

Docket No. AAN-CV-18-6029468 S

JUDICIAL DISTRICT
SUPERIOR COURT
MILFORD

2021 OCT 26 PM 12:01

PRECISION COMPUTER
SERVICES, INC.

v.

NEWTOWN SAVINGS BANK

:
:
:
:
:
:
:

SUPERIOR COURT

JUDICIAL DISTRICT OF
ANSONIA-MILFORD AT DERBY

OCTOBER 26, 2021

MEMORANDUM OF DECISION
RE CROSS MOTIONS FOR SUMMARY JUDGMENT (Nos. 121 & 124)

STATEMENT OF THE CASE

This action involves monetary losses sustained by the plaintiff as a result of a wire transfer obtained by fraud. At the heart of the parties’ cross motions for summary judgment—and at the center of this litigation—“is the question of who should bear the risk of loss when a wire transfer is fraudulently [procured] by a [third party] unconnected to either the issuing bank or its customer.” *Choice Escrow & Land Title, LLC v. BancorpSouth Bank*, United States District Court, Docket No. 10-03531-CV-S-JTM (W.D. Mo. March 18, 2013), *aff’d in part and rev’d in part*, 754 F.3d 611 (8th Cir. 2014).

The following facts are undisputed unless otherwise indicated. The plaintiff, Precision Computer Services, Inc., is a Shelton, Connecticut based company engaged in the business of reselling computer related goods and services. The plaintiff is owned by Michael FitzSimons and his wife, Irene FitzSimons. Michael FitzSimons also serves as the plaintiff’s vice president.

The defendant, Newtown Savings Bank, is a Connecticut bank having a principal location in Newtown, Connecticut. In 2017, and for some years prior, the plaintiff was a customer of the defendant.

The Wire Transfer Agreement

In March of 2017, the parties executed and entered into a written contract entitled, “WIRE TRANSFER AGREEMENT” (agreement), which was drafted by the defendant. The agreement defines the plaintiff as “Customer” and the defendant as “Financial Institution.” Pertinent to the resolution of the present motions are the following provisions of the agreement:

“Customer and Financial Institution agree as follows:

“1. Financial Institution is authorized to debit the account or accounts designated by Customer for payment of transfer requests. Customer’s transfer requests may involve any one or more of the following:

* * *

“b. the transfer of funds from any designated account with Financial Institution to a third party or account of a third party whether such third party accounts are maintained with Financial Institution or any other financial institution.

“There are no restrictions or limitations on the amounts that may be ordered or requested, or on the location or address of the beneficiary, unless Customer gives Financial Institution written instructions specifying otherwise and agreed to in writing by Financial Institution.”

The plaintiff’s “Operating Account” is listed as the account that can be accessed for payment of transfer requests under the agreement. In addition, Michael FitzSimons, Irene FitzSimons, and Jennifer Atkinson are listed as the individuals “authorized to issue payment orders to the Financial Institution under this [a]greement”¹ According to the agreement, “[a]ny one of the authorized originators may issue a payment order on [the Operating Account].”

¹ Under the agreement, Atkinson’s right to initiate a payment order was subject to a \$250,000 limit. By contrast, Michael and Irene FitzSimons were not subject to any monetary ceiling for originating payment orders.

Thereafter, the agreement lists the same individuals—Michael FitzSimnos, Irene FitzSimons, and Jennifer Atkinson—as persons authorized to *confirm* payment orders. The agreement provides that these individuals “are authorized to receive calls from the Financial Institution in accordance with paragraphs 5 and 9 of this [a]greement to confirm payment orders transmitted to the Financial Institution. To confirm a payment order, the Financial Institution may call any person named . . . *except the person who issued the payment order.*” (Emphasis added.) Thus, under the foregoing protocol, either Michael FitzSimons or Irene FitzSimons had to originate or confirm any wire transfer on behalf of the plaintiff.

The agreement contains a series of numbered “ADDITIONAL PROVISIONS,” including Section 9, which reads, in part, as follows:

“Financial Institution and Customer agree that the following security procedures are a commercially reasonable method of providing security against unauthorized Payment Orders:

“a. Individuals Authorized to Originate shall issue wire transfer requests to the Financial Institution; and

“b. Financial Institution reserves the right to call on an individual Authorized to Confirm to confirm a transfer request in any amount, although Financial Institution is not obliged to do so. If confirmation cannot be obtained to Financial Institution’s satisfaction, Financial Institution reserves the right to refuse to honor the wire transfer.

“Financial Institution shall have no responsibility to verify the identity of a person identifying himself or herself as the individual authorized to receive the call back other than to verify that the name given by such person corresponds to one of those previously specified to Financial Institution, provided that Customer designates such individuals. If Financial Institution attempts to verify authorization and for any reason is not satisfied that the transfer request was

issued by an Individual Authorized to Originate or confirmed by an individual Authorized to Confirm, Financial Institution may refuse to execute the transfer request. In so refusing, Financial Institute shall not incur any liability whatsoever”

Section 10 reads as follows: “Financial Institution and Customer agree that transfer requests received by Financial Institution are effective as the transfer request of Customer, whether or not authorized, if Financial Institution accepted the transfer request in compliance with the above security procedures.”

The agreement was signed by Michael FitzSimons and Irene FitzSimons on behalf of the plaintiff. The agreement was executed by Ryan Storms on behalf of the defendant. At the time the parties entered into the agreement, and on the date of the incident in question, Storms was an assistant vice president and branch manager of the defendant.

The Wire Transfer Fraud

On June 14, 2017, an email communication from an actor purporting to be Michael FitzSimons was sent to Storms, on which Atkinson was copied, with a subject line reading, “Payment,” with an attachment entitled, “PCS Invoice.” (First email). The first email reads, in part: “Hi Ryan, Please process the attached by wire transfer, call Jennifer [i]f you have any questions. Thanks.”

Attached to the first email is an invoice from an entity identified as ME-GA INVEST S.R.O. of Budapest, Hungary. The invoice, in the total amount of \$67,560, purports to be for advisory services rendered by the sender, more specifically, for “legal services, assistance and strategic advice rendered from January, 2017 through to date in particular related to legal and tax advice to PCS.”

Atkinson responded by a responsive email reading, in part, “Yes, I will have [Storms] initiate the wire. You will need to authorize as well.” Thereafter, the actor impersonating Michael FitzSimons sent another email to Atkinson and Storms, stating, “Please process the attached by wire transfer, call Jennifer if you have any questions. Thanks.”

The emails sent to Storms show that they originated from a sender whose email address is “mfitzsimons@precisiongroup.com.” Michael Fitzsimons’ actual email address is “mfitzsimons@precisiongroup.com.” The fraudulent actor mislead Storms and Atkinson by substituting the letter “q” for the letter “g,” which letters resemble closely one another in the typeface used for the email communication. It is undisputed that substitution of the letter “q” for the letter “g” in Mr. FitzSimons’ email address was visible to Storms and Atkinson. Storms and Atkinson failed to detect that the email was fraudulent and the defendant processed the wire transfer to a bank account in Hungary in the amount of \$67,560.

Wire Transfer Fraud Prevention

The United States Department of the Treasury maintains a financial crimes enforcement network known as FinCEN, which issues advisories to financial institutions such as the defendant. In June, 2016, the defendant monitored advisories from FinCEN and reviewed such advisories promptly after they were issued.

According to the uncontested portions of the affidavit of plaintiff’s expert—Lance James, an information security specialist—this case involves a fraudulent wire transfer in which an imposter employed a character substitution fraud to “spoof” the email address of Michael FitzSimons, leading to a transfer of the plaintiff’s funds to Hungary. By June of 2017, the existence of this type of fraud was well known in the banking industry.

On September 6, 2016, FinCEN issued an advisory to financial institutions concerning “E-Mail Compromise Fraud Schemes.” The advisory reads, in part, that FinCEN “is issuing this advisory to help financial institutions guard against a growing number of e-mail fraud schemes, in which criminals misappropriate funds by deceiving financial institutions and their customers into conducting wire transfers. This advisory . . . provides red flags . . . that financial institutions may use to identify and prevent such e-mail fraud schemes.” The FinCEN advisory refers to several “Business E-Mail Compromise (BEC) Schemes,” including where “[c]riminals seek to access unlawfully the e-mail accounts of a company’s executives or employees to . . . [m]islead a company employee into submitting fraudulent transaction instructions to the company’s financial institution by impersonating . . . a company executive to authorize or order payment through seemingly legitimate internal e-mails.”

One of the “red flags” referred to in the FinCEN advisory involves “[t]ransaction instructions originat[ing] from an e-mail account *closely resembling* a known customer’s e-mail account; however, the e-mail address has been slightly altered by adding, changing, or deleting one or more characters.” (Emphasis added.) This is precisely what occurred on June 14, 2017.

According to James’ uncontested averment, the FinCEN guidance describes a standard, consistent with many other cybersecurity standards, including the Federal Financial Institutions Examination Council (FFIEC) guidelines. Further according to James, by June of 2017, it was an industry standard for financial institutions to detect character substitution frauds by training employees to spot them and to refrain from processing wire transfers which are requested by fraudsters using this technique. Character substitution frauds are one of the easiest types of fraud for a person to spot with minimal training, as it only requires the recipient to look at the email address of the purported sender. The FinCEN Guidance also notes that emails directing transfers

to foreign countries raise a red flag for fraud. Cyber security standards (which cover the banking industry) make clear that Hungary is a known destination of fraudulent transfers, and the defendant should have been even more careful in the case of the fraud at issue here. The defendant did not have in place other security methods that would have discovered the fraudulent nature of the emails that led to the plaintiff's loss. This includes Yellowhammer, which was not configured to cover the system receiving emails from Michael FitzSimons' imposter. Programs like these would have detected that the emails at issue here came from a fraudulent domain. According to James, given that these other measures were not in place, the defendant should have been even more vigilant about looking at email sender addresses to determine whether they were legitimate. Further according to James, if the defendant contends that it could process a wire transfer based on Atkinson's approval alone, that would not be commercially reasonable under the circumstances of this case, or generally. If the defendant merely reserved the right to call a second employee of the plaintiff, such as Atkinson, it would not be commercially reasonable. It would also unreasonably deprive the plaintiff of the security it understood it had, which required approval from an originator (not an imposter) and actual involvement in the approval process by either Michael or Irene FitzSimons. In any event, under the circumstances of the wire transfer at issue in this case, the obvious misspellings in the emails from the imposter should have alerted the defendant to the fraud.

The Cross Motions for Summary Judgment

This action was brought initially in five counts, alleging breach of contract (Count I), liability pursuant to General Statutes § 42a-4A-201 et seq. (Article 4A of the Uniform Commercial Code [UCC]) (Count II), negligence (Count III), breach of the implied covenant of good faith and fair dealing (Count IV), and breach of fiduciary duty (Count V). On February 9, 2019, the court

(*Stevens, J.*) struck all the plaintiff's claims, other than Count II, on the grounds that Article 4A of the UCC displaces and preempts all common law claims involving funds transfers that are covered by that article, and further, that the plaintiff's claims in this case were governed by Article 4A (No. 101.20). Following the court's ruling, the plaintiff filed a one-count amended complaint in which it alleged liability pursuant to Article 4A alone (No. 113). In response, the defendant filed an answer with three special defenses, claiming (1) that the payment order at issue was verified pursuant to General Statutes §§ 42a-4A-202 and 42a-4A-203, (2) that the payment order was authorized by the plaintiff and the wire transfer was authorized pursuant to § 42a-4A-202, and (3) that the plaintiff is estopped by the conduct of its authorized agent from denying that the transfer was unauthorized (No. 114). The plaintiff denied these defenses (No. 117).

Thereafter, the plaintiff filed a motion for summary judgment as to liability only, claiming that it is entitled to summary judgment on its UCC claim, and seeking summary judgment on the defendant's special defenses (No. 121). Some weeks later, the defendant filed its own motion for summary judgment, requesting the entry of judgment as a matter of law on the plaintiff's remaining claim (No. 124). Several filings were submitted by the court in connection with these motions (Nos. 125, 126, 127, 128, and 129). Oral argument on the cross motions for summary judgment was held on August 5, 2021.

DISCUSSION

I

“The motion for summary judgment is designed to eliminate the delay and expense [accompanying] . . . a trial when there is no real issue to be tried.” (Internal quotation marks omitted.) *Dowling v. Kielak*, 160 Conn. 14, 16, 273 A.2d 716 (1970). The standard of review applicable to motions for summary judgment is well established in our law. “Practice Book § [17-

49] provides that summary judgment shall be rendered forthwith if the pleadings, affidavits and any other proof submitted show that there is no genuine issue as to any material fact and that the moving party is entitled to summary judgment as a matter of law In deciding a motion for summary judgment, the trial court must view the evidence in the light most favorable to the nonmoving party The party seeking summary judgment has the burden of showing the absence of any genuine issue [of] material facts which, under applicable principles of substantive law, entitle him to a judgment as a matter of law . . . and the party opposing such a motion must provide an evidentiary foundation to demonstrate the existence of a genuine issue of material fact [I]ssue-finding, rather than issue-determination, is the key to the procedure [T]he trial court does not sit as a trier of fact when ruling on a motion for summary judgment [Its] function is not to decide issues of material fact, but rather to determine whether any such issues exist.” (Internal quotation marks omitted.) *Northrup v. Witkowski*, 175 Conn. App. 223, 230–31, 167 A.3d 443 (2017), *aff’d*, 332 Conn. 158, 210 A.3d 29 (2019). “It is not enough for the moving party merely to assert the absence of any disputed factual issue; the moving party is required to bring forward . . . *evidentiary facts*, or *substantial evidence outside the pleadings* to show the absence of any material dispute.” (Emphasis in original; internal quotation marks omitted.) *Doty v. Shawmut Bank*, 58 Conn. App. 427, 430, 755 A.2d 219 (2000). The legal standard applicable to the movant is strict. See *Ramirez v. Health Net of the Northeast, Inc.*, 285 Conn. 1, 11, 938 A.2d 576 (2008) (“courts hold the movant to a strict standard.”); *Anderson v. Gordon, Muir & Foley, LLP*, 108 Conn. App. 410, 416, 949 A.2d 488, cert. denied, 289 Conn. 927, 958 A.2d 156 (2008). “The test is whether a party would be entitled to a directed verdict on the same facts.” (Internal quotation marks omitted.) *Doty v. Shawmut Bank*, *supra*, 58 Conn. App. 431.

In response to a summary judgment motion, “the party opposing summary judgment must substantiate its adverse claim by showing that there is a genuine issue of material fact together with the evidence disclosing the existence of such an issue To oppose a motion for summary judgment successfully, the nonmovant must recite specific facts in accordance with Practice Book . . . §§ 17-45 and 17-46 . . . which contradict those stated in the movant’s affidavits and documents and show that there is a genuine issue [of material fact] for trial. If he does not so respond, summary judgment shall be entered against him.” (Citation omitted; internal quotation marks omitted.) *Id.*, 430. A party opposing the motion “must provide an evidentiary foundation to demonstrate the existence of a genuine issue of material fact.” *Appleton v. Board of Education*, 254 Conn. 205, 209, 757 A.2d 1059 (2000). Mere assertions of fact are insufficient to establish the existence of a material fact and cannot rebut properly presented evidence in support of the motion. See *Maffucci v. Royal Park Ltd. Partnership*, 243 Conn. 552, 554-55, 707 A.2d 15 (1998). “[A] party may not rely on mere speculation or conjecture as to the true nature of the facts to overcome a motion for summary judgment.” (Internal quotation marks omitted.) *Doty v. Shawmut Bank*, *supra*, 58 Conn. App. 430. “The existence of [a] genuine issue of material fact must be demonstrated by counter-affidavits and concrete evidence.” (Internal quotation marks omitted.) *Pion v. Southern New England Telephone Co.*, 44 Conn. App. 657, 663, 691 A.2d 1107 (1997). In the context of a motion for summary judgment, a material fact “[is] a fact which will make a difference in the result of the case” (Internal quotation marks omitted.) *Romprey v. Safeco Ins. Co. of America*, 310 Conn. 304, 313, 77 A.3d 726 (2013).

II

A

i

“Article 4A of the Uniform Commercial Code [UCC] governs fund transfers, otherwise known as wholesale wire transfers, a common form of payment between business and financial institutions.” Annot., 62 A.L.R.6th 1 (2011). “The funds transfer governed by Article 4A is in large part a product of recent and developing technological changes. [Article 4A was developed because there] was no comprehensive body of law—statutory or judicial—that defined the juridical nature of funds transfer or the rights and obligations flowing from payment orders

* * *

“In the drafting of Article 4A, a deliberate decision was made to write on a clean slate and to treat a funds transfer as a unique method of payment to be governed by unique rules that address the particular issues raised by this method of payment. A deliberate decision was also made to use precise and detailed rules to assign responsibility, define behavioral norms, allocate risks and establish limits on liability, rather than to rely on broadly stated, flexible principles.” Conn. Gen. Stat. Ann. § 42a-4A-102 (West 2009), UCC comment, p. 88.

“Recognizing the shortcomings of Article 4 [UCC—Bank Deposits and Collections] and the pastiche of ancillary rules, the American Law Institute and National Conference of Commissioners on Uniform State Laws had been drafting a wire transfer code for more than a decade. Their solution, [was] the new Article 4A” *General Electric Capital Corp. v. Central Bank*, 49 F.3d 280, 282 (7th Cir. 1995). “Article 4A was developed in order to define the rights and obligations associated with payment orders and funds transfers Article 4A sets out standards that banks must follow when a customer makes a request to send money to a recipient.”

(Citation omitted.) *Starbrands Capital, LLC v. Original MW, Inc.*, United States District Court, Docket No. 14-12270-ADB (D. Mass. August 14, 2015). “Whether the risk of loss for an unauthorized wire transfer order falls upon the bank or its customer is governed by [statutes] . . . adopted from Sections 4A-202 and 4A-203 of the [UCC].” *Experi-Metal, Inc. v. Comerica Bank*, United States District Court, Docket No. 09-14890 (E.D. Mich. July 8, 2010). In writing Article 4A, the drafters aimed “to achieve national uniformity, speed, efficiency, certainty, and finality in the funds transfer system.” *Grabowski v. Bank of Boston*, 997 F. Supp. 111, 121 (D. Mass. 1997).

Connecticut adopted Article 4A, entitled, “Uniform Commercial Code—Funds Transfers,” effective January 1, 1991. Public Acts 1991 No. 90-202, § 3. Article 4A is codified at General Statutes § 42a-4A-101 et seq.

ii

“The issue of whether a wire transfer is authorized is governed by section 4A-202 of the [UCC]” *Skyline International Development v. Citibank, F.S.B.*, 302 Ill. App. 3d 79, 83, 706 N.E.2d 942 (Ill. App. 1998). “Under Article 4A, a bank receiving a payment order ordinarily bears the risk of loss of any unauthorized funds transfer The bank may shift the risk of loss to the customer in one of two ways, one of which involves the commercial reasonableness of security procedures and one of which does not First, the bank may show that the ‘payment order received . . . is the authorized order of the person identified as sender if that person authorized the order or is otherwise bound by it under the law of agency.’” (Citation omitted.) *Patco Construction Co., Inc. v. People’s United Bank*, 684 F.3d 197, 208 (1st Cir. 2012); see General Statutes § 42a-4-202 (a). “But, as the Article 4A commentary explains, ‘[i]n a very large percentage of cases covered by Article 4A . . . [c]ommon law concepts of authority of agent to bind principal are not helpful’ because the payment order is transmitted electronically and the bank ‘may be required to

act on the basis of a message that appears on the computer screen' "If the sender of the payment order had no authority to act for the customer, and there are no additional facts on which estoppel might be found, the 'Customer is not liable to pay the order and [the] Bank takes the loss' In such cases, 'these legal principles [of agency] give the receiving bank very little protection The only remedy of [the] Bank is to seek recovery from the person who received payment as beneficiary of the fraudulent order'

* * *

"Accordingly, the drafters provided a second way by which a bank may shift the risk of loss and protect itself whether or not the payment order is authorized." (Citations omitted.) *Patco Construction Co., Inc. v. People's United Bank*, supra, 684 F.3d 208.

The second way is governed by § 42a-4A-202 (b), which, as adopted in Connecticut, provides as follows: "If a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure, a payment order received by the receiving bank is effective as the order of the customer, whether or not authorized, if: (i) the security procedure is a commercially reasonable method of providing security against unauthorized payment orders; and (ii) 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 restricting acceptance of payment orders issued in the name of the customer. The bank is not required to follow an instruction that violates a written agreement with the customer or notice of which is not received at a time and in a manner affording the bank a reasonable opportunity to act on it before the payment order is accepted."

"'Security procedure' means a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending

or cancelling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication. A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices. Comparison of a signature on a payment order or communication with an authorized specimen signature of the customer is not by itself a security procedure.” § 42a-4A-201.

“Commercial reasonableness of a security procedure is a question of law” § 42a-4A-202 (c); see also *Federal Ins. Co. v. Benchmark Bank*, United States District Court, Docket No. 2:17-cv-135 (S.D. Ohio February 11, 2020) (“The issue of commercial reasonableness is a question of law.”); *Experi-Metal, Inc. v. Comerica Bank*, supra, United States District Court, Docket No. 09-14890 (E.D. Mich. July 8, 2010) (“Whether the security procedure that [a sending bank] employed for its wire transfer service was commercially reasonable is a question of law.”). “The purpose of subsection (b) [of § 42a-4A-202] is to encourage banks to institute reasonable safeguards against fraud but not to make them insurers against fraud [A] security procedure that fails to meet prevailing standards of good banking practice applicable to the particular bank should not be held to be commercially reasonable.” Conn. Gen. Stat. Ann. § 42a-4A-203 (West 2009), UCC comment, p. 104.

Section 4A-202 “*compels reimbursement* of unauthorized funds transfers if (1) the authorizing bank nevertheless failed to act in good faith or (2) the security procedure was not commercially reasonable.” (Emphasis added.) *Banco del Austro, S.A. v. Wells Fargo Bank, N.A.*, 215 F. Supp. 3d 302, 305 (S.D.N.Y. 2016). “The UCC defines ‘good faith’ as ‘honesty in fact and the observance of reasonable commercial standards of fair dealing.’ This ‘two-pronged definition,’ which includes both objective and subjective components, ‘ensure[s] that each party

to the contract performs its contractual duties in a way that reflects the reasonable expectations of the other party.’

* * *

“In addition to an assessment of good faith, Section [42a-4A-202 (b)] requires a separate inquiry into whether the agreed-upon security procedure itself was ‘commercially reasonable.’

* * *

“To be sure, the questions whether a bank has adopted a ‘commercially reasonable’ security procedure, and whether the bank observed ‘reasonable commercial standards of fair dealing’ when authorizing specific funds transfers, in many cases are redundant.” (Footnotes omitted.) *Id.* “The court must assess whether the agreed-upon security procedure was commercially reasonable *and* whether the authorizing bank’s use of that procedure to authenticate the transfers at issue comported with reasonable commercial standards of fair dealing.” (Emphasis in original.) *Id.*

For the reasons that follow, in this case, neither path permitting a bank to shift the risk of loss to its customer is available to the defendant.

B

i

“Unless the statute designates a provision as one that may not be varied by agreement, the agreement of the parties will trump the provisions of the UCC. In that sense, [i]n an electronic funds transfer case an agreement between the parties may be the most significant source of law in the entire transaction.” (Internal quotation marks omitted.) *Regatos v. North Fork Bank*, 257 F. Supp. 2d 632, 640 (S.D.N.Y. 2003). In this case, the security procedure provided by the agreement required that Michael FitzSimons, Irene FitzSimons, or Atkinson originate a payment order to the

defendant. An authorized individual other than the originator—again, either of the FitzSimonses or Atkinson—had to confirm the order. While Atkinson, an authorized individual, *confirmed* the order, no authorized individual *originated* the payment order at issue—rather, the payment order was originated by an imposter purporting to be Michael FitzSimons. This violates the plain terms of the security procedure established by the agreement and is not an “authorized order,” as contemplated by § 42a-4A-202 (a), of a person identified as the sender, because Michael FitzSimons did not authorize the order.²

Moreover, the defendant cannot shift the loss arising from the fraudulently obtained wire transfer to the plaintiff on the ground that the imposter was the plaintiff’s agent, nor is the plaintiff otherwise bound by the fraudulent order under the law of agency. See § 42a-4A-202 (a) (“A payment order received by the receiving bank is the authorized order of the person identified as sender if that person . . . is otherwise bound by it under the law of agency.”).

As the official comment of the UCC observes, “[i]n a very large percentage of cases covered by Article 4A, transmission of the payment order is made electronically. The receiving bank may be required to act on the basis of a message that appears on a computer screen. Common law concepts of authority of agent to bind principal are not helpful. There is no way of determining the identity or the authority of the person who caused the message to be sent. The receiving bank is not relying on the authority of any particular person to act for the purported sender Rather, the receiving bank relies on a security procedure pursuant to which the authenticity of the message

² To the extent the defendant argues that the security procedure does not require the originator to be one of the three individuals identified as authorized originators under the agreement—and only confirmation by an individual authorized to receive a call back, whose identity the bank is not obligated to verify (agreement, § 9.b.)—the security procedure would be rendered commercially unreasonable, thereby requiring the defendant to refund to the plaintiff the fraudulently obtained funds. See *Banco del Austro, S.A. v. Wells Fargo Bank, N.A.*, supra, 215 F. Supp. 3d 305.

can be 'tested' by various devices which are designed to provide certainty that the message is that of the sender identified in the payment order. In the wire transfer business the concept of 'authorized' is different from that found in agency law. In that business a payment order is treated as the order of the person in whose name it is issued *if it is properly tested pursuant to a security procedure and the order passes the test.*" (Emphasis added.) Conn. Gen. Stat. Ann. § 42a-4A-203 (West 2009), UCC comment, p. 102.

The defendant cannot argue that the imposter was the agent of Michael FitzSimons under any known theory of agency and, as discussed above, the defendant failed to follow the applicable security procedure in that it accepted a payment order from an individual who was not authorized to initiate such an order. Thus, the fraudulent payment order issued in the name of Michael FitzSimons failed to "pass the test" of the parties' security agreement.

In any event, Atkinson's conduct is insufficient as a matter of law to estop the plaintiff from denying the fraudster's apparent authority or agency. Put another way, Atkinson's conduct could not have justifiably been relied upon by the defendant in concluding that the payment order was legitimate. Apparent agency, or agency by estoppel, and apparent authority, require justifiable or good faith reliance by the party claiming the agency. See, e.g., 1 Restatement (Third), Agency, Estoppel to Deny Existence of Agency Relationship § 2.05, comment (c), p. 146 (2006) ("The estoppel stated in this section protects third parties who *justifiably* rely on a belief that an actor is an agent and who act on that belief to their detriment." [Emphasis added.]); *Beckenstein v. Potter & Carrier, Inc.*, 191 Conn. 120, 140-41, 464 A.2d 6 (1983) ("[T]he party seeking to impose liability upon the principal must demonstrate that it acted in good faith based upon the actions or inadvertences of the principal."). As set forth below, the defendant's acceptance of the fraudulent

payment order was not justifiable or in good faith, in that it failed to satisfy reasonable commercial standards of fair dealing.

In light of the foregoing, this case requires application of “[t]he default rule of the UCC . . . that the bank will bear the loss of any unauthorized funds transfer.” *Regatos v. North Fork Bank*, supra, 257 F. Supp. 2d 640. “[T]he bank has an invariable duty to refund payment for a funds transfer that is not effective and unauthorized The customer has an invariable right of refund.” *Id.*, 641. “When a funds transfer is executed in violation of a commercially reasonable security procedure, the bank must refund the amount wrongfully transferred, no matter what.” *Id.*, 642.³

ii

Although the defendant failed to comply with the technical requirements of the security procedure by processing a payment order that was not originated by an authorized individual, thereby entitling the plaintiff to summary judgment on its claim, the defendant’s acceptance of the payment order at issue was also unjustified in that it failed to comply in good faith with the security procedure established by the agreement. “[T]echnical compliance with a security procedure is not enough under Article 4A; instead . . . the bank must abide by its procedures in a way that reflects the parties’ reasonable expectations as to how those procedures will operate.” *Choice Escrow & Land Title, LLC v. BancorpSouth Bank*, supra, 754 F.3d 623.

“[T]he focus of our good faith inquiry is on the aspects of [the] wire transfer that are left to the bank’s discretion [T]o establish that it acted in good faith, [the defendant bank] must

³ “Article 4A of the [UCC] . . . requires a sending bank to reimburse account holders for unauthorized wire transfers.” *Grabowski v. Bank of Boston*, supra, 997 F. Supp. 119. Thus, General Statutes § 42a-4A-204 (a) provides, in part, that “[i]f a receiving bank accepts a payment order issued in the name of its customer as sender which is (i) not authorized and not effective as the order of the customer under section 42a-4A-202, or (ii) not enforceable, in whole or in part, against the customer under section 42a-4A-203, the bank shall refund any payment of the payment order received from the customer to the extent the bank is not entitled to enforce payment”

establish that its employees accepted and executed the . . . payment order in a way that comported with [the plaintiff customer's] reasonable expectations, as established by reasonable commercial standards of fair dealing.” (Citations omitted.) Id.

The defendant's handling of the payment order, from an actor impersonating Michael FitzSimons, failed to comply with reasonable commercial standards of fair dealing and did not comport with the plaintiff's reasonable expectations. In this case, the defendant accepted the payment order issued by the fraudster, in the form of an email bearing a misleading address, as an authentic order, without taking steps sufficient to confirm its authenticity. The plaintiff's expert avers, without contradiction by the defendant, that the defendant's processing of the subject payment order based on Atkinson's confirmatory approval alone would not be commercially reasonable under the circumstances of this case, or generally. The defendant cannot show that such a procedure satisfied its good faith obligations to comport with the plaintiff's reasonable expectations—which included, inter alia, the expectation, enshrined in the agreement, that one of the FitzSimonses would have to originate a payment order subsequently approved by Atkinson.

Furthermore, for most commercial banking customers, contemporary reasonable commercial standards of fair dealing require multifactor authentication. The procedure that the defendant asks the court to sanction is, in essence, a single-factor procedure that would shift liability for fraud to the defendant's customer based on the conduct of Atkinson alone. Multifactor authentication is the lodestar of reasonableness in wire transfer transactions. See, e.g., *All American Siding & Windows, Inc. v. Bank of America, National Assn.*, 367 S.W.3d 490, 501 (Tex. Ct. App. 2012) (security procedure reasonable that required multifactor authentication including use of an ID, passcode, and digital certificate verification); *Filho v. Interaudi Bank*, United States District Court, Docket No. 03 Civ. 4795 (SAS) (S.D.N.Y. April 15, 2008) (three-step security

procedure involving confirmation of fax requests by telephone call to customer, requirement that customer answer security questions, and logging and recording of customer call, held to be commercially reasonable); see also § 42a-4A-201 (“A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices.”).⁴

In this case, the defendant did not use multifactor protocols to determine the authenticity of the fraudulent payment order—it relied solely on Atkinson’s confirmation. The defendant did not call FitzSimons to confirm that the payment order originated from him, require FitzSimons to answer security questions, require the provision of identifying words or numbers, or the use of a passcode. In sum, the defendant failed to authenticate the payment order by having the actor who purported to be FitzSimons prove his identity. As noted by the FFIEC in 2005 in connection with internet banking, “[g]enerally, the way to authenticate customers is to have them present some sort of factor to prove their identity. Authentication factors include one or more of the following: Something a person knows—commonly a password or PIN Something a person has—most commonly a physical device referred to as a token Something a person is—most commonly a physical characteristic, such as a fingerprint, voice pattern, hand geometry, or the pattern of veins

⁴ See also FFIEC guidance dated October, 2005, entitled, “Authentication in an Internet Banking Environment”: “The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. . . .

* * *

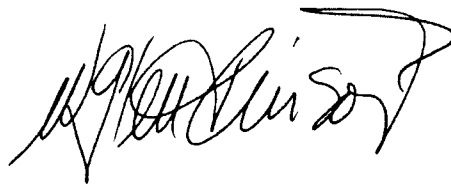
“There are a variety of technologies and methodologies financial institutions can use to authenticate customers. These methods include the use of customer passwords, personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs), USB plug-ins or other types of ‘tokens’, transaction profile scripts, biometric identification, and others.” Federal Financial Institutions Examination Council, “Authentication in an Internet Banking Environment,” (2005), p. 1-2, available at http://www.ffiec.gov/pdf/authentication_guidance.pdf (last visited October 22, 2021).

in the user's eye." (Emphasis omitted.) Federal Financial Institutions Examination Council, "Authentication in an Internet Banking Environment," (2005), p. 7, available at http://www.ffiec.gov/pdf/authentication_guidance.pdf (last visited October 22, 2021).

The defendant failed to accept and execute the payment order in a way that comported with the plaintiff's reasonable expectations, as established by reasonable commercial standards of fair dealing. The plaintiff is entitled to summary judgment on the issue of liability under Count II; the defendant's special defenses fail as a matter of law.

CONCLUSION

For the foregoing reasons, the plaintiff's motion for summary judgment (No. 121) is GRANTED; the defendant's motion for summary judgment (No. 124) is DENIED.

A handwritten signature in black ink, appearing to read "J. Pierson", written in a cursive style.

PIERSON, J.