Bank Customer – Not the Bank – Liable for Fraudulent Wire Transfer

July 8, 2014

Recent security breaches have focused attention on the allocation of risk associated with fraudulent payments. The recent U.S. 8th Circuit Court of Appeals decision in *Choice Escrow & Land Title, LLC v. BancorpSouth Bank* provides a timely reminder that when a bank develops and implements proper security procedures for commercial electronic funds transfers (consumer electronic fund transfers have different rules), those procedures can protect the bank from the risk of loss for a fraudulent wire transfer made from a commercial customer's account. In *Choice Escrow* the Court held that a bank that had complied with its commercially reasonable security measures was not responsible for a commercial customer's loss resulting from a fraudulent wire transfer payment and further expands on the 2012 decision in *Patco Const. Co., Inc. v. People's United Bank*, which we summarized in a prior alert.

Article 4A of the Uniform Commercial Code, which governs commercial funds transfers such as wire and ACH transfers, provides a finely-balanced allocation of rights, obligations and risks between a bank and its commercial customer. The general rule is that the bank bears the risk of loss when a third party initiates an unauthorized payment order on a customer's account unless the bank is able to shift the loss to the accountholder. Article 4A provides the bank two methods for shifting the risk of loss to its customer. The first is for the bank to prove that, under the law of agency, either by actual or apparent authority, its customer is bound by the payment order. The second method is based on the bank and its customer agreeing to implement a security procedure to protect against fraud. Under this second method, the customer bears the risk of loss 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.

Choice Escrow, like the *Patco*, involved this second method. In *Choice Escrow*, an employee of the bank's commercial customer was the victim of a phishing attack that installed malware which provided the "internet fraudsters" with access to the employee's username and password and allowed them to mimic the IP

address and other characteristics of the employee's computer. The fraudsters then initiated a wire transfer in the amount of $440,000 from the customer's account to an account in the Republic of Cyprus. The customer sued the bank claiming that the bank should bear the loss from the fraudulent payment order.

The security procedures offered by the bank included password prompts, daily transfer limits, a dual control system, and authentication software designed to determine whether the computer from which the transfer is initiated is an "authorized" computer. These security procedures were all offered to Choice Escrow but the customer chose to use only the user ID and password procedure and the authentication software. The customer was aware of the potential of phishing scams and at one point, after receiving information on a potential phishing scam, inquired whether the bank could restrict transfers to foreign banks. The bank replied that it could not stop such transfers, but stated that a solution to the problem would be the "dual control" procedure, which the customer declined.

The customer did not dispute that the bank complied with its security procedures in accepting the payment order at issue but did dispute (1) whether the bank's security procedures were commercially reasonable, (2) whether the bank accepted the payment order in good faith, and (3) whether the bank accepted the payment order in compliance with the customer's written instructions. Upon reviewing the security procedures that were in place and available to the customer, the court concluded that the bank's procedures were commercially reasonable. The bank had followed the 2005 Federal Financial Institutions Examination Council (FFIEC) security guidelines and also enhanced its security procedures to address issues that had arisen after the issuance of that guidance.

Having decided that the bank had a commercially reasonable security procedure, the court next had to determine whether the bank accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer. The customer conceded that the bank acted honestly and the Court concluded that there was nothing so unusual about the payment that it should have raised eyebrows. Therefore the bank had no obligation to further review to determine whether the payment order was suspicious. The court also held that the bank acted in good faith in processing the requested payment because there was no independent reason to suspect that the payment was fraudulent and the payment request has cleared the bank's commercially reasonable security procedures.

Ultimately, because the bank's security procedures were commercially reasonable, the bank complied with its security procedures and with any customer instructions (there were none), and the payment order was accepted in good faith, the court held that the customer bore the loss of funds, not the bank.

In addition to the lessons learned from *Patco*, as set forth in our prior alert, there are several key take-a-ways from the *Choice Escrow* decision:

- It is important to update your security procedures instead of relying solely on outdated security guidance. Banks have an ongoing obligation to make sure that their security procedures are evolving as threats evolve.
- Understanding what security procedures other banks offer to similar customers can also assist with the evaluation of whether your security procedures are reasonable.
- Because the court looked at the reasonable expectations of the bank customer in determining whether the payment order was accepted in good faith, it is important to set forth your security procedures in an agreement with customers so that it is understood and agreed to what security procedures will be used.
- Compliance by the bank with the established security procedures is a necessity in order to shift the risk of loss to its customer.