United States Court of Appeals
For the Eighth Circuit

No. 13-1879

Choice Escrow and Land Title, LLC

Plaintiff - Appellant

v.

BancorpSouth Bank

Defendant - Appellee

No. 13-1931

Choice Escrow and Land Title, LLC

Plaintiff - Appellee

v.

BancorpSouth Bank

Defendant - Appellant

Appeal from United States District Court
for the Western District of Missouri - Springfield

Submitted: March 11, 2014
Filed: June 11, 2014

Before WOLLMAN, MURPHY, and GRUENDER, Circuit Judges.

WOLLMAN, Circuit Judge.

Internet fraudsters stole $440,000 from a bank account that Choice Escrow and Land Title, LLC (Choice), maintained at BancorpSouth Bank (BancorpSouth). Choice sued BancorpSouth for the lost funds, and BancorpSouth counterclaimed for attorney's fees. The questions presented in this case are thus (1) who should bear the loss of the funds from Choice's account, and (2) who should pay BancorpSouth's attorney's fees. The district court, interpreting Article 4A of the Uniform Commercial Code (U.C.C.), held that Choice should bear the loss of the funds from its account and that BancorpSouth should pay its own attorney's fees. We affirm the district court's loss-of-funds ruling, reverse its dismissal of BancorpSouth's counterclaim, and remand for further proceedings.

I.

This litigation began after an unknown third party accessed Choice's online bank account at BancorpSouth and instructed BancorpSouth to "wire" a large sum of money from Choice's account to a bank account in the Republic of Cypress. To wire money is to transfer it electronically, so named because it was once done via telegram. In a typical wire transfer, a bank's customer transmits instructions to the bank to transfer money from the customer's account to the account of a beneficiary; these instructions are called a payment order. Because the customer is not physically present at the bank, the bank uses security procedures, such as passwords and electronic tokens, to verify that the person sending the payment order is actually the customer. In this case, we confront what happens when those security procedures fail.

Choice is a Missouri company that provides real estate escrow services. When parties to a real estate transaction need a third party to hold money in escrow until closing, they give it to Choice for safekeeping. In 2009, Choice opened a trust account at BancorpSouth for this purpose: when a buyer entrusted funds to Choice, Choice deposited the funds in its account at BancorpSouth and then wired the money to the seller at closing. Choice's employees performed these tasks over the Internet using an online banking platform called InView. BancorpSouth provided Choice with four security measures designed to ensure that Choice's employees, and only Choice's employees, would be able to access Choice's account.

First, BancorpSouth required each InView user to register a unique user id and password. Whenever an employee of one of BancorpSouth's institutional customers wished to access the customer's online bank account, the employee would be prompted to enter this information. Without it, access to the account was impossible.

Second, BancorpSouth installed device authentication software called PassMark. When a customer's employee first registered for InView, PassMark recorded the IP address[1] of the employee's computer as well as information about the computer itself—information relating to, for instance, the computer's operating system, central processing unit, browser, screen, time zone settings, and language settings. Whenever any subsequent user attempted to access InView using that employee's user id and password, PassMark verified that the characteristics of that user's computer were consistent with the information PassMark had recorded about the employee's computer. In this way, PassMark verified that each InView user was accessing InView from a recognized computer. If a user attempted to access InView from an unrecognized computer, the user would be prompted to answer "challenge questions" to verify the user's identity. If the user answered these questions correctly,

[1]IP stands for Internet Protocol. An IP address is a series of numbers that identifies a computer or other device on a network.

the new computer would be added to the list of recognized computers, and the user would be able to access InView.

Third, BancorpSouth allowed its customers to place dollar limits on the daily volume of wire transfer activity from their accounts. For instance, a customer could limit the daily volume of wire transfers to $10,000 per day, in which case any attempt to transfer more than $10,000 in a single day would be automatically denied. Choice declined to place daily transfer limits on its account.

Fourth, BancorpSouth offered its customers a security measure called "dual control." Under this system, when an InView user submitted a payment order, InView would not send the order to the bank immediately; rather, the request would create a "pending" payment order that would appear in a separate queue in InView. To send a pending payment order to the bank, a second authorized user, using a unique user id and password, would have to log in to InView and separately approve the pending payment order. If a customer declined the use of dual control, BancorpSouth required that customer to sign a waiver acknowledging that it was waiving dual control and that it understood the risks associated with using a single-control (i.e., single-user) security system.

Choice declined the use of dual control and signed the requisite waiver. Thus, Choice's account at BancorpSouth was protected only by (1) the user id's and passwords of its employees, and (2) PassMark. Choice authorized two of its employees, Cara Thulin and Brooke Black, to use InView, and it issued each employee a unique user id and password for this purpose.

With these security measures in place, Choice could issue a payment order by taking the following steps: First, either Thulin or Black would access BancorpSouth's website and log in to InView using her user id and password. Second, PassMark would verify that Thulin or Black was accessing InView from a

recognized computer by checking the IP address and other specifications of the computer. If the user was accessing InView from an unrecognized computer, she would be prompted to answer challenge questions. Once the user cleared PassMark, either by using a recognized computer or by correctly answering the challenge questions, she would gain access to Choice's bank account via InView. From there, the user could issue payment orders to BancorpSouth and, as long as Choice had enough funds in its account, those orders would be sent to one of six BancorpSouth employees responsible for routing Choice's payment orders. That employee would then execute the payment order based on the information contained therein, and BancorpSouth would debit the funds from Choice's account and send Choice a fax confirmation of the wire transfer.

In November 2009, Choice received an e-mail from one of its underwriters describing a "phishing" scam in which an unscrupulous person tricks an unsuspecting Internet user into downloading a computer virus, uses the virus to collect the victim's user id's and passwords, and then uses that information to issue fraudulent payment orders to the victim's bank, transferring money from the victim's account to overseas banks beyond the reach of U.S. authorities.[2] Jim Payne, the Director of Business Development at Choice, forwarded the e-mail to BancorpSouth on November 11, 2009, with the following note:

---

[2]As another court has explained:

> Phishing involves an attempt to acquire information such as usernames, passwords, or financial data by a perpetrator masquerading as a legitimate enterprise. Typically, the perpetrator will provide an e-mail or link that directs the victim to enter or update personal information at a phony website that mimics an established, legitimate website which the victim either has used before or perceives to be a safe place to enter information.

Patco Constr. Co. v. People's United Bank, 684 F.3d 197, 204 (1st Cir. 2012).

> Please read the email forwarded from one of our underwriters. They suggest a plan of action that included limiting wires to foreign banks. Can we implement this and to what extent would our liability be if fraudulent wire transfers were to occur?

Ashley Kester of BancorpSouth responded two days later:

> Hi Jim, sorry to just now be responding. I had to do some research to find out if this was possible. We are unable to stop just foreign wires, the solution is dual control. We always recommend dual control on wires. We discussed this when we setup InView and you decided to waive the dual control. Would you like to consider adding it now? This is the best solution, that way if someone in the company is compromised then the hacker would not be able to initiate a wire with just the one user's information.

After Kester described the mechanics of dual control to Payne, Payne e-mailed Kester once again declining the use of dual control:

> Actually I don't think that would be a good procedure for us—lots of times Paige [Payne] is here by herself and that would be really tough unless we all shared pass words.

Sometime after this exchange, a Choice employee fell prey to a phishing attack and contracted a computer virus. This virus gave an unknown third party access to the employee's username and password and allowed the third party to mimic the computer's IP address and other characteristics, rendering InView's password prompts and PassMark's device authentication procedures ineffectual. On March 17, 2010, this third party accessed Choice's online bank account and issued a payment order instructing BancorpSouth to transfer $440,000 from Choice's account to a banking institution in the Republic of Cypress. BancorpSouth accepted and executed the payment order. After attempts to recover the funds failed, Choice sued

BancorpSouth for the lost funds, and BancorpSouth counterclaimed for attorney's fees based on an indemnification agreement that it had executed with Choice.

The district court granted summary judgment to BancorpSouth after concluding that Article 4A of the U.C.C. allocated the risk of loss from the fraudulent payment order to Choice. The court then dismissed BancorpSouth's counterclaim for attorney's fees on the pleadings after concluding that the indemnification agreement at issue conflicted with the provisions of Article 4A and was thus unenforceable.

II.

We review the district court's grant of summary judgment to BancorpSouth *de novo*, viewing the evidence in the light most favorable to Choice. Hill v. Walker, 737 F.3d 1209, 1216 (8th Cir. 2013). 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). The parties agree that Article 4A, which Mississippi enacted in its entirety in 1991, see Miss. Code Ann. § 75-4A-101 *et seq.*, governs this dispute.[3]

Article 4A was drafted in 1989 to account for a dramatic increase in wire transfers between financial institutions and other commercial entities, commonly called wholesale wire transfers to differentiate them from wire transfers by consumers, which are governed by a separate federal statute, see 15 U.S.C. § 1693.

[3]The parties specified in their contracts, and they agree now, that Mississippi law governs this lawsuit. In this opinion, we refer to the relevant section of the Mississippi code rather than the relevant section of the U.C.C. In enacting Article 4A, the Mississippi legislature kept the same numerical identifiers for each provision, except that each identifier is proceeded by a "75-". So, for example, U.C.C. § 4A-202(a) becomes Miss. Code Ann. § 75-4A-202(a). Interested readers may therefore derive the relevant U.C.C. provision by looking at the latter two numerical groupings.

At the time Article 4A was drafted, the total volume of these wholesale transfers exceeded one trillion dollars per day, see U.C.C. Art. 4A Refs. & Annos. prefatory note, yet "there was no comprehensive body of law—statutory or judicial—that defined the juridical nature of a funds transfer or the rights and obligations flowing from payment orders[,]" Miss. Code Ann. § 75-4A-102 cmt. The drafters of Article 4A sought to create a legal framework that balanced these rights and obligations between the bank and its institutional customer. As the Official Comments note:

> Funds transfers involve competing interests—those of the banks that provide funds transfer services and the commercial and financial organizations that use the services, as well as the public interest. These competing interests were represented in the drafting process and they were thoroughly considered. The rules that emerged represent a careful and delicate balancing of those interests and are intended to be the exclusive means of determining the rights, duties and liabilities of the affected parties in any situation covered by particular provisions of the Article.

Id.

One of the liabilities balanced by Article 4A is the risk that a third party will steal a customer's identity and issue a fraudulent payment order to the bank. Generally, the bank bears this risk.[4] Miss. Code Ann. § 75-4A-204. In two circumstances, however, the bank may shift the risk of a fraudulent payment order to the customer. The first is the rare circumstance in which the bank can prove that the customer "authorized the order or is otherwise bound by it under the law of agency." Miss. Code Ann. § 75-4A-202(a). This circumstance is rare because ordinarily the bank has "no way of determining the identity or the authority of the person who

[4]For a more thorough discussion of the different ways in which Article 4A allocates this risk, see Patco Construction Co. v. People's United Bank, 684 F.3d 197, 207-10 (1st Cir. 2012).

caused the message to be sent," and thus "[c]ommon law concepts of authority of agent to bind principal are not helpful" in determining whether a customer is bound by a payment order issued in its name. Miss. Code Ann. § 75-4A-203 cmt. 1.

Because of this inadequacy, Article 4A contemplates a second circumstance in which a customer will bear the risk of a fraudulent payment order. If a bank and its customer agree to implement a security procedure designed to protect themselves against fraud, then the customer will bear the risk of a fraudulent payment order 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.

Miss. Code Ann. § 75-4A-202(b). Article 4A thus permits the bank to take steps to protect itself from liability by implementing commercially reasonable security procedures. If the bank complies with these procedures in good faith and in accordance with the customer's instructions, the customer will bear the risk of loss from a fraudulent payment order. Choice concedes that BancorpSouth complied with its security procedures in accepting the March 17 payment order. Thus, BancorpSouth is entitled to summary judgment if the undisputed facts show (1) that BancorpSouth's security procedures were commercially reasonable, (2) that BancorpSouth accepted the payment order in good faith, and (3) that BancorpSouth accepted the payment order in compliance with Choice's written instructions.

A.

We first consider whether BancorpSouth's security procedures were commercially reasonable. We conclude that they were.

1.

A "security procedure" is a "procedure established by agreement of a customer and a receiving bank for the purpose of . . . verifying that a payment order . . . is that of the customer." Miss. Code Ann. § 75-4A-201. As this definition makes clear, only security measures "established by agreement" are considered "security procedures" for purposes of Article 4A; security measures implemented unilaterally by the bank are irrelevant. See Miss. Code Ann. § 75-4A-201 cmt.

There is one exception to the "established by agreement" rule. If a bank offers its customer a security procedure, and the customer declines to use that procedure and agrees in writing to be bound by payment orders issued in its name and accepted by the bank in accordance with another security procedure, then the customer will bear the risk of loss from a fraudulent payment order if the *declined* procedure was commercially reasonable. Miss. Code Ann. § 75-4A-202(c). To synthesize the rule and its exception: in assessing commercial reasonableness, courts consider (1) security measures that the bank and customer agree to implement, and (2) security measures that the bank offers to the customer but the customer declines, as long as the customer agrees in writing to be bound by payment orders issued in its name in and accepted by the bank in accordance with another procedure.

Our first task is determining which of BancorpSouth's security measures fit this definition. Choice does not dispute that BancorpSouth's password prompts, daily transfer limits, and dual control system are security procedures that we may consider under Article 4A, but it asserts that PassMark does not qualify as a security procedure

because BancorpSouth did not mention PassMark in any of its written contracts with Choice or formally offer Choice the option to use the software.

Notwithstanding the absence of any explicit reference to PassMark in the parties' written contracts, however, there is ample evidence that the parties agreed to implement PassMark. An agreement under the U.C.C. need not be a written contract; rather, an "'[a]greement,' as distinguished from 'contract,' means the bargain of the parties in fact, as found in their language or inferred from other circumstances[.]" Miss. Code Ann. § 75-1-201. All BancorpSouth customers were required to register for PassMark when they signed up for InView. It was thus impossible for any InView user not to know that they were also using PassMark, and any customer that declined to register for PassMark would be unable to use InView. Additionally, the addendum to the Business Services Agreement between Choice and BancorpSouth states that Choice "assumes full responsibility and risk of loss for all transactions made by BancorpSouth . . . in accordance with . . . the procedures set forth in the InView User Manual(s) and Help screens." BancorpSouth posted a digital manual entitled "PassMark Login Security" on the InView portal, so PassMark was incorporated at least implicitly into the parties' written contracts. In light of these facts, we are satisfied that PassMark was "established by agreement" between Choice and BancorpSouth. We thus consider all four of BancorpSouth's security measures—password protection, daily transfer limits, PassMark, and dual control—in determining whether BancorpSouth's security procedures were commercially reasonable.

2.

In making this determination, we consider:

> 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.

Miss. Code Ann. § 75-4A-202. The commercial reasonableness standard is designed "to encourage banks to institute reasonable safeguards against fraud but not to make them insurers against fraud." Miss. Code Ann. § 75-4A-203 cmt. 4. Thus, "[t]he standard is not whether the security procedure is the best available. Rather it is whether the procedure is reasonable for the particular customer and the particular bank, which is a lower standard." Id.

At the threshold, we reject Choice's argument that a commercially reasonable security procedure must include a process whereby a human being manually reviews every payment order submitted to the bank to ensure that no irregularities exist—what Choice calls "transactional analysis." Article 4A never mentions transactional analysis, but Choice argues that because commercial reasonableness depends on the "size, type, and frequency" of a customer's payment orders, a commercially reasonable security procedure must differentiate between payment orders based on these factors. Choice further asserts that transactional analysis is the only way to achieve this differentiation.

This argument misunderstands Article 4A's intended audience. Article 4A does not instruct the bank to consider the "size, type, and frequency" of each payment order it receives in determining if those payment orders are potentially fraudulent; it instructs the court to consider these factors in determining if a bank's security procedure is commercially reasonable—in other words, that the commercial reasonableness of a bank's security procedure depends on whether that procedure is adequate to screen payment orders of the size, type, and frequency normally issued to the bank. Such a procedure might involve "algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices,"

Miss. Code Ann. § 75-4A-201, none of which differentiate between payment orders based on their "size, type, [or] frequency." Yet notwithstanding that "[t]he concept of what is commercially reasonable in each case is flexible," Miss. Code Ann. § 75-4A-203 cmt. 4, Choice argues that even all of these procedures combined would be commercially unreasonable, as none of them involve transactional analysis. This attempt to graft a rigid, foreign standard onto the commercial reasonableness inquiry is at odds with essentially all of Article 4A, and we reject it.

Nor does the record evidence establish that BancorpSouth was required to perform transactional analysis under these specific circumstances. The only person who mentioned transactional analysis was Choice's expert, who stated in his report that transactional analysis "could be a very effective aid in deterring fraudulent payment order transactions" and "would . . . be in line with Article 4A 202 (c)." Neither statement indicates that BancorpSouth's failure to use transactional analysis was commercially unreasonable, and at any rate Choice's expert admitted in his deposition that, under the circumstances of this case, dual control could be a commercially reasonable security procedure. BancorpSouth's Senior Vice President further testified that BancorpSouth conducts tens of thousands of wire transfers on behalf of its roughly 400,000 checking account customers and that reviewing each one of these transactions would be impracticable. Choice has presented no evidence to contradict this testimony and, indeed, has failed to present any evidence tending to show that a genuine question of fact exists as to whether BancorpSouth was required to perform transactional analysis.

Having determined that BancorpSouth was not required to perform transactional analysis, we turn to what it was required to do. We begin at the broadest level of generality, by considering "security procedures in general use by customers and receiving banks similarly situated[,]" Miss. Code Ann. § 75-4A-202. Our primary authority in this endeavor is a 2005 report published by the Federal Financial

Institutions Examination Council (FFIEC)[5] called "Authentication in an Internet Banking Environment," (the Guidance), see Fed. Fin. Insts. Examination Council, Authentication in an Internet Banking Environment (Oct. 12, 2005), available at https://www.ffiec.gov/pdf/authentication_guidance.pdf. The parties agree that the Guidance provides applicable standards of commercial reasonableness in this case.

The Guidance draws a basic distinction between single-factor and multifactor authentication. As the Guidance explains, most modern security procedures involve one or more of the following three factors:

(1) Something the user knows, like a password or PIN;

(2) Something the user has, like an ATM card or smart card; and

(3) Something the user is, like a person with a unique fingerprint or biometric characteristic.

Id. at 3. Security procedures that involve only one of the above three factors, according to the Guidance, are inadequate to safeguard against modern Internet fraud. Accordingly, the Guidance recommends that financial institutions implement security procedures that use two or more of the above factors in combination. An ATM, for instance, uses a multifactor security procedure that requires the user to provide something the user has (an ATM card) as well as something the user knows (a PIN) to use the machine. BancorpSouth's security procedures also used multifactor

[5]The FFIEC is a federal interagency council empowered to "prescribe uniform principles and standards for the Federal examination of financial institutions by the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System, the Federal Home Loan Bank Board, and the National Credit Union Administration and make recommendations to promote uniformity in the supervision of these financial institutions." 12 U.S.C. § 3301.

authentication: to access InView, a BancorpSouth customer had to enter the correct password (something the user knows) and use a recognized computer (something the user has).

Of course, cyber-crime evolves rapidly, and guidance issued in 2005 may become obsolete in subsequent years. The Guidance thus states that banks should "[a]djust, as appropriate, their information security program[s] in light of any relevant changes in technology, the sensitivity of its customer information, and internal or external threats to information." Id. As BancorpSouth's expert acknowledged, during 2009 and 2010, cyber-criminals began using more sophisticated software that could "take on the identity and internet configuration of the victim organization's personnel that were involved in the wire transfer process," emulating the computer's IP address and using the employee's passwords to bypass even multifactor security procedures. This testimony suggests that multifactor authentication alone may have been an inadequate safeguard against Internet fraud perpetrated in 2010.

BancorpSouth responded to this new threat by offering its customers dual control, which dramatically reduces the possibility of such a breach. With dual control in place, a customer's account remains secure even if a third party manages to obtain an employee's password and IP address; to issue a payment order, that third party would have to obtain a second, wholly independent set of identifying information. Phishing scams work because one out of every few thousand recipients of a malicious email will click on a link containing a virus, and the probability that two employees at the same company would fall for the same scam is quite low. Moreover, without a second user's information, any attempt by a third party to issue a payment order would alert the customer to the security breach by creating a pending payment order that no one at the company had authorized.

Accordingly, because BancorpSouth comported with the 2005 Guidance and expanded its security procedures to address security threats that arose after 2005, we

conclude that BancorpSouth's security procedures comported with the standards set by "security procedures in general use by customers and receiving banks similarly situated."

This does not end the inquiry, however: we must also consider whether BancorpSouth's security procedures were suitable for Choice given "the wishes of the customer expressed to the bank" and "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." Miss. Code Ann. § 75-4A-202.

Contrary to Choice's assertion, this does not mean that a bank must always use a different security procedure for each customer. The Official Comment to § 75-4A-203 states that "[a] receiving bank *might* have several security procedures that are designed to meet the varying needs of different customers" (emphasis added), but it does not make this a requirement. If a bank develops a single effective and versatile security procedure, it is not commercially unreasonable for the bank to use that security procedure for the majority of its customers and depart from the procedure only when necessary.

Choice asserts that such a departure was necessary in this case because Choice did not have enough employees on hand to use dual control effectively—in other words, that dual control was commercially unreasonable given the "circumstances of the customer known to the bank" and the "wishes of the customer expressed to the bank." As set forth above, when BancorpSouth offered Choice dual control for the second time, on November 13, 2009, Jim Payne of Choice responded, "Actually, I don't think that would be a good procedure for us—lots of times Paige [Payne] is here by herself and that would be really tough unless we all shared pass words."

Assuming that this statement is true, it does not mean that dual control was any less suitable for Choice than the single-control option Choice ultimately chose to

implement. Paige Payne was not an authorized InView user, and if she was in the office by herself, she would have been unable to issue payment orders regardless of whether Choice had implemented single or dual control.

Perhaps Jim Payne intended in his e-mail to refer to either Thulin or Black, the two Choice employees authorized to use InView, instead of Paige Payne. But both Thulin and Black were full-time employees who were typically in the office during normal business hours. To the extent that Choice needed to issue payment orders outside of these hours, dual control would have been no less suitable for Choice than single control, since neither Black nor Thulin would have been in the office at that time.

Even if only one authorized InView user was in the office at certain times, dual control would not have been a major hindrance on Choice's ability to issue payment orders. Simultaneous approval of a payment order is not required under dual control; one employee may create a pending payment order in the morning, and a second employee may come into the office in the afternoon and confirm the pending payment order. Choice has not argued that it needed to be able to wire money at a moment's notice; indeed, the nature of its business suggests that Choice generally knew beforehand when it needed to wire money to beneficiaries (namely, the date of a real estate closing) and that it could plan accordingly. And even if a quick response time was necessary in some circumstances, Choice could have solved this problem by authorizing employees besides Black and Thulin to use InView.

In short, no genuine dispute of fact exists as to whether BancorpSouth's security procedures were commercially reasonable. Rather, this appears to be a case where "an informed customer refuses a security procedure that is commercially reasonable and suitable for that customer and insists on using a higher-risk procedure because it is more convenient or cheaper[,]" in which case "the customer has voluntarily assumed the risk of failure of the procedure and cannot shift the loss to

the bank." See Miss. Code Ann. § 75-4A-203 cmt. 4. Choice knew that dual control provided a reliable safeguard against Internet fraud, and it explicitly assumed the risks of a lesser procedure notwithstanding the relative ease with which it could have implemented dual control. Accordingly, we conclude that BancorpSouth's security procedures, which included password protection, daily transfer limits, device authentication, and dual control, were commercially reasonable.

B.

The risk of a fraudulent payment order remains with BancorpSouth, however, unless BancorpSouth also "proves that it accepted the [March 17] 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." Miss. Code Ann. § 75-4A-202(b). Choice asserts that BancorpSouth did not accept the payment order in good faith and that it violated Choice's written instructions in doing so. We disagree.

1.

Good faith "means honesty in fact and the observance of reasonable commercial standards of fair dealing." Miss. Code Ann. § 75-1-201(b)(20). This two-pronged definition has both a subjective component—honesty in fact—and an objective component—the observance of reasonable commercial standards of fair dealing. In re Nieves, 648 F.3d 232, 239 (3d Cir. 2011). We are concerned with the latter prong in this case: Choice concedes that BancorpSouth accepted the payment order honestly, but it asserts that BancorpSouth did not observe reasonable commercial standards of fair dealing in doing so.

The U.C.C.'s requirement that parties to a contract abide by reasonable commercial standards of fair dealing—and the good faith doctrine generally—is designed to ensure that each party to the contract performs its contractual duties in a way that reflects the reasonable expectations of the other party. As the Permanent Editorial Board Commentary explains:

> The principal author of the Code, Karl Llewellyn, recognized that parties develop expectations over time against the background of commercial practices and that if commercial law fails to account for those practices, it will cut against the parties' actual expectations. . . . [T]he doctrine of good faith . . . [thus] serves as a directive to protect the reasonable expectations of the contracting parties.

U.C.C. App. II Commentary 10; see also Restatement (Second) of Contracts § 205 cmt. a ("Good faith performance or enforcement of a contract emphasizes faithfulness to an agreed common purpose and consistency with the justified expectations of the other party."). One of the challenges in applying the good faith doctrine in the Article 4A context is the apparent overlap between a bank's compliance with "commercial standards of fair dealing" and its compliance with "commercially reasonable" security procedures. It may appear at first glance that these inquiries are redundant, and some courts have suggested (although not in the Article 4A context) that this is indeed the case. See Watson Coatings, Inc. v. Am. Exp. Travel Related Servs., Inc., 436 F.3d 1036, 1042 (8th Cir. 2006); DBI Architects, P.C. v. Am. Express Travel-Related Servs. Co., 388 F.3d 886, 895 (D.C. Cir. 2004).

But while there may be some evidentiary overlap between the commercial reasonableness of a bank's security procedures and its compliance with reasonable commercial standards of fair dealing, we do not believe that the two inquiries are coextensive. While the commercial reasonableness inquiry concerns the adequacy of a bank's security procedures, the objective good faith inquiry concerns a bank's acceptance of payment orders in accordance with those security procedures. In other

words, technical compliance with a security procedure is not enough under Article 4A; instead, as the above-quoted materials indicate, the bank must abide by its procedures in a way that reflects the parties' reasonable expectations as to how those procedures will operate.

Thus, the focus of our good faith inquiry is on the aspects of wire transfer that are left to the bank's discretion. See Milford-Bennington R. Co., Inc. v. Pan Am Railways, Inc., 695 F.3d 175, 179 (1st Cir. 2012) ("The good-faith obligation limits the parties' discretion in contractual performance."). Where, as here, a bank's security procedures do not depend on the judgment or discretion of its employees, the scope of the good-faith inquiry under Article 4A is correspondingly narrow. The automation of agreed-upon procedures generally ensures that those procedures will operate in a way that is consistent with the customer's expectations, as long as the procedures do not "unreasonably vary from general banking usage"—in other words, as long as they are commercially reasonable. Watson Coatings, 436 F.3d at 1042. We have already determined that BancorpSouth's security procedures were commercially reasonable, and we need not revisit that determination here. Rather, to establish that it acted in good faith, BancorpSouth must establish that its employees accepted and executed the March 17 payment order in a way that comported with Choice's reasonable expectations, as established by reasonable commercial standards of fair dealing.[6]

---

[6]The litigants propose a test for fair dealing first articulated by the Supreme Judicial Court of Maine in Maine Family Federal Credit Union v. Sun Life Assurance Co. of Canada, 727 A.2d 335, 342-43 (Me. 1999). For several reasons, we do not believe the application of the Maine Family test in this case would be appropriate. For one, the Maine Family test has been criticized for conflating fair dealing with due care. See Travelers Cas. & Sur. Co. of Am. v. Wells Fargo Bank N.A., 374 F.3d 521, 527 (7th Cir. 2004); White, Summers, & Hillman, Uniform Commercial Code § 1:10 (6th ed.). For another, the Maine Family test seems tailored to the context of that case, which concerned a holder in due course, and its application in the Article 4A context would distort the balance of rights and obligations that Article 4A attempts to strike between the bank and its institutional customer.

We are satisfied that BancorpSouth has met this burden. Choice was well aware that the only time BancorpSouth employees saw its payment orders was after those orders had already cleared BancorpSouth's security procedures. Choice was also aware that the role of those employees was not to check for any irregularities but to route these payment orders to the correct beneficiaries. Jeff Jaggers, a senior vice president at BancorpSouth, testified that in his thirty years of banking experience it was "normal banking practice" for a bank's employees to route payment orders submitted in compliance with a security procedure without conducting any further review to determine if those payment orders were somehow suspicious.[7] And even if BancorpSouth's employees should have been expected to conduct some common-sense manual review of payment orders—for instance, by flagging a payment order for $10,000,000 from a customer with only $10,000 in its account—the March 17 payment order was not so unusual that it should have raised eyebrows. BancorpSouth provided evidence that the March 17 payment order was not the largest order that Choice had ever submitted and that Choice's wire transfers followed no general pattern and varied in size from a few thousand dollars to a few hundred thousand dollars. In response, Choice asserts that the memo line of the March 17 payment order, which read "invoice:equipment," was inconsistent with Choice's business and with its past practice in issuing payment orders. Choice, of course, is a real estate escrow company with little use for equipment, and the memo line had been filled out in only 13% of Choice's previous payment orders. But the memo line's two-word description does not make the March 17 payment order so suspicious that BancorpSouth acted in bad faith by failing to notice it; if BancorpSouth's employees had to remember the business of each of BancorpSouth's 400,000 clients to ensure that

[7]Choice asserts that, under Federal Rule of Evidence 702, expert testimony is necessary to establish reasonable commercial standards of fair dealing in an industry. But Rule 702 has nothing to do with issues of proof; it merely explains the conditions under which an expert witness may testify. Expert testimony is one way to establish reasonable commercial standards of fair dealing, but it is not the only way. See, e.g., Nanakuli Paving & Rock Co. v. Shell Oil Co., 664 F.2d 772, 784-85 (9th Cir. 1981).

the memo line of each payment order made sense, BancorpSouth would not be in business long. This is not a case where a bank "allow[ed] overdrafts totaling *$5 million* from a single account that usually ha[d] a zero balance." Experi-Metal, Inc. v. Comerica Bank, 2011 WL 2433383, at *14 (E. D. Mich. June 13, 2011). This is a case where a bank promptly executed a payment order that had cleared the bank's commercially reasonable security procedures and that the bank had no independent reason to suspect was fraudulent. Accordingly, we conclude that BancorpSouth has met its burden of establishing beyond genuine factual dispute that it accepted the March 17 payment order in good faith.

2.

The last element BancorpSouth must prove to shift the loss from the March 17 payment order to Choice is that BancorpSouth accepted the payment order in compliance with Choice's instructions. Choice attempts to shortcut the issue by arguing that BancorpSouth admitted in its answer that it had violated Choice's instructions by "Admit[ting]" the following allegation in Choice's complaint:

> 61. Choice by email on or about November 11, 2009, from Jim Payne to Ashley Kester, expressed to BancorpSouth its wish, requirement and/or instruction that BancorpSouth limit transfers to foreign banks.

According to Choice, BancorpSouth's response of "Admit" to this paragraph amounts to an admission that BancorpSouth violated Choice's "wish, requirement, and/or instruction" to limit foreign wire transfers. The merit of this argument depends on how one interprets "and/or." Choice asserts that "and/or" means "and," which is incorrect: "and/or" is an ambiguous phrase that usually means "one or the other or both." See Bryan A. Garner, Garner's Modern American Usage 45 (3d ed. 2009). The natural reading of BancorpSouth's admission is thus that Choice had expressed to

BancorpSouth its "wish, requirement, or instruction, or some combination of the three" that BancorpSouth stop foreign wires. A judicial admission must be deliberate, clear, and unambiguous, see MacDonald v. Gen. Motors Corp., 110 F.3d 337, 340 (6th Cir. 1997); Rowe Int'l, Inc. v. J-B Enterprises, Inc., 647 F.2d 830, 836 (8th Cir. 1981), and Choice's use of the phrase "and/or" in its complaint renders BancorpSouth's subsequent concession anything but.

Turning to the substance of this dispute, we conclude that BancorpSouth did not violate any of Choice's instructions by accepting the March 17 payment order. The only evidence of an instruction is the November 11 e-mail from Jim Payne to Ashley Kester asking if it would be possible to stop foreign wire transfers. Payne himself agreed in his deposition that the e-mail was properly characterized as an "inquir[y]," and when BancorpSouth replied that it was "unable to stop just foreign wires," Choice did not press the issue further. This exchange does not constitute an instruction.

In sum, because BancorpSouth's security procedures were commercially reasonable, because BancorpSouth complied with its security procedures and with Choice's instructions, and because BancorpSouth accepted the March 17 payment order in good faith, the loss of funds from Choice's account falls on Choice.

III.

Finally, we turn to whether BancorpSouth is entitled to attorney's fees based on an indemnification agreement it executed with Choice. The district court dismissed BancorpSouth's counterclaim for attorney's fees on the pleadings after concluding that the indemnification provision in question conflicted with the provisions of Article 4A and was thus unenforceable. We review the dismissal of this counterclaim *de novo*. Levy v. OHL, 477 F.3d 988, 991 (8th Cir. 2007).

The indemnification provision states as follows:

> As long as BancorpSouth has performed as provided in Section 8 above, the Customer shall indemnify and hold BancorpSouth harmless from any and all claims, damages, losses, liabilities, and costs and expenses, including reasonable attorney's fees, which relate in any manner to the Services performed under this Agreement.

"Unless displaced by the particular provisions of the Uniform Commercial Code, the principles of law and equity . . . supplement" the provisions of Article 4A. Miss. Code Ann. § 75-1-103. But Article 4A preempts common law causes of action "in two specific areas: (1) where the common law claims would create rights, duties, or liability inconsistent with [Article 4A]; and (2) where the circumstances giving rise to the common law claims are specifically covered by [Article 4A]." Zengen, Inc. v. Comerica Bank, 158 P.3d 800, 808 (Cal. 2007). The district court, acknowledging that the issue was a "close call," held that the above-quoted indemnification provision would create rights and liabilities that were inconsistent with Article 4A because the provision "could effectively require Choice to pay back to [BancorpSouth] those amounts that [BancorpSouth] might owe to Choice under [Article 4A]." D. Ct. Order of Aug. 30, 2012, at 3. In other words, by requiring Choice to indemnify BancorpSouth for all "damages, losses, [and] liabilities" stemming from a fraudulent payment order, the indemnification provision would frustrate Article 4A's attempts to balance this risk between the bank and its customer.

But the section of the indemnification provision dealing with "damages, losses, [and] liabilities" is not at issue in BancorpSouth's counterclaim. BancorpSouth's counterclaim seeks attorney's fees, not damages stemming from the fraudulent payment order, and Article 4A contains no provision allocating attorney's fees between the bank and its customer in the event of litigation. Although awarding attorney's fees to a bank under an indemnification agreement might reduce a customer's overall recovery against that bank, it would do so for reasons extrinsic to

Article 4A's attempts to balance the risk of loss due to a fraudulent payment order. We thus conclude that the portion of the indemnification provision relating to attorney's fees is not inconsistent with Article 4A and that BancorpSouth may seek attorney's fees from Choice under this provision.[8]

IV.

We affirm the district court's grant of summary judgment to BancorpSouth, reverse the district court's dismissal of BancorpSouth's counterclaim on the pleadings, and remand for further proceedings consistent with this opinion.

---

[8]We have considered, and we now deny, Choice's motion to strike portions of BancorpSouth's appellate brief relating to attorney's fees.