

Du v. Jameson Bank 2017 ONSC 2422 – who bears the loss with a fraudulent wire transfer?

Wire transfers are a common way to move money. While such transfers are generally pretty safe, there can be risks involved – including risks of cyber-crime. When a fraudster hacks an account and steals money from a person’s bank account, who pays the loss? Generally speaking, it is not the bank! A recent decision of the Ontario Superior Court provides a good example how difficult it can be for a bank customer to sue his own bank for losses arising out of a fraudulent wire transfer.

The plaintiff in this case was a Mr. Du. He and his wife had lived in Canada for 16 years and had opened many bank and brokerage accounts over the years. In 2011, Du opened an account at Jameson Bank (“the Bank”), a Schedule 1 Bank. As part of the process of opening up his new account, he completed the Bank’s “Client Application Form”. Among other things, the Form stated that “you acknowledge that you were provided with the [Bank’s] Terms and Conditions ...”. While Du acknowledged that he had indeed received a copy of the Terms and Conditions (“the account agreement”), he claimed that he had not read them. At all times, he communicated with the Bank using this email address: duwang888@hotmail.com.

The account agreement provided that the Bank was entitled to rely upon email instructions “from or purporting to be from [Du] which [the Bank] believes in good faith to be genuine”. It also provided that, except in cases of gross negligence or wilful misconduct by the Bank, the Bank would bear no responsibility for losses which might occur in connection with any wire transfer.

As it turned out, someone hacked into Du’s email account and fraudulently instructed the Bank using Du’s email address to make wire transfers to third party accounts in the total amount of \$135,000 USD. The money was not recovered. Du blamed these losses on the Bank. He initially complained to the Ombudsman for Banking Services which rejected his complaint. Then he sued the Bank; initially in negligence and then in breach of contract, conversion, breach of fiduciary duty and damages for breach of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (“the Act”). Like so many before him, Du tried to get his bank to pay for his losses.

The Court noted that S. 54 of the Act requires that every financial entity must ascertain the identity of a person who opens an account before conducting a foreign currency exchange transaction of \$3,000 or more. However, this requirement does not apply where the person has signed “a signature card in respect of an account ...”. The court concluded that in opening the account and in signing the account agreement, this requirement was met, so that that the *Act* did not apply. The judge did not address the issue as to whether a breach of the Act might give rise to a private cause of action to a Bank’s customer (in other cases, regulatory statutes have not given rise to such a cause of action).

Meanwhile, the Court held that the terms of the account agreement provided a complete defence. It allocated the risk of loss in any wire transfer to the customer. The fact that Du claimed that he had not read this agreement did not affect its enforceability. In any event, the Bank had no obligation to question any of the transfers; the bank was obligated to follow its customer’s actual or purported instructions, and this is what it did. There were no suspicious circumstances that gave rise to any duty to inquire on the part of the Bank. Moreover, Du did not introduce expert evidence as to the standard of care of a “reasonable banker”, and such evidence would have been required to prove “gross negligence”. Finally, in the absence of special facts, a bank owes no fiduciary duty to its customers and none was owed here. The case was dismissed.