IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF MISSOURI SOUTHERN DIVISION

Choice Escrow and Land Title, LLC,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**Case No. 10-03531-CV-S-JTM**
	)	
BancorpSouth Bank,	)	
	)	
Defendant.	)	

ORDER

In 2010, plaintiff Choice Escrow and Land Title, LLC ("Choice") maintained a trust account with defendant BancorpSouth Bank ("BSB"). On March 17, 2010, BSB received an internet-based request to make a wire transfer of $440,000.00 out of Choice's trust account through BSB's internet wire transfer system. BSB thereafter transferred $440,000 to an intermediary bank [Bank of New York] which then transferred the funds to an institution in the Republic of Cypress, as a beneficiary for an entity identified only as "Brolaw Services, Ltd."

The present litigation ensued with Choice suing BSB, arguing that it "ha[d] never heard of, done business with, or held money in escrow for Brolaw," that it did not initiate, approve, authorize, or ratify the March 17, 2009 wire transfer, and that the wire transfer was fraudulently initiated by an unknown third party. Choice's claims arise under the "Funds Transfers Act" provisions of the Uniform Commercial Code ("UCC") as adopted by Mississippi, MISS. CODE ANN. §§ 75-4A-101, *et seq* (Rev. 2002). Presently pending before the Court is PLAINTIFF'S FIRST MOTION FOR SUMMARY JUDGMENT [Doc. 159], PLAINTIFF'S SECOND MOTION FOR SUMMARY JUDGMENT [Doc. 163], and the MOTION OF DEFENDANT BANCORPSOUTH BANK FOR SUMMARY JUDGMENT [Doc. 160]. The Court will take up the latter motion first.

At the heart of BSB's summary judgment motion – and at the center of the entire litigation – is the question of who should bear the risk of loss when a wire transfer is fraudulently undertaken by a third-party unconnected to either the issuing bank or its customer. With regard to the allocation of such risk, the Funds Transfers provisions of the Uniform Commercial Code ("UCC"), enacted in the State of Mississippi at MISS. CODE ANN. §§ 75-4A-101, *et seq.*,[1] provide guidance. Initially, as a general rule, unless otherwise provided in the UCC, the risk of loss for unauthorized transfers lies with a bank. MISS. CODE ANN. § 75-4A-204.

In its summary judgment motion, BSB asserts that the exception to the general rule as codified in the UCC applies and relieves it of liability. To that end, the law provides:

> If a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure, a payment order received by the receiving bank is effective as the order of the customer, whether or not authorized, if (i) the security procedure is a commercially reasonable method of providing security against unauthorized payment orders, and (ii) the bank proves that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer. The bank is not required to follow an instruction that violates a written agreement with the customer or notice of which is not received at a time and in a manner affording the bank a reasonable opportunity to act on it before the payment order is accepted.

MISS. CODE. ANN. § 75-4A-202(b) (*emphasis added*). Thus, the risk of loss for an unauthorized transaction will lie with a customer if the bank can establish that its "security procedure is a commercially reasonable method of providing security against unauthorized payment orders," and "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."

[1] The parties are in seeming agreement that Mississippi UCC law applies, though Missouri UCC law appears to be identical. *See* MO. REV. STAT. §§ 400.4A-101, *et seq.*

However, notwithstanding the foregoing, a customer still will not have to bear the risk of loss over an unauthorized transaction if the customer can prove that the unauthorized transaction order "was not caused, directly or indirectly," by any person:

> (1) entrusted at any time with duties to act for the customer with respect to payment orders or the security procedure, or
>
> (2) who obtained access to transmitting facilities of the customer or who obtained, from a source controlled by the customer and without authority of the receiving bank, information[2] facilitating breach of the security procedure, regardless of how the information was obtained or whether the customer was at fault.

MISS. CODE. ANN. § 75-4A-203(a)(2)(i)-(ii).

As noted above, in its motion for summary judgment, BSB argues that – as a matter of law – the risk of loss associated with the unauthorized $440,000 wire transfer on March 17, 2009, lies with Choice. In order for BSB to prevail, the Court must be satisfied that there are no genuine issues of material fact regarding:

> (1) whether BSB's security procedure was a commercially reasonable method of providing security against unauthorized payment orders,
>
> (2) whether BSB accepted the $440,000 payment order in good faith and in compliance with the security procedure and any written agreement or instruction of Choice restricting acceptance of payment orders issued in the name of the Choice, and
>
> (3) whether the fraudster(s) who initiated the unauthorized transfer obtained the necessary security information from a source controlled by Choice and without authority of BSB.[3]

BSB has the burden of proving the first two points. MISS. CODE. ANN. § 75-4A-202(b) The burden on the third point, however, shifts to Choice. MISS. CODE. ANN. § 75-4A-203(a)(2)

---

[2] The statute defines "information" to encompass "any access device, computer software, or the like." Miss. Code. Ann. § 75-4A-203(a)(2).

[3] There is no contention that the subject $440,000 wire transfer was an "inside job" undertaken with the knowledge and cooperation of employees of Choice.

I. BSB's security procedure is deemed a commercially reasonable method of providing security against unauthorized payment orders.

The Funds Transfers provisions of the UCC contain a basic definition of a "security procedure," noting that the term includes any "procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication." MISS. CODE ANN. § 75-4A-201. The statute further notes that a security procedure "may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices." MISS. CODE ANN. § 75-4A-201. The Funds Transfers provisions of the UCC also contain guidance regarding a determination of "commercial reasonableness," to wit:

> 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. A security procedure is deemed to be commercially reasonable if (i) the security procedure was chosen by the customer after the bank offered, and the customer refused, a security procedure that was commercially reasonable for that customer, and (ii) the customer expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by the bank in compliance with the security procedure chosen by the customer.

MISS. CODE ANN. § 75-4A-202(c).

In this case, BSB argues that its security procedure must be "deemed to be commercially reasonable" under the second sentence of Section 202(c). Consequently, BSB must establish that:

(1) a security procedure was chosen by Choice after BSB offered, and Choice refused, a security procedure that was commercially reasonable for Choice, and

(2) Choice expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by BSB in compliance with the security procedure that was selected by Choice.

As set out herein, based on the summary judgment record before the Court, BSB establishes both of these requirements.

On April 16, 2009, Choice established an account with BSB to be utilized as an escrow/trust account. Shortly after opening this account, Choice determined that it wished to utilize a BSB online banking product ("InView") so as to have the ability to wire transfer funds electronically. In essence, the InView system allowed a BSB customer to effectuate a wire transfer of funds via the Internet by utilizing a User ID and password assigned to the customer by BSB.

In 2009, BSB typically required its customers enrolling in the InView system to utilize "Dual Control," which meant that an electronic wire transfer could only be effectuated by two individuals using separate User IDs and passwords. Basically, one individual would enter and approve the requested wire transfer in the InView system; however, no funds would be released until a second individual logged on to the InView system and released the funds. Choice declined the use of "Dual Control." Consistent with its policy,[4] BSB had Choice execute a MEMO on May 6, 2009, that stated (with emphasis in the original):

> We, Choice Escrow and Land Title, LLC, and all related entities which utilize [BSB's] InView Wire Module to transact online wire requests, understand the additional risks we assume by waiving

[4] If a customer refused to utilize "Dual Control," BSB would permit the customer to make electronic wire transfer of funds through the InView system if the customer would sign an agreement acknowledging it was waiving the use of "Dual Control" and the additional risks associated with such a waiver.

> [BSB's] requirement to utilize Dual Control for outgoing wires. By signing below we understand that although InView can restrict the account from which wires are sent and the amount related to said wire, InView **CANNOT** restrict to where the wire is sent.
>
> Since we wish to waive Dual Control anyone who has a User ID and Password or obtains access to a user ID and Password can wire funds to any other financial institution without restriction by [BSB] or the InView system. We understand that this can occur if our password is stolen. Further if funds are fraudulently wired out in this manner there is a substantial probability that we will be unable to retrieve our funds or recover losses.

The same day that Choice signed the above-quoted Dual Control waiver, it completed paperwork with BSB designating two of its employees (Cara Thulin and Brooke Black) as authorized to "enter," "approve," "release," and "cancel" wire transfers from Choice's escrow account at BSB. To that end, the designation form also provided:

> If desired, enter a daily wire transfer limit to apply at the company level. When this daily limit is reached, users at the company may not approve or release additional wire transfers on that day. (Note: Regardless of company or user limits for higher amounts, an account's current ledger balance will govern whether or not a wire transfer can be processed.)

In designating Ms. Thulin and Ms. Black, Choice declined to place a daily transfer limit on either employee, and Choice further declined to put a daily limit on the daily transfers for Choice company-wide.

In November of 2009, a Choice employee (Jim Payne) received an e-mail from one of its underwriters containing an "Escrow Bulletin" that warned of a scam whereby a fraudster would embed a "Trojan horse" on to a victim's computer, collect the victim's passwords, and then (using the passwords) wire funds from the victim's account to foreign banks. On November 11, 2009, Mr. Payne forwarded the e-mail to BSB and asked whether wire transfers to foreign banks could be limited. Two days later, Ashley Kester with BSB responded:

> 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 set up InView and you decided to waive 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 one user's information. Let me know, thanks!

Mr. Payne responded to this e-mail within a few minutes by asking for the "mechanics" of Dual Control and noting that it "[s]ound[ed] as if it would be a good precaution." Ms. Kester thereafter e-mailed Mr. Payne and informed him:

> It will take two people within InView to send a wire. One person to enter and another to approve/send. We will need to alter our agreements and will send the changes to you.

However, a half-hour later, Mr. Payne responded to Ms. Kester's e-mail:

> Actually, I don't think that would be a good procedure for us – lots of time Paige [Payne, a Choice employee] is here by herself and that would be really tough unless we all shared passwords.

Ms. Kester acknowledged Mr. Payne's e-mail, noting everything would be left as it was and informing Mr. Payne to let her know "if [Choice] would like to make any changes." Between the e-mail exchange on November 13, 2009, and March 17, 2010, no changes were made to Choice's InView procedures.

Between May 6, 2009 (when the InView access was created for Choice), and March 17, 2010, Ms. Thulin and Ms. Black made over 250 wire transfers on behalf of Choice using the InView system to send funds to numerous individuals, companies and financial institutions, including some wire transfers exceeding $400,000. The transfers made by Ms. Thulin and Ms. Black did not follow any routine schedule or pattern regarding the amount, the recipient, or destination. In addition, approximately 87% of the wire transfer requests made by Choice

through the InView system left blank the "Originator Bank Information" field – essentially a field permitting Choice to add a "memo line" to its request (akin to a memo line on a paper check).

Near noon on March 17, 2010, BSB received a wire transfer request via the InView system requesting a transfer of funds in the amount of $440,000 from Choice's escrow account for the benefit of Brolaw Services, Ltd. ("the Brolaw request"). The Brolaw request noted that the receiver bank was the Bank of New York, but that the beneficiary's bank (*i.e.*, the ultimate destination of the funds) was the Popular Bank Public Co. Ltd., an institution in the Republic of Cyprus. The Brolaw request was initiated using the InView User ID and password assigned to Ms. Black and was initiated from the IP address registered to Choice (and confirmed by BSB when Choice's access to InView was created). In addition, upon receipt of the Brolaw request, BSB authenticated that Ms. Black's computer was being used to make the request by detecting the secure device ID token that BSB had previously downloaded to Ms. Black's computer.

At 12:54 p.m., a BSB employee (Brenda Dulaney) confirmed that all of the information necessary to process the Brolaw request had been inputted. Ms. Dulaney then released the request for further processing within BSB's system. In particular, this processing included:

(1) checking the parties and accounts identified in the Brolaw request against the "black list" of terrorist individuals and organizations maintained by the Office of Foreign Assets Control, and

(2) checking the balance of funds available in Choice's escrow account to confirm the sufficiency of the funds.

The Brolaw request cleared this further processing – no terrorist connections were triggered and Choice had sufficient funds in its escrow account.

After Ms. Dulaney released the funds, BSB automatically generated a Transaction Receipt that was faxed to Choice and received by Choice at 12:54:30 p.m. on March 17.

Sometime thereafter, the Transaction Receipt was moved from Choice's fax machine to a shipping table where it was found by Choice employee (Paige Payne) the next morning. After determining that no Choice employee had requested the transfer, Choice contacted BSB and notified it that the Brolaw request was unauthorized. BSB then undertook efforts through the FBI, the State Department and the U.S. Embassy in Cyprus to recover the funds, but it was unsuccessful.

As previously noted, a security procedure must be "deemed to be commercially reasonable" under the second sentence of Section 202(c) in this case if:

> (1) a security procedure was chosen by Choice after BSB offered, and Choice refused, a security procedure that was commercially reasonable for Choice, and
>
> (2) Choice expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by BSB in compliance with the security procedure that was selected by Choice.

Based on the summary judgment record, the Court finds that both of these criteria have been established within the requirements of FED. R. CIV. P. 56.

As detailed above, on two different occasions, Choice was offered the opportunity to employ "Dual Control" as part of its utilization of BSB's InView system and Choice refused the option on both occasions. There can be little doubt that "Dual Control" meets the definition of a security procedure as set out in MISS. CODE ANN. § 75-4A-201. Thus the first element comes down to whether "Dual Control" was commercially reasonable for Choice.

Choice argues that "Dual Control" was not commercially reasonable for it because "at times, one or both of the two individuals authorized to perform wire transfers through the InView system [Ms. Black and Ms. Thulin] were out of the office due to various reasons." The Court disagrees. As set out in the UCC as adopted by Mississippi, the determination of what is

commercially reasonable is a question of law – which the Court believes imposes an objective test of reasonableness. Viewing the summary judgment record, the Court finds that the opportunity to use "Dual Control" was commercially reasonable. The record discloses that Ms. Black and Ms. Thulin were both in the office most days. Even assuming that Choice did not want to designate a third employee as an emergency back-up, the likelihood that both Ms. Black and Ms. Thulin would be unavailable for extended periods was small and represented more of an inconvenience to Choice rather than an impediment. As noted in the Official Comments to the Funds Transfers provisions of the UCC:

> The purpose of [having a security procedure deemed to be commercially reasonable] is to encourage banks to institute reasonable safeguards against fraud but not to make them insurers against fraud. A security procedure is not commercially unreasonable simply because another procedure might have been better or because the judge deciding the question would have opted for a more stringent procedure. The standard is not whether the security procedure is the best available. . . . Sometimes 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 that case, under the last sentence of subsection (c), the customer has voluntarily assumed the risk of failure of the procedure and cannot shift the loss to the bank.

U.C.C. § 4A-203 (Official Comment) (*emphasis added*). The Official Comment further notes the obvious: "a security procedure that fails to meet prevailing standards of good banking practice applicable to the particular bank should not be held to be commercially reasonable." *Id*.

However, the Court finds that the "Dual Control" option offered by BSB and refused by Choice did meet the prevailing standards for good banking practices. This is borne out in the testimony of BSB's expert witness as well as Choice's expert (Brad Maryman). As to the latter, Mr. Maryman gave the following testimony:

Q: Would you also agree that dual control as we've just been discussing it with all of these assumptions[5] . . . would be a commercially reasonable security procedure?

A: I believe it could, yes.

Having determined that BSB's "Dual Control" security procedure was offered to Choice, was refused by Choice, and was commercially reasonable for Choice, the Court briefly addresses the final requirement, namely that Choice must have expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by BSB in compliance with the security procedure that was selected by Choice. The Court finds that this requirement has been satisfied. In addition to the agreements previously quoted, Choice executed a Funds Transfer Agreement. Among other matters, this agreement provides that "[a]ny request received by [BSB] with the valid security code shall be irrebutably presumed to be from [Choice's authorized employees]. The Funds Transfer Agreement also explicitly states:

> [Choice] hereby authorizes [BSB] to honor, execute, and charge to [Choice's] account(s) any and all requests or orders to transfer or to pay funds through InView. [BSB] is authorized to complete all such transactions on [Choice's] account(s), which are initiated through the use of [Choice's] access code. [Choice] assumes full responsibility and risk of loss for all transactions made by [BSB] in good faith reliance upon [Client's] request or orders through InView. . . .

The Court finds BSB's security procedure was a commercially reasonable method of providing security against unauthorized payment orders under MISS. CODE. ANN. § 75-4A-202(b)(i).

II. BSB accepted the Brolaw request in good faith and in compliance with the security procedure and any written agreement or instructions of Choice restricting acceptance of payment orders issued in the name of Choice.

[5] Mr. Maryman was asked to assume that Ms. Black and Ms. Thulin had separate computers and did not share User IDs and passwords.

Inasmuch as the Court finds that BSB's security procedure was a commercially reasonable method of providing security against unauthorized payment orders, the Court must next turn to the second requirement of the UCC's risk-shifting statute wherein BSB must prove:

> that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer.

MISS. CODE. ANN. § 75-4A-202(b)(ii)

The definition for good faith is set forth in the UCC and encompasses "honesty in fact and the observance of reasonable commercial standards of fair dealing." MISS. CODE. ANN. § 75-4A-105(6). Consequently, there is both an objective and subjective component to good faith. With regard to objective good faith, there is little case law on the subject *vis-à-vis* the Funds Transfers provisions of the UCC, but the Court generally agrees with the test formulated by the Maine Supreme Court:

> The factfinder must . . . determine, first, whether the conduct of the holder comported with industry or "commercial" standards applicable to the transaction and, second, whether those standards were reasonable standards intended to result in fair dealing. Each of those determinations must be made in the context of the transaction at hand.

Maine Family Credit Union v. Sun Life Assurance Co. of Canada, 727 A.2d 335, 343 (Me. 1999). *See also Experi-Metal, Inc. v. Comerica Bank*, 2011 WL 2433383, op. at *12 (E.D. Mich. Jun. 13, 2011) (applying the *Maine Family Credit Union* standard to the Funds Transfers provisions of the UCC).

Applying that test, the Court finds that that the record is sufficient to establish that there are no genuine disputes with regard to the material facts as to whether BSB comported with industry or "commercial" standards and whether those standards were reasonable standards intended to result in fair dealing. The parties and their respective experts are in agreement that

the Federal Financial Institutions Examination Council's 2005 Guidance ("FFEIC 2005 Guidance") provides the applicable standards. The Court finds that BSB provided unrefuted evidence that it comported with industry standard as set forth in the FFEIC 2005 Guidelines, in particular as they relate to the use of multi-factor identification in providing for security procedures.[6] Finally, although it is surely self-evident, the Court finds the standards included in the FFEIC 2005 Guidelines with regard to security procedures were reasonable standards intended to result in fair dealing.

In its summary judgment pleadings, Choice makes no argument that BSB did not act honestly in accepting the Brolaw request on March 17, 2010. Nonetheless, the Court has reviewed the summary judgment record and is satisfied that BSB has established for purposes of Fed. R. Civ. 56 that it acted in subjective good faith in processing the Brolaw request.

Finally, as previously addressed, the Court finds that the payment of the Brolaw request by BSB was in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer. The Court would simply add that it does find any written agreements between BSB and Choice

---

[6] Essentially, Choice argues that BSB's security procedure was a single-factor authentication and thus contrary to the FFEIC 2005 Guidelines. The FFEIC 2005 Guidelines describe three different methodologies for authenticating customers:

(1) something known only to the user (e.g., User IDs and/or passwords);

(2) something only the user has (e.g., an ATM card, a specific IP address, a computer security token); and

(3) something the user fundamentally is (e.g., a biometric characteristic such as a fingerprint or voice recognition).

The FFEIC 2005 Guidelines required the use of two or more of these factors to constitute an acceptable multi-factor authentication. The Court finds that Choice's argument that BSB's security was a single-factor authentication to not be supported by evidence and, indeed, contrary to the record before the Court.

to be defective or ineffectual merely because BSB's internal Passmark system (which authenticated the Choice computer through the detection of a secure device ID token) was not mentioned in any of the agreements. In addition, the Court does not find that Mr. Payne's e-mail in November of 2009 asking whether BSB could limit transfers to foreign banks was an instruction by Choice restricting BSB's ability to accept payment orders.

Consequently, based on the foregoing, the Court finds that BSB has met its burden of proving consistent with Fed. R. Civ. P. 56 that the requirements of MISS. CODE. ANN. § 75-4A-202(b) have been met. As a result, pursuant to the intent of the drafters of the UCC, the risk of loss for the unauthorized wire transfer on March 17, 2010, shifts to Choice.

One final matter must be addressed. As the Court noted previously, even if the risk-shifting conditions of Section 202(b) are met, a customer may still prevail if it can satisfy the requirements of Section 203(a)(2). Under that statute, a customer still will not have to bear the risk of loss over an unauthorized transaction if the customer can prove that the unauthorized transaction order "was not caused, directly or indirectly," by any person:

> (1) entrusted at any time with duties to act for the customer with respect to payment orders or the security procedure, or
>
> (2) who obtained access to transmitting facilities of the customer or who obtained, from a source controlled by the customer and without authority of the receiving bank, information facilitating breach of the security procedure, regardless of how the information was obtained or whether the customer was at fault.

MISS. CODE. ANN. § 75-4A-203(a)(2)(i)-(ii).

Choice makes no argument for relief under Section 203(a)(2). Accordingly, the Court will simply note that, although there is no evidence that Choice employees were involved in the fraud, it does appear from the summary judgment record that the fraudster(s) effectively hacked into Ms. Black's computer to accomplish the March 17, 2010 transfer. There is no evidence that

the fraudster(s) was/were acting under the authority or permission of BSB. Consequently, Section 203(a)(2) provides no relief to Choice from the risk-shifting application of Section 202(b).

The tension in modern society between security and convenience is on full display in this litigation. Choice understandably feels as though it did nothing wrong, but yet is out $440,000. BSB, as well, feels as though it has done nothing wrong. In essence, both parties are correct – yet someone must bear the risk of loss. While such a risk generally would lie with a banking institution, the UCC has delineated a particular circumstance where the risk should be shifted to the customer. This case falls within that exception.

The result is not wholly unjust. The experts in this case agree that the fraud would not likely have occurred if Choice had utilized the "Dual Control." It elected not to . . . twice. In refusing the option the first time, Choice agreed that:

> Since we wish to waive Dual Control anyone who has a User ID and Password or obtains access to a user ID and Password can wire funds to any other financial institution without restriction by [BSB] or the InView system. We understand that this can occur if our password is stolen. Further if funds are fraudulently wired out in this manner there is a substantial probability that we will be unable to retrieve our funds or recover losses.

Unfortunately, that is exactly what came to pass. In refusing the "Dual Control" option the second time, Choice ignored BSB's admonition:

> We always recommend Dual Control on wires. We discussed this when we set up InView and you decided to waive Dual Control. Would you like to consider adding it now? <u>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 one user's information</u>.

Again, unfortunately, this appears to be exactly what happened.

For the foregoing reasons, the Court **GRANTS** the MOTION OF DEFENDANT BANCORPSOUTH FOR SUMMARY JUDGMENT [Doc. 160]. All other pending motions, including all other motions for summary judgment (including motions for partial summary judgment), are **DENIED** as moot. Accordingly, it is

ORDERED that summary judgment is entered in favor or defendant BancorpSouth Bank.

/s/ John T. Maughmer
John T. Maughmer
United States Magistrate Judge