Delaware Banker

Winter 2019
Vol. 15 No. 1

Call to Innovate

Is Your Bank Ready?

Lending Law Update

by
Eugene A. DiPrinzio
Young Conaway Stargatt & Taylor, LLP

"..all parties to a transaction must take reasonable precautions to prevent their computers from being hacked..."

Email Fraud and Contract Liability: An Interesting Dilemma

In a recent U.S. Sixth Circuit Court of Appeals decision (Beau Townsend Ford Lincoln, Inc. v. Don Hinds Ford, Inc., No. 17-4177, WL 6181643 (Ohio Ct. App. 11/27/18).), a three (3) judge panel ruled that a full fact finding trial was required for a court to determine whether a contract loss suffered through email fraud could be attributed to one party or another. The case involved the sale and purchase of excess car inventory (20 Ford Explorers) between two dealerships, the seller in Ohio and the buyer in Indiana. The two dealerships had historically made deals for transfers of vehicles and simply exchanged checks when effectuating their transactions. In this particular instance, a typical transaction turned ugly when a hacker intercepted a few email messages and was able to convert the transaction from a check exchange to a wire funds transfer. The hacker was successful in causing approximately $736,000.00 to be transferred to a domestic bank account which was subsequently closed and drained with the hacker vanishing into parts unknown.

Prior to the appeal, the District Court for the Southern District of Ohio entertained motions for summary judgment from both sides as to whether or not one party had been either negligent or innocent in the transaction. Because the buyer dealership received the vehicles but the seller dealership never received the cash, the District Court awarded judgment in favor of the seller dealership as the party who did not obtain the money. In the appellate proceeding, the Court analyzed the difficulties involving the fact pattern presented and concluded that it touched many different areas of law, including contract, Uniform Commercial Code, and agency law. In light of the many areas of law affected, it was difficult to reach a final decision on liability without determining the proper party to suffer the loss. Under the Uniform Commercial Code and various state statutes, the Court needed to determine whether the failure to exercise ordinary care contributed to the hacker's success. This analysis suggests that any court would have to apportion the recovery amount according to a party's comparative fault, similar to a negligence standard. The Court also reasoned that a final determination could turn on whether there was a mutual mistake of fact. The judicial panel determined, on the motions submitted, that both parties believed they were acting correctly and neither knew the other was mistaken. Lastly, the Court looked at agency law to provide a basis to determine if one party had justifiably relied upon a proper appearance of authority and had operated in good faith and had exercised reasonable care in the transaction. Given the complexity of the liability issue, the inability to apportion blame on the record presented, and the lack of case law, the Court concluded "to decide this case, the factfinder must determine which party was in the best position to prevent the fraud." To answer that question, an arbiter or judge needs to make findings of fact and therefore, a full trial must be held.

The scope of this article is not intended to predict how the courts will eventually rule on this issue, but merely to point out that there is no clear cut answer in many cases involving wire fraud and funds transfers, particularly where wire instructions and/or email confirmations have been intercepted or hacked. The conclusion one needs to reach in this regard is that all parties to a transaction must take reasonable precautions to prevent their computers from being hacked and must also use careful diligence in making secure wire instructions and transfers when doing business. All roads seem to lead to an analysis of the precautions and firewalls that are being built when utilizing a computer system and whether or not parties are using a standard of care that will in fact prevent or reduce fraud. It is no wonder that cyber security is and should remain at the forefront (and one of the top priorities) for all financial institutions and their customers.