Choice Escrow and Land Title, LLC v. BancorpSouth Bank

United States Court of Appeals for the Eight Circuit, 754 F.3d 611 (11 June 2014)

The federal circuit court of appeals construed the provisions of the US Uniform Commercial Code, which governs how parties allocate responsibility for losses from unauthorised online banking transfers, which could prove useful for banks.

When unauthorised online transfers take place in the account of a commercial banking customer, Article 4A of the Uniform Commercial Code governs how the parties allocate responsibility for the loss. Article 4A was promulgated in the late 1980s and has since been enacted in all 50 states. Its original focus was wholesale wire transfers, not online banking, but it continues to provide the only legal framework for resolving commercial banking disputes over cyber losses.

In spite of the prevalence of online banking fraud, reported decisions construing Article 4A are sparse. The law covers only commercial transactions - online fraud in consumer accounts is covered under the federal Electronic Funds Transfer Act - and it may be that most commercial customers who suffer cyber losses opt to resolve disputes with their banks pre-suit. It also may be that the magnitude of a typical cyber loss - though painful for a business to absorb - does not justify the costs of litigation.

The recent ruling by the United States Court of Appeals for the Eight Circuit in *Choice Escrow and Land Title, LLC v. BancorpSouth Bank*, 754 F.3d 611 (8th Cir., 11 June 2014) is one of only two decisions issued by federal circuit courts of appeals construing the provisions of Article 4A. The other case, *Patco Construction Company, Inc. v. People's United Bank*, 684 F.3d 197 (1st Cir. 2012) was decided less than two years before *Choice Escrow*. These cases stand in contrast to one another: The court in *Patco* found in favour of the customer, and its decision generally was viewed as increasing the burden on banks to provide security against online fraud. The Eight Circuit's holding in *Choice Escrow* found against the customer, and it could prove useful to banks in future disputes involving cyber losses.

Article 4A's risk-shifting rules

As a starting proposition, Article 4A assumes that a bank bears the risk of an unauthorised online banking transaction. However, even if a transaction is unauthorised, Article 4A enables a bank to shift the risk of loss back to the customer if it can prove: (1) that the bank and customer had an agreement that the authenticity of payment orders received by the bank from the customer would be verified pursuant to a security procedure; (2) the agreed upon security procedure was a commercially reasonable method of providing security against unauthorised payment orders; and (3) the bank accepted the payment order in good faith and in compliance with the security procedure.

As to whether a particular security procedure is 'commercially reasonable,' Article 4A expressly makes this determination a question of law that is dependent on four factors: (1) The wishes of the customer expressed to the bank; (2) 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; (3) alternative security procedures offered to the customer; and (4) security procedures in general use by customers and receiving banks similarly situated. This is designed to be a flexible, case-by-case inquiry. The statute's aim is to encourage banks to institute reasonable safeguards but not make them insurers against fraud. The rights and obligations of a bank and its customers arising under Article 4A cannot be varied by agreement.

A particular security procedure will be deemed commercially reasonable, regardless of the foregoing analysis, if (1) the 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 (2) the customer expressly agreed in writing to be bound by any payment order accepted by the bank in compliance with the security procedure chosen by the customer.

Patco Construction

Over the course of several days in May 2009, cyber thieves successfully initiated a series of online ACH ('Automated Clearing House') payment orders in the account of Patco Construction, a building and construction company in Maine. These transactions were uncharacteristic of Patco's normal online banking activity insofar as they sent money to numerous individuals to whom Patco had never before sent funds, they were for greater amounts than Patco's ordinary third-party ACH transactions and they originated from computers that were not recognised by Patco's bank.

The bank's security procedures consisted primarily of the use of challenge questions, but it configured its system to pose these questions every time a customer initiated an online ACH transfer. Although the bank had in place a transaction monitoring system that assigned a weighted risk score to every transaction, it did not monitor the scores or do anything in response to them. So, for example, in the case of the fraudulent transactions in Patco's account, these triggered extremely high scores that were indicative of suspicious, high-risk activity, yet the bank did not notify Patco or otherwise do anything with this information.

Reversing a finding of the trial court, the First Circuit Court of Appeals held that the bank's security procedures were commercially unreasonable because its across-the-board decision to trigger challenge questions - the primary layer of security - on every transaction amounted to a 'one-size-fits-all' approach that deprived the questions of their appropriate functionality, namely, to challenge transactions that were unusual or suspicious. The court reasoned this was a failure by the bank to take into account 'the circumstances of the customer' as required by the Article 4A criteria. The court also faulted the bank for failing to implement any other security measures, such as hardware-based tokens, immediate verification with customers of high-risk transactions or out-of-band authentication techniques, to supplement its procedures in light of its decision to dilute the effectiveness of the challenge questions.

Choice Escrow

Choice Escrow was a real estate escrow company that regularly wired funds to various recipients as part of its business. On 17 March 2010, cyber thieves accessed Choice's account and successfully instructed BancorpSouth to wire $440,000 to an account in Cypress. When Choice first set up its online wire transfer capability, the bank offered it the option of 'dual control' authorisation. Dual control requires a second authorised user, using a unique ID and password, to log into the online banking system to give separate approval to any transaction before it can be finalised. The bank offered dual control to all its customers. Choice declined the dual control option and signed a waiver acknowledging that it understood the risks associated with its decision. Sometime after it opened its account, Choice separately inquired about whether the bank could block wires to foreign banks. The bank responded that it could not, and it suggested that Choice reconsider using dual control. Choice again declined, indicating that dual control would not be a convenient option because it generally used only one employee to perform its wire transfers.

Affirming the trial court, the Eight Circuit Court of Appeals held that the bank's security procedures were deemed commercially reasonable under UCC Art. 4A-202(c) because it offered Choice a commercially reasonable option, dual control, which it expressly declined. In determining that dual control was itself a commercially reasonable procedure, the court stated that it 'dramatically' reduced the possibility of a breach by requiring an unauthorised user to compromise not one, but two sets of employee user IDs and passwords.

The court also rejected Choice's argument that any commercially reasonable procedure must include some form of transactional analysis that differentiated payment orders based on their size, type and frequency. The court reasoned that the 'size, type and frequency' criteria in Article 4A were merely intended to guide courts in weighing whether a particular security procedure was commercially reasonable, and Choice's position sought to 'graft a rigid, foreign standard onto the commercial reasonableness inquiry.' The court also held that a bank could use a single security procedure for the majority of its customers as long as the procedure was 'effective and versatile.' In other words, contrary to the court's suggestion in *Patco*, Article 4A did not preclude 'one-size-fits-all' security procedures under appropriate circumstances.

As its final order of business, the court reversed the trial court's dismissal of BancorpSouth's counterclaim for attorney's fees based on an indemnification provision in the parties' account agreement. The trial court had ruled that the provision was displaced by Article 4A, which does not provide attorney's fees as a remedy for either party. The appellate court, however, concluded that the provision was not inconsistent with Article 4A because it was 'extrinsic to [its] attempts to balance the risk of loss due to the fraudulent payment order.'

Conclusion

The outcome in *Choice Escrow* is not remarkable given the facts of the case - the customer made an informed choice to reject the dual control option offered by the bank, and even the customer's own expert conceded that it could have been a commercially reasonable procedure under the circumstances. However, the Eighth Circuit's reasoning is likely to play a role in future cases where the outcomes are closer calls - and the most lasting impact of the decision may be increased efforts by banks to shift legal fees to commercial customers in disputes over cyber losses.

Dan J. Mitchell Shareholder
Bernstein Shur, Portland
mitchell@bernsteinshur.com