[PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 11-15804

D.C. Docket No. 1:10-cv-23244-EGT

ROGER CHAVEZ,

Plaintiff - Appellant,

versus

MERCANTIL COMMERCEBANK, N.A.,

Defendant - Appellee.

Appeal from the United States District Court
for the Southern District of Florida

(November 27, 2012)

Before BARKETT and PRYOR, Circuit Judges, and BATTEN,[*] District Judge.

BATTEN, District Judge:

Roger Chavez is a customer of Mercantil Commercebank, N.A. ("the bank"). This case involves an allegedly fraudulent payment order that resulted in the bank's transfer of $329,500 from his account to someone in the Dominican Republic. Chavez sued the bank to recover the $329,500. In response to Chavez's complaint, the bank asserted, inter alia, an affirmative defense premised upon Fla. Stat. § 670.202(2), which relieves a bank of liability for fraudulent payment orders in certain situations. The district court granted the bank's motion for summary judgment and denied Chavez's motion for partial summary judgment on this defense. Chavez appeals.

Generally speaking, under Florida's version of the Uniform Commercial Code ("UCC"), if a bank and its customer agree upon a "security procedure," as that phrase is defined by Fla. Stat. § 670.201, and the procedure is commercially reasonable, a bank is absolved of liability for a fraudulent transfer of the customer's funds if the bank, when processing an order to transfer the customer's funds, follows the security procedure in good faith. See FLA. STAT. §§ 670.201 & 670.202(2). We conclude that the parties' agreed-upon security procedure does not

[*] Honorable Timothy C. Batten, Sr., United States District Judge for the Northern District of Georgia, sitting by designation.

satisfy § 670.201 and consequently § 670.202(2) does not apply. Accordingly, we reverse.

I. BACKGROUND

In September 2002, Chavez, a resident of Venezuela, opened an account with the bank, which is located in Miami, Florida. Chavez contends that when he opened his account, the bank created and maintained an electronic file that had a copy of his passport and that included his address and phone number.

Chavez's account was subject to the bank's funds transfer agreement ("FTA"). Relevant to the current dispute is § 5 of the FTA, which details the security procedure for the account. In general, a security procedure is a procedure that the bank uses when processing payment orders in order to verify the authenticity of the order and to detect any errors in their transmission or content. FLA. STAT. § 670.201. Section 5 of the FTA provides in pertinent part:

> (i) The parties shall comply with the security procedure selected on Annex 1 to this Agreement (the "Security Procedure"). . . .
>
> (ii) The use of the Security Procedure is hereby accepted and authorized by the Client and, unless and until any writing that is signed by the Bank and made a part of this Agreement, the use of the Security Procedure in the manner set forth in this Agreement shall be the sole security procedure required with respect to any Order, and the Client acknowledges and agrees that: (a) the Bank offers various procedures affording differing degrees of security; (b) the Security Procedure is sufficient to protect the interests of the Client in light of the Client's needs, and no special circumstances exist with respect to the Client that would require any other security procedure; and (c) the

> Security Procedure is a method of providing security against unauthorized Orders that is commercially reasonable under the circumstances of the Client and in light of the size, type, frequency and volume of Transfers the Client contemplates undertaking.
>
> (iii) The Bank may execute any Payment Order and act on any other instruction relating to the Payment Order and the Payment Order or instruction shall be effective as the Client's Order, whether or not authorized by the Client and regardless of the actual transmitter, provided that the Bank accepts the Payment Order or instruction in good faith and in compliance with the Security Procedure. At its option, the Bank may use, in addition to the Security Procedure selected by the Client, any other means to verify any Payment Order or related instruction.
>
> (iv) The Client shall preserve the security and confidentiality of the Security Procedure and any related devices or materials, and shall promptly notify the Bank of any suspected compromise of the integrity of the Security Procedure.
>
> (v) The Client acknowledges that the sole purpose of the Security Procedure is to determine the authenticity of Orders, and not to determine their accuracy. . . .

As indicated above, § 5(i) incorporates by reference a document entitled Annex 1, which lists three different options for security procedures that the bank will use when processing a customer's payment orders. Depending on the option, customers can select one option and at most two options.

Chavez selected only the first option, "Written Payment Orders." It provides:

> Written Payment Orders shall be delivered by an Authorized Representative (as defined below) to the Bank either in original form, in person or by mail, or by facsimile transmission. Each written

> Payment Order must be signed by at least one Authorized Representative or, if the terms of the account to which the Payment Order relates (the "Affected Account") require signature by more than one Authorized Representative, by the number of Authorized Representatives so required. Each written Payment Order not delivered to the Bank in person by an Authorized Representative must be confirmed by the Bank by telephone callback to any person who identifies himself or herself to the Bank's satisfaction as one of the Authorized Representatives, (irrespective of whether the terms of the Affected Account require more than one Authorized Representative to sign Payment Orders)….

For Chavez's account, he was the only authorized representative. Thus, for written payment orders delivered in person, Chavez had to sign the payment order.

On February 4, 2008, Chavez flew to Miami and visited the bank's Doral branch. He inquired about why he had not been receiving monthly statements, and he made a large cash deposit. The next day, he returned and made a smaller cash deposit. On February 6, he returned his rental car to the Miami airport around 6:40 a.m. and flew back to Venezuela.

On February 6, someone purporting to be Chavez went to the Doral branch with a written payment order for $329,500. Chavez contends that he had already departed for Venezuela at the time the payment order was delivered to the bank. The order was processed by bank employee Rossana Gutierrez, who was a greeter at the bank, but she occasionally performed the responsibilities of a customer service representative, the type of employee who would typically process a payment order.

According to the district court, Gutierrez confirmed (1) the information on the payment order, (2) the customer's identity via an identification document provided by the customer, (3) the sufficiency of funds in the account, (4) the existence of an FTA for the account, and (5) the authenticity of the signature on the payment order. She then obtained written approval from two branch officers, Talia Pina and Lolita Peroza, who then performed additional steps to verify the authenticity of the payment order. After Pina and Peroza signed off on the order, Gutierrez submitted the payment order for completion, and on February 7 the funds were transferred from Chavez's account to a beneficiary in the Dominican Republic.

The bank's security cameras were not working on the day the payment order was delivered, and Gutierrez did not make a copy of the ID she was shown. As a result, the identity of the person allegedly impersonating Chavez cannot be determined. The bank does not concede that the person presenting the payment order was not in fact Chavez or someone acting on his behalf.

On April 14, 2008, over two months after the payment order was processed, Chavez checked his account online from Venezuela. He claims that this is when he first learned that his balance was considerably lower than expected. He called the bank and allegedly learned for the first time of the February 7 payment order and transfer of the $329,500.

On August 6, 2010, Chavez filed this action against the bank in state court, seeking to recover the $329,500 transferred from his account. The bank timely removed the action to the U.S. District Court for the Southern District of Florida.

The bank filed a motion for summary judgment in which it argued that its third affirmative defense, premised upon the safe-harbor provision in § 202, shifted the risk of loss to Chavez. Chavez filed a motion for partial summary judgment in which he contended that the bank's safe-harbor defense failed as a matter of law.

The district court entered an order granting the bank's motion and denying Chavez's. The district court ruled that the safe-harbor provision in § 202(2) shifted the risk of loss from the bank to Chavez because the parties' agreed-upon security procedure satisfied the statutory definition of a "security procedure" contained in § 201, the bank's security procedure was commercially reasonable, and the bank complied with its security procedure in good faith.

II. STANDARD OF REVIEW

We review de novo a district court's rulings on cross-motions for summary judgment, Owen v. I.C. Sys., Inc., 629 F.3d 1263, 1270 (11th Cir. 2011), and the facts are viewed in the light most favorable to the non-moving party on each motion, Am. Bankers Ins. Grp. v. United States, 408 F.3d 1328, 1331 (11th Cir. 2005). Summary judgment is appropriate when "there is no genuine dispute as to

any material fact and the movant is entitled to judgment as a matter of law." FED. R. CIV. P. 56(a).

III. DISCUSSION

We divide our discussion into three parts. We begin with a brief overview of Article 4A of the UCC, which has been adopted in Florida. We then address the safe-harbor defense and what the bank must show to shift the risk of loss from the bank to Chavez. Lastly, we address what the parties' agreed-upon security procedure actually was and whether that procedure satisfied § 201.

A. Article 4A of the Uniform Commercial Code

As this case involves a payment order, Article 4A of the UCC applies. Given the oftentimes confusing nature of UCC provisions and case law applying them, we give a brief overview of the article.

Article 4A, as adopted in Florida, "governs a specialized method of payment referred to in the Article as a funds transfer but also commonly referred to in the commercial community as a wholesale wire transfer." FLA. STAT. § 670.102 cmt. The article is meant to govern the rights, duties and liabilities of banks and their customers with respect to funds transfers, which may be initiated by a written payment order. Id. § 670.103.

The statutes at issue here are Fla. Stat. §§ 670.201 & 670.202. Section 201 defines "security procedure." Section 202 addresses when a bank can shift the risk of loss to the customer, i.e., the safe-harbor provision.

Ordinarily, the bank receiving a payment order bears the risk of loss of any unauthorized funds transfer. FLA. STAT. § 670.204. However, pursuant to § 202 the bank may shift the risk of loss to the customer by showing one of two things: (1) 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," id. § 670.202(1), or (2) the parties agreed to a security procedure that is commercially reasonable and that the bank followed in good faith, id. § 670.202(2).

Section 202(1) is not before us, as the bank did not rely upon it when filing its motion for summary judgment. The bank moved for summary judgment pursuant to only § 202(2), which provides in pertinent part,

> 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 the security procedure is a commercially reasonable method of providing security against unauthorized payment orders 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 restricting acceptance of payment orders issued in the name of the customer. . . .

Thus, § 202(2) imposes three requirements: (1) the bank and the customer must have agreed on a security procedure for verifying payment orders; (2) the agreed-upon security procedure must be a "commercially reasonable method of providing security against unauthorized payment orders"; and (3) the bank must have accepted the payment order in good faith and in compliance with the security procedure and any relevant written agreement or customer instruction. With respect to the first requirement, the agreed-upon security procedure must satisfy the definition of that term in § 201. With respect to the second requirement, the commercial reasonableness of a security procedure is a question of law for the court. Id. § 670.202(3).

B. Safe Harbor

The bank based its third affirmative defense on § 202(2), asserting that the parties' agreed-upon security procedure was commercially reasonable, it accepted the payment order in good faith, and consequently the safe-harbor provision shifted the risk of loss to Chavez. The district court agreed and granted the bank summary judgment based on this defense.

As stated above, the first element of § 202(2) requires the bank to show that it and Chavez agreed upon a security procedure and that the procedure satisfies the definition of that term in § 201. Consequently, this is where we begin our analysis. It is undisputed that the parties agreed to a security procedure for verifying

payment orders. However, the parties disagree as to the scope of the agreed-upon security procedure. Thus, we first identify the security procedure to which the parties agreed. We then assess whether the agreed-upon procedure satisfies the definition of "security procedure" contained in § 201.

1. The Agreed-Upon Security Procedure

Chavez contends that the district court misinterpreted the FTA and the security procedure identified therein. He asserts that § 5 of the FTA "expressly provides that the sole agreed security procedure is set forth in Annex 1 and shall remain exclusively so unless and until amended by a writing signed by the bank and made a part of the contract." Chavez argues that no such writing exists, and as a result the security procedure is limited to the annex option selected by Chavez, i.e., a written payment order signed and delivered by an authorized representative.

The bank responds that Chavez misconstrues the FTA by ignoring § 5(iii), which provides in part, "At its option, the Bank may use, in addition to the Security Procedure selected by the Client, any other means to verify any Payment Order or related instruction." The bank contends that this language allows it to add additional procedures—which it actually used—and which, when coupled with the security procedure set forth in the annex, combine to provide for a security procedure that satisfies §§ 201 & 202. In other words, the bank asserts that the

agreed-upon security procedure included both the procedure in the annex and the "other means" referenced in § 5(iii).

The district court accepted the bank's position, citing Filho v. Interaudi Bank, No. 03 Civ. 4795(SAS), 2008 WL 1752693, at *4 (S.D.N.Y. Apr. 16, 2008), and held that the agreed-upon security procedure was (1) the procedure in the annex and (2) certain procedures (but not all) the bank, at its option, used when it processed a payment order.

Section 201 defines a security procedure as a "procedure established by agreement of a customer and a receiving bank for the purpose of: (1) Verifying that a payment order or communication amending or canceling a payment order is that of the customer; or (2) Detecting error in the transmission or the content of the payment order or communication." Thus, the security procedure must be one established by agreement of the parties. To determine what Chavez and the bank agreed to, we turn to the FTA and the annex.

Section 5(i) of the FTA provides, "The parties shall comply with the security procedure selected on Annex 1 to the Agreement (the 'Security Procedure')." Thus, the FTA makes the phrase "Security Procedure" a defined term, and through Chavez's selection of option one on the annex, limits its meaning to a written payment order delivered and signed by an authorized representative. The remainder of § 5 refers solely to "the Security Procedure," which further shows

that the parties consistently used the limited term in its defined sense. In addition, § 5(ii) states that "the use of the Security Procedure in the manner set forth in this Agreement shall be the sole security procedure required with respect to any Order." (Emphasis added.) This unambiguous language shows that the parties agreed upon only the security procedure selected by Chavez in the annex.

The district court's holding that the parties agreed in § 5(iii) that the bank could use other procedures, in addition to the one selected by Chavez, to satisfy § 201 was error. Section 5(iii) provides that the bank "may use . . . any other means to verify any Payment Order or related instruction." (Emphasis added.) Relying on Filho, 2008 WL 1752693, at *4, the district court interpreted § 5(iii) as broadening the parties' agreed-upon security procedure to include an identification verification before execution of payment orders. However, the language of § 5 does not support the district court's holding.

As discussed above, §§ 5(i) & (ii) of the FTA explicitly limit the agreed-upon security procedure to the procedure selected by Chavez. Section 5(iii) does not change that. It provides that the bank "may use, in addition to the Security Procedure selected by the Client, any other means" to verify payment orders. This language does not show that the "any other means" is a security procedure. In fact, it shows just the opposite, as § 5(iii) intentionally sets "any other means" apart from the defined "Security Procedure." In addition, the bank—which drafted the

FTA and therefore will have any ambiguities construed against it—defined "the Security Procedure" in § 5(i) and chose not to include within that definition the language in § 5(iii). Consequently, "any other means" is not synonymous with "additional security procedures agreed upon by the parties," as the district court held.

Filho, upon which the district court relied, is inapposite. There, the plaintiffs signed an agreement that explicitly provided that their bank would "select security procedures for accepting instructions that are commercially reasonable," 2008 WL 1752693, at *4, and the court understandably held that in so doing the plaintiffs had agreed that they would be bound by whatever commercially reasonable security procedure the bank selected. The court reasoned that as long as the selected procedure was commercially reasonable, the plaintiffs could not complain about what the bank selected. What was important was that the agreement, signed by the plaintiffs, explicitly granted to the bank the right to select the security procedure.

Section 5(iii) does not do this. Its language that the bank may use "any other means to verify any Payment Order" does not constitute an agreement by Chavez that the bank had the power, at its sole discretion, to select any security procedure as long as the procedure was commercially reasonable. It appears that the bank drafted § 5(iii) to enable but not require it to use other means when processing

payment orders, and Chavez could not be heard to complain if the bank failed to employ those additional security procedures—because the parties never agreed that the bank would use such additional security procedures.[1] As a result, in § 5(ii)(c) the parties agreed that only "the Security Procedure [from the annex] is a method of providing security against unauthorized Orders that is commercially reasonable." Conspicuously absent from this provision is incorporation of the "any other means" provided for in § 5(iii).

The procedure for adding or changing "the Security Procedure" further supports the conclusion that Chavez did not agree in § 5(iii) that the bank could choose whatever security procedures it wanted. Section 5(ii) provides that "unless and until any additional or different procedures are specified in a writing that is signed by [the bank] and made a part of" the FTA, the only required security procedure was the one Chavez selected. It is undisputed that there was no writing modifying the security procedure he selected.

[1] As Filho suggests, the bank could edit the FTA to permit it to use commercially reasonable security procedures without providing additional detail about what those procedures are; then it would be free to choose whatever procedures it wanted to verify payment orders, of course mindful that "a bank that chooses unreasonable procedures does so at its own peril." Filho, 2008 WL 1756293, at *4. See also Patco Constr. Co. v. People's United Bank, No. 2:09-cv-503-DBH, 2011 WL 2174507, at *24 (D. Me. May 27, 2011) (addressing commercial reasonableness first and not addressing customer's argument that it did not agree to security procedures bank used because customer failed to respond to bank's argument that it had in fact agreed "expressly and/or implicitly, to the full panoply of security measures implemented by the Bank."), rev'd on other grounds, Patco Constr. Co. v. People's United Bank, 684 F.3d 197 (1st Cir. 2012).

The bank contends that § 5(ii) applies only to changes to the annex, not to the additional security procedures it could add through § 5(iii). However, even assuming that § 5(iii) actually allows the bank to add additional security procedures, § 5(ii) does not contain any language that supports the limitation the bank proposes. Quite plainly, § 5(ii) provides that it applies to additional and different procedures, and there is nothing therein to suggest that this language excludes the procedures in § 5(iii). In fact, there is nothing in the FTA that exempts § 5(iii) from the amendment process; consequently, if we were to accept the bank's contention that Chavez agreed that the bank could add additional security procedures through § 5(iii) without having to comply with § 5(ii), we would have to negate the amendment process entirely. This is contrary to the basic rules of contract construction.

The official comment to § 201 also shows that the parties did not agree in § 5(iii) that the bank could at its sole discretion use additional security procedures. The comment explains that the "definition of security procedure limits the term to a procedure 'established by agreement of a customer and a receiving bank.' The term does not apply to procedures that the receiving bank may follow unilaterally in processing payment orders." Section 5(iii)'s language that the bank may use "any other means to verify any Payment Order" is akin to the procedures a bank follows in processing payment orders, not procedures established by agreement, as

required by § 201. And, adopting this interpretation gives effect to both the amendment process in § 5(ii) and the language in § 5(iii).

In sum, the parties did not agree in § 5(iii) that the bank could add additional procedures at its discretion; consequently, the only agreed-upon security procedure is the one Chavez selected in the annex. The district court erroneously concluded that the security procedure agreed to by the parties included the procedure selected by Chavez in the annex and the other procedures the bank purportedly added through § 5(iii). However, this conclusion does not end our analysis of whether the bank has satisfied the first element of § 202(2). We must next determine whether the agreed-upon procedure satisfies the definition of "security procedure" in § 201.

2. "Security Procedure" as Defined in § 201

The security procedure selected by Chavez requires only that payment orders delivered in person be in writing and delivered and signed by Chavez. Chavez asserts that this procedure does not satisfy § 201's definition of a security procedure because § 201 explicitly disavows the adequacy of the parties' agreed-upon security procedure. We agree.

Section 201 states that "[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." Consequently, the parties' agreed-upon procedure

must have at least this and one other step in order to qualify as a § 201 "security procedure."

Here, the agreed-upon security procedure does not even require a signature comparison. In fact, the security procedure is silent as to how the bank would verify a payment order delivered in person. For example, there is no requirement that the bank check the identification of the person presenting the payment order to ensure that Chavez was the one presenting the order. Nor does the FTA (or the annex) require a signature comparison or verification that the account even allows payment orders delivered in person. Rather, the agreed-upon procedure imposes requirements only upon Chavez before he can present a payment order to the bank. Because the agreed-upon procedure does not specify what the bank would do to verify a payment order, it cannot satisfy § 201. Consequently, the parties' agreed-upon procedure is not in fact a security procedure as defined by § 201, and the bank failed to shift the risk of loss to Chavez pursuant to § 202(2).

IV. Conclusion

For the foregoing reasons, we hold that the bank and Chavez did not have an agreed-upon security procedure as that term is defined in § 201. Consequently, § 202(2) does not apply to this case, and the bank was not entitled to summary judgment on its affirmative defense premised thereon. The district court's order

granting the bank summary judgment and denying Chavez summary judgment is **REVERSED**.

PRYOR, Circuit Judge, dissenting:

I respectfully dissent. The majority opinion concludes that Chavez and Mercantil Commercebank agreed only to the security procedure defined in section 5(i) of the Funds Transfer Agreement and that section 5(iii) of the Agreement, which permits the Bank also to use "any other means" to verify payment orders, is not part of the parties' agreed upon security procedure. Majority Opinion at 13–14. But that conclusion reflects a strained reading of the Agreement and related provisions of Florida law. Because the Agreement encompassed both the required and discretionary security procedures, which together here were commercially reasonable, and the Bank acted in good faith when it accepted the payment order, I would affirm the judgment in favor of the Bank.

A. The Agreement to Additional Means for Verification of Payment Orders Is Part of the Agreed Security Procedures.

Under Florida law, Chavez bears the risk of loss for the allegedly fraudulent payment order if he agreed to a commercially reasonable security procedure, and the Bank relied on that procedure in good faith when it accepted the payment order. Florida law defines a "security procedure" in relevant part as "a procedure established by agreement of a customer and a receiving bank for the purpose of . . . [v]erifying that a payment order or communication amending or canceling a payment order is that of the customer." Fla. Stat. § 670.201. The "security procedure" under Florida law is not limited to what the parties expressly define as

the "security procedure," but incorporates all procedures agreed upon by the parties to serve that purpose.

These parties agreed to two procedures for verifying the authenticity of payment orders. Section 5(i) provides that "[t]he parties shall comply with the security procedure selected on Annex 1 to this Agreement." And Section 5(iii) provides that "[a]t its option, the Bank may use, in addition to the Security Procedure selected by the Client, any other means to verify any Payment Order or related instruction." These provisions, when read together, establish that Chavez agreed to the use of both the required procedure he selected in Annex 1 and any other security procedures adopted by the Bank, in its discretion, to verify the payment order.

The majority contends that "any other means" is not synonymous with "additional security procedures agreed upon by the parties" because the Agreement had already defined "Security Procedure" in a more limited manner, Majority Opinion at 13–14, but that argument both misreads the Agreement and Florida law. Section 5(iii) provides that, "[a]t its option, the Bank may use, in addition to the Security Procedure selected by the Client, any other means to verify any Payment Order or related instruction." Section 5(iii) reflects that the Bank must use the security procedure selected by the customer in Annex 1 and that the Bank, at its option, may also employ additional security procedures. The use of the words "in

addition" and "any other means" clarify that the additional means envisioned are additional security procedures, as does the location of this provision in section 5, which is titled "Security Procedure." And Florida law defines "Security Procedure" in section 670.201 in language that tracks the text of section 5(iii) of the Agreement. Section 670.201 defines a security procedure as "a procedure established by agreement . . . for the purpose of . . . [v]erifying . . . a payment order," Fla. Stat. § 670.201, and section 5(iii) permits the Bank to use "any other means to verify any Payment Order."

The majority also misreads section 5(ii) of the Agreement. Section 5(ii) provides, in relevant part, that "unless and until any additional or different procedures are specified in a writing that is signed by the Bank and made a part of this Agreement, the use of the Security Procedure in the manner set forth in this Agreement shall be the sole security procedure required with respect to any Order." According to the majority, this language "shows that the parties agreed upon only the security procedure selected by Chavez in the annex." Majority Opinion at 13. But the majority reaches this conclusion by relying on the word "sole" at the expense of the rest of the provision. See id. The text clarifies that the security procedure selected in Annex 1 was the "sole security procedure required with respect to any Order." But that provision does not undermine the discretionary authority granted to the Bank in section 5(iii) to adopt additional

security procedures to verify payment orders. When section 5(ii) is read in the light of section 5(iii), the meaning of the Agreement is evident. Chavez could not require the Bank to adopt "any other means" under the Agreement, but he could also not object to the adoption by the Bank of any other means because he had agreed to that exercise of discretion by the Bank. Contrary to the majority's suggestion, see id. at 16, the amendment process is still meaningful under this reading because Chavez could not gain greater rights to security under the Agreement without the consent of the Bank.

The majority attempts to distinguish Filho v. Interaudi Bank, No. 03 Civ. 4795(SAS), 2008 WL 1752693 (S.D.N.Y. Apr. 16, 2008), on the ground that the agreement in that case "explicitly granted to the bank the right to select the security procedure," Majority Opinion at 14, but the Agreement in this appeal too explicitly granted the bank the right to select an additional security procedure. The only difference between this case and Filho is that the Agreement in this case also established a minimum level of security selected by Chavez that the Bank had to provide to him. The creation of that minimum baseline of security does not override the additional grant of authority to the Bank to use additional means to verify the authenticity of payment orders. To the extent that the Bank adopted additional procedures in this case and those procedures were commercially

reasonable, the Bank may rely on them under section 202. See Fla. Stat. § 670.202(2).

B. The Bank Adopted Commercially Reasonable Procedures.

Although section 5(iii) of the Agreement allowed the Bank to adopt additional security procedures, those procedures had to be commercially reasonable for Chavez to bear the risk of loss under section 202. The Bank performed several security procedures to determine the authenticity of the allegedly fraudulent order: the Bank employee checked the presenter's identification, compared the signature on the written order to the signature on file, verified the accuracy of the account number provided on the order, reviewed the availability of sufficient funds to process the requested order, and confirmed that Chavez had a funds transfer agreement in place for the account.

The security procedures adopted by the Bank for payment orders on Chavez's account were commercially reasonable. The Florida statute instructs us to consider several factors to determine commercial reasonableness:

> The commercial reasonableness of a security procedure is a question of law to be determined by considering 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.

Fla. Stat. § 670.202(3). All of these factors weigh in favor of a finding of commercial reasonableness. The Bank complied with Chavez's requested security procedure and adopted additional procedures for Chavez's protection. Chavez had certified in the Agreement that "the Security Procedure is sufficient to protect the interests of the Client in light of the Client's needs, and no special circumstances exist with respect to the Client that would require any other security procedure." The Bank offered, and Chavez rejected, two different security procedures that would have utilized individual passcodes and test keys. And an expert for the Bank presented undisputed testimony that the security procedures used by the Bank satisfied the prevailing standards in the banking industry.

C. The Bank Complied with Its Security Procedure in Good Faith When It Accepted the Payment Order.

The final requirement for the application of the safe harbor provision of section 202 is that the Bank acted in good faith and in compliance with the agreed-upon security procedures when it accepted the payment order. See Fla. Stat. § 670.202(2). The district court held that "Mercantil acted in good faith in accepting and processing the subject payment order." Chavez did not challenge this holding on appeal. Chavez waived any argument that the Bank did not act in good faith and in compliance with its security procedures when it accepted the order. See United States v. Nealy, 232 F.3d 825, 830 (11th Cir. 2000).

D. Conclusion.

For the foregoing reasons, I respectfully dissent. I would affirm the judgment in favor of the Bank.