 187 A. 640 (N.J. 1936). A creditor-debtor relationship will rarely give rise to a fiduciary duty because the positions of the creditor and the debtor are essentially adversarial. *See Paradise Hotel Corp. v. Bank of Nova Scotia*, 842 F.2d 47, 53 (3d Cir. 1988); *see also United Jersey Bank v. Kensey*, 704 A.2d 38, 44 (N.J. Super. Ct. App. Div. 1997) (noting that "there is no presumed fiduciary relationship between a bank and its customer" because

"their respective positions are essentially adversarial"). As such, common law claims cannot proceed where they would "contravene the provisions of UCC Article 4." *ADS Ass'n Grp., Inc.*, 99 A.3d at 358.

The scope of Article 4A encompasses the very situation alleged by Plaintiff in which "[a] payment order purporting to be that of Customer is received by Receiving Bank but the order was fraudulently transmitted by a person who had no authority to act for Customer." *See* N.J.S.A. § 12A:4A-203 cmt. 2. Plaintiff's attempt to convert TD's conduct (the investigation of the transfers upon receiving a police report and the attempt to process a reversal of the transfers) into a special undertaking giving rise to a special relationship is thus, misplaced. Indeed, the comments to the UCC assume that such an investigation will occur. *See* N.J.S.A. § 12A:4A-203 cmt. 5 ("Because of bank regulation requirements, in this kind of case there will always be a criminal investigation as well as an internal investigation of the bank to determine the probable explanation for the breach of security.").

Further, Plaintiff does not identify any particular facts, or case law for that matter, to show that TD was acting on behalf of anyone else other than for its own self-interest when it undertook those actions. (*See* Pl. Opp.). After all, TD did not act until it had received a police report. And importantly, banks like TD are subject to various regulatory duties including the requirement to prepare Suspicious Activity Reports in connection with suspicious transactions and suspected violations of federal banking law. *See, e.g.*, 12 C.F.R. § 21.11. Additionally, section 12A:4A-204(a) places the risk of loss on the bank when there is a violation of section 12A:4A-202 or section 12A:4A-203. N.J.S.A. § 12A:4A-204 cmt. 1 ("Subsection (a) of Section 4A-204 states that the bank must recredit the account or refund payment to the extent the bank is not entitled to enforce payment.").

Therefore, Plaintiff's allegations are insufficient to overcome the "heavy presumption" that a creditor-debtor relationship like the one at issue here does not give rise to a special relationship.

Galayda v. Wachovia Mortg., FSB, No. 10-1065, 2010 WL 5392743, at *17 (D.N.J. Dec. 22, 2010). Plainly, Article 4A provides a comprehensive remedy to address Plaintiff's injury arising out of the alleged fraudulent transfers, and to allow Plaintiff's common law claims to go forward in the absent of such a special relationship would be to allow Plaintiff to sidestep the "careful and delicate" scheme of loss allocation contemplated and expressed by the legislature. *See ADS Assocs. Grp., Inc.*, 99 A.3d at 361 ("In Article 4A, the Legislature has treated electronic funds transfers as *a distinct category* of transactions governed by special rules, and has carefully limited the liability of banks to refund money transferred in accordance with a payment order that the customer has not authorized."); *Girard Bank v. Mount Holly State Bank*, 474 F.Supp. 1225, 1239 (D.N.J. 1979) ("Courts should be hesitant to improvise new remedies outside the already intricate scheme of Articles 3 and 4"); *see also New Jersey Bank, N.A. v. Bradford Securities Operations, Inc.*, 690 *F*.2d 339, 345 (3d Cir. 1982) (holding that a common-law tort action is barred where Article 8 provides a "comprehensive remedy").

For these reasons, the Court dismisses Counts II and III *with prejudice.*

IV. CONCLUSION

For the foregoing reasons, the Court DENIES TD's motion to dismiss as to Count I and GRANTS TD's motion to dismiss as to Counts II and III *with prejudice*. An appropriate Order accompanies this Opinion.

s/Esther Salas
Esther Salas, U.S.D.J.