

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

Case No. 10-23244-CIV-TORRES

ROGER CHAVEZ,

Plaintiff,

v.

MERCANTIL COMMERCEBANK, N.A.,

Defendant.

_____ /

**ORDER ON DEFENDANT'S
MOTION FOR SUMMARY JUDGMENT**

This matter is before the Court on Mercantil Commercebank's, N.A. ("Mercantil" or "the Bank"), Motion for Summary Judgment [D.E. 73] filed July 7, 2011; Roger Chavez's ("Chavez") Response in Opposition [D.E. 83] filed July 18, 2011; and Mercantil's Reply [D.E. 95] filed August 12, 2011. Mercantil's motion will be granted because there is no genuine issue of material fact as to whether the Bank complied in good faith with the commercially reasonable security procedure agreed to by it and Chavez.

I. BACKGROUND

In September of 2002, Chavez opened a bank account at Mercantil. His account was subject to a Funds Transfer Agreement ("FTA") that implemented one of three security procedures offered to Chavez. In this case, Chavez chose the first option contained within Annex 1 of the FTA, which requires the Bank only to verify the

signature of written payment orders when delivered in person. [D.E. 74, Exhibit A] Mercantil states that it also utilized additional security procedures for processing payment orders by following steps set forth in the Customer Services Manual (the “CSM”), including a requirement to verify account and balance information, the existence of an FTA, and identification. [D.E. 79, Exhibit C]

On February 4, 2008, Chavez, a resident of Venezuela, flew to Miami to visit the Bank’s Doral branch because he had not been receiving his monthly bank statements and because he wanted to make a large cash deposit into the account. On February 5, 2008, Chavez returned to make another small cash deposit. On February 6, 2008, Chavez returned his rental car to the rental car facility at the Miami airport at 6:40 AM, and then departed on a flight to Caracas, Venezuela.

On February 7, 2008, the Bank wire transferred \$329,500 from Chavez’s account to the account of a beneficiary in the Dominican Republic. This transfer was made pursuant to a payment order (“subject payment order”) dated February 6, 2008, that bore Chavez’s signature and was delivered in person by a man purporting to be Chavez. No video footage inside or outside of the bank was available because the security cameras were either broken or their recordings were taped over.

The subject payment order was processed by Mercantil’s employee Rossana Gutierrez (“Gutierrez”), who was a “greeter” that occasionally assumed the responsibilities of a Customer Service Representative (“CSR”). In processing the order, Gutierrez confirmed all the information on the subject payment order; the identity of the customer by requesting an identification document, e.g. a passport or Cedula; the sufficiency of funds by checking the account balance; the existence of an FTA; and the

authenticity of the signature. Gutierrez then obtained the written approval from two officers, Talia Pina and Lolita Peroza, that, in accordance with their habit and practice, took extra steps to verify the authenticity of the Payment Order and ensure that Gutierrez had completed her duties. Following this approval, Mercantil completed the order and transferred funds to a beneficiary in the Dominican Republic.

On or about April 14, 2008, while in Venezuela, Chavez checked his account information online and claims that this is when he first learned that his balance was considerably lower than expected. When Chavez contacted Mercantil to inquire about the missing funds, it informed him that \$329,500 was wire transferred from his account. When Chavez's demand that the funds be returned by the bank failed, he filed this suit in order to retrieve the funds.

II. ANALYSIS

A. Summary Judgment Standard

Summary judgment “shall be rendered forthwith if the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law.” Fed. R. Civ. P. 56(c). “The moving party bears the initial burden to show the district court, by reference to materials on file, that there are no genuine issues of material fact that should be decided at trial. Only when that burden is met does the burden shift to the non-moving party to demonstrate that there is indeed a material issue of fact that precludes summary judgment.” *Clark v. Coats & Clark, Inc.*, 929 F.2d 604, 608 (11th Cir. 1991). Rule 56(e) “requires the

nonmoving party to go beyond the pleadings and by her own affidavits, or by the ‘depositions, answers to interrogatories, and admissions on file,’ designate ‘specific facts showing that there is a genuine issue for trial.’” *Celotex Corp. v. Catrett*, 477 U.S. 317, 324 (1986). Thus, the non-moving party “may not rest upon the mere allegations or denials of his pleadings, but . . . must set forth specific facts showing that there is a genuine issue for trial.” *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986).

B. Mercantil’s Security Procedures are “Security Procedures” as defined by Section 670.201 of the Florida Statutes

Florida law requires that a “security procedure” be established by agreement of the customer and the bank. Fla. Stat. § 670.201. This requirement was satisfied when the parties, in their FTA, unambiguously assented to implement the security procedures in Annex 1 of the FTA, requiring all written payment orders to be signed and delivered by an authorized representative “in person or by mail, or by facsimile transmission.” If the payment order was delivered by mail or fax, Mercantil would be required to complete a follow-up phone call for the purpose of verifying the authorized representative’s identity.

In addition to these agreed-upon procedures, clause (iii) of the FTA also permitted the bank to, “at its option,” use other security procedures in addition to those selected by the client that would permit it to verify any payment order or related instruction. For instance, this means that, although Annex 1 of the FTA between Mercantil and Chavez did not explicitly state that a procedure for I.D. verification would be implemented, the use of this procedure was agreed upon according to clause (iii) of the FTA. *See Braga Filho v. Interaudi Bank*, No. 03 Civ. 4795(SAS) 2008 WL

1752693 at *4 (S.D.N.Y. 2008), *aff'd*, 334 Fed. Appx. 381 (2d Cir. 2009) (finding that by signing “explicit agreement” as to the security procedures, the plaintiff agreed to the procedures even if he did not know what they were). Thus, the security procedures at issue in this case were established by agreement between the customer and the bank for the purpose of verifying a payment order pursuant to § 670.201.

Plaintiff’s argument that Mercantil’s security procedures do not fit within § 670.201’s definition of “security procedure” fails. The Advisory Committee Notes of the statute explain that the requirement of “algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar devices” is clearly only contemplated in instances where the fund transfer is not requested *in person*. Indeed, we have not identified, nor has Plaintiff cited, a single case where algorithms or encryptions were ever required by a customer that stood directly in front of the bank’s employee and could simply provide identification.

Plaintiff’s main case on this issue, *Hedged Investment Partners, LP v. Norwest Bank Minnesota, N.A.*, 578 N.W. 2d 765, 774 (Ct. App. Minn. 1998), actually supports the notion that the illustrations of acceptable security procedures in § 670.201 are directed to electronic transactions. Yet this case, unlike *Hedged Investment Partners*, involves a wire transfer request that was made in person. While plaintiff is correct in stating that “the proper inquiry is whether the procedure is the same as, or the functional equivalent of, an algorithm or other code, identifying number, encryption or a call back procedure,” this Court cannot say that the requirement for a customer to present identification in-person does not satisfy such an inquiry. Thus, as a matter

of law, both parties have agreed on security procedures that are within the definition of § 670.201. The inquiry that follows then is whether these security procedures are commercially reasonable for verifying payment orders delivered in person.

C. Mercantil's Security Procedures Were Commercially Reasonable

“The commercial reasonableness of a security procedure is a question of law.”

Fla. Stat. § 670.202(3) (2011). The statute sets out the following factors to be analyzed when determining whether a security procedure is commercially reasonable:

the wishes of the customer expressed to the bank; the circumstances of the customer known to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank; alternative security procedures offered to the customer; and security procedures in general use by customers and receiving banks similarly situated.

Id.

There is very little jurisprudence discussing commercially reasonable security procedures in the context of § 670.202; in fact, there is none to speak of in the Eleventh Circuit. Additionally, the only cases considering UCC Article § 4A-202 involve wire transfers initiated via electronic transmissions. Thus, this case involving the commercial reasonableness of security procedures used for in person wire transfers is largely one of first impression.

Guided primarily by the plain language of the statute, we must determine whether the security procedures implemented by Mercantil were commercially reasonable. These procedures impose a responsibility upon a customer service representative to verify that: (i) all of the necessary information in the payment order,

i.e. account numbers, was provided; (ii) the customer's identity through the request of a form of identification; (iii) the customer's signature compared favorably with one on file; (iv) the customer had an FTA on file; (v) the account balance was sufficient to cover the payment order. The sixth (vi) security procedure required that, for transfers over a threshold amount, the customer service representative processing the transfer obtain approval from two other officers.

It is clear from the Uniform Commercial Code Comment to the statute that the primary purpose of the security procedures is to "authenticate" payment orders, i.e. to verify that the identity of the anonymous person on the other side of an electronic transmission is in fact the person who is authorized to make transfers to and from the account. Fla. Stat. § 670.201 Cmt. 1 (2011). A secondary purpose is to protect against erroneous or mistaken transfers, e.g. transfers that overdraw an account or multiple transmissions of the same payment order. For purposes of deciding the case at hand, this court should look only at the security procedures that go to establishing the authenticity of a payment order because this order was not a mistake; rather it was fraudulently filed by either Chavez or some other party purporting to be Chavez.

Therefore, we should not consider the procedures verifying (i) that the payment order had all the necessary information, (iv) that the customer had an FTA on file, or (v) that the account balance was sufficient to cover the payment order. These "security procedures" are essentially safeguards against mistaken or erroneous transfers and not measures that truly authenticate payment orders by verifying a customer's identity. Similarly, we will not consider the (vi) security procedure that requires two officers to

verify that procedures (i-v) were taken by the customer service representative because, if the steps taken by the customer service representative were not commercially reasonable in the first place, the officers would simply be “rubber-stamping” unsatisfactory procedures. Indeed, the officers sitting behind closed doors had no way of verifying the identity of the person purporting to be Chavez that day by simply reviewing the paperwork completed and submitted by their customer service representative.

The security procedures implemented by Mercantil that are meant to protect against the type of fraudulent transfers that Fla. Stat. § 670.202 is designed to prevent include (ii) an identification (“I.D.”) check and (iii) a signature comparison. Therefore, these are the two security procedures that this Court must find to be commercially reasonable. Both procedures protect against fraudulent transfers as opposed to mistaken or erroneous transfers. It is clear that signature comparison is an approved security procedure under § 670.202 because the statute states “[c]omparison of a signature on a payment order or communication with an authorized specimen signature of the customer is not by itself a security procedure.” (emphasis added). If signature comparison was not an approved procedure, the statute would have plainly said so and would not have bothered to make this distinction.

Therefore, the final and most difficult question is whether a request for a form of identification for the purpose of verifying the customer’s identity is a commercially reasonable security procedure that, when combined with a signature comparison, satisfies the requirements § 670.202(2). Logically, it would seem that there can be no

better safeguard against the fraudulent submission of payment orders than by requiring the customer to present an I.D. that has the customer's picture on it and a name that matches both the name entered on the payment order and the name on the customer's account.

In today's technological world, however, the creation of false identification might be too easy. For example, it is absolutely reasonable to believe that an impersonator could have copied plaintiff's form of identification while superimposing or replacing a picture of the impersonator over the picture of the plaintiff. If a recording or copy of the plaintiff's I.D. was kept within the bank's computer system, the customer sales representative would easily be able to detect this type of fraud because the picture that was superimposed onto the legitimate form of identification could be checked against the picture on file instead, for example, of having the customer service representative ensure that the names match up in all three places.

But because the statute does not require banks to keep a copy of a customer's I.D. on file, and because verifying a customer's identity by checking the customer's I.D. is commercially reasonable, outside of the single example discussed above, a reasonable juror could not find that a signature comparison combined with a request for a form of I.D. is not a commercially reasonable way of protecting the customer from fraudulent transfers, *when the customer submits the payment order in person*. This finding is further supported by the unrebutted opinion of Ms. McGuire, Mercantil's expert, who states that Mercantil's security procedures are the prevailing standards in banking and that they provide a "reliable and secure means of processing funds transfers for its

customers.” See § 670.202(3) (commercial reasonableness is to be determined by considering, *inter alia*, the “security procedures in general use by customers and receiving banks similarly situated”).

Finally, it is important to note that Chavez was offered two alternative security procedures, which options would have offered a higher level of security. These other options were rejected by Chavez, who ultimately selected the security procedures discussed in this case. The fact that the transfer at issue here today was much larger than the only other two transfers Chavez had ever authorized cannot alone create a genuine issue as to the commercial reasonableness of the procedures. Indeed, the Bank had two officers review Ms. Gutierrez’s work before they signed off on it, showing that they recognized the peculiarity of the transfer. However, if someone wants to transfer a large sum of money although the person typically does not, the bank cannot stand in that person’s way if it is presented with the required information, signature, and identification.

In sum, there is no genuine issue of fact in this record to support the contention that the procedures utilized here were not commercially reasonable. And under the statute this analysis is an issue of law for the Court to determine. Therefore, the Court must find on this record that Mercantil’s procedures were commercially reasonable under Fla. Stat. § 670.202.

D. Mercantil Complied with its Security Procedure in Good Faith

The final issue is whether Mercantil acted in good faith in accepting the subject payment order. “Good faith’ means honesty in fact and the observance of reasonable

commercial standards of fair dealing.” Fl. St. § 670.105(1)(f). In order to prove that there was a lack of “good faith,” a party must show that the person was either dishonest or unfair; proof of negligence is not dispositive of a lack of “good faith.” See *Wachovia bank, N.A. v. Federal Reserve Bank of Richmond*, 338 F.3d 318 (4th Cir. 2003) (rejecting claim that bank acted in bad faith in handling item; expert affidavit that bank did not observe commercial standards in handling item did not prove bad faith, which requires proof of dishonesty); *Wooten v. Altamaha Bank and Trust*, 2005 WL 1330775 *3 (S.D. Ga. 2005) (bank’s alleged failure to follow procedures in handling checks failed to show a lack of “honesty in fact”).

As a matter of law, Mercantil acted in good faith in accepting and processing the subject payment order. The record evidence here shows that Gutierrez followed each procedure required by the Bank when processing transfer orders. We cannot accept the notion that Gutierrez is a “serial rule offender” based upon just two violations, and accepts that she requested an identification document pursuant to her training and habit. Additionally, two of the Bank’s officers reviewed Gutierrez’s work and signed off on it.

Most convincingly, the plaintiff has not offered any evidence that would lead a reasonable juror to find that the Bank should have had any reason whatsoever to suspect that the I.D., which was presented by the person purporting to be Chavez, was false. Of course, if Mercantil processed an order despite being presented with an I.D. that had a picture of the person purporting to be Chavez scotch-taped over Chavez’s picture on an otherwise legitimate form of I.D., then the bank would have been

expected to question the authenticity of the I.D. and would have acted dishonestly or recklessly in accepting it as true. But where Chavez considered multiple security options, chose one offering less security, and suffered a security breach even though the Bank followed his instructions, it is difficult to see how the Bank can be required to bear the loss under the law that governs this case. And as tragic as it is for Chavez to have suffered this loss, if indeed he had no complicity in carrying out the scheme, under Florida law he has no remedy against the Bank under these circumstances.

And while the plaintiff does conclusorily state that this transfer was the product of an “inside job” where someone impersonated Chavez and filed the payment order, the evidence supporting this contention is one coincidental encounter between a Mercantil employee and Chavez at a La Carreta restaurant in Miami and a broken video camera on the day of the transaction. Such speculative evidence is not enough to create any issue of fact as to the good faith implementation of commercially reasonable security procedures that indisputably were used in this case.

For these reasons, this Court finds that there is no genuine issue of fact in this record to rebut a finding that Mercantil complied in good faith with the commercially reasonable security procedures it implemented upon instruction by Chavez. Chavez is, of course, not without a remedy against the alleged perpetrator of the fraud who may be identified by tracking the funds at issue. But, as a matter of law, Chavez has no legal recourse against the Bank.

* * *

III. CONCLUSION

For the foregoing reasons, this Court finds that there is no genuine issue of fact or law that the Mercantil's security procedures were within § 670.201's definition of "security procedure," commercially reasonable, and complied with in "good faith." Therefore, the Court has no choice but to grant Mercantil's Motion for Summary Judgment in full.

DONE AND ORDERED in Chambers at Miami, Florida, this 1st day of November, 2011.


EDWIN G. TORRES
United States Magistrate Judge