Cheques, Rogues and Mobile Banking

Yesterday I received an email telling me to destroy the cheques I deposited to my business bank account 90 days ago by simply taking a photo of them with my iPhone. Technology and mobility has its benefits, saving me the time of physically going to my financial institution, confirming my deposit by email and providing some security with respect to preventing my cheques from being redirected by a rogue or forged endorsement. Whether the system is foolproof is yet to be determined, especially when it comes to the banks' ability to confirm the authenticity of the cheque and its depositor.

Some businesses have had cheques intercepted by a rogue, who will change the payee and/or cheque amount or forge the endorsement for deposit into his own account. The money gets withdrawn from the issuing business account and the actual payee never sees the funds. When the payee complains of non-payment months later, the issuing business realizes it has been duped out of money it believed it had paid. Recovery of the funds is possible based on rules set out in the *Bills of Exchange Act* and procedures of cheque clearing under the Canadian Payments Association.

Once the issuing company provides written notice to its bank of the forgery, its bank should issue credit for the amount to the company account and seek reimbursement of the funds from the bank that processed the forged cheque. The processing bank then has the ability to freeze the account into which the funds were illegally deposited, assuming they haven't already been spent or redirected, and seek recourse from the rogue if he can be found. What seems like a simple process has resulted in many court cases between banks and the issuing company on determining which innocent party gets stuck with the loss of funds relating to the altered or forged cheque.

Generally banks require its business clients to enter into a banking agreement setting out the terms governing funds in the accounts, including the requirement for clients to review and confirm the accuracy of statements within 30 days of issuance. Banks are also expected to know their customers, their signatures and banking processes, which is harder to do in the case of larger companies. Where the issuing company failed to comply with the banking agreement or ought to have discovered or prevented the forgery, it will bear the loss. If the company's bank failed to comply with its processes, like confirming the processing of large amounts or dual signatures on a company cheque, the company's bank will be out of funds. Where the processing bank didn't follow its policies, like placing a five day hold on large funds before releasing, it will bear the loss.

Mobile banking takes away some of the checks and balances generally available to the banks. For example, they no longer obtain possession of the cheque, which normally goes through a clearinghouse process, as the payee retains it until the 90 day period has lapsed. I'm not sure whether technology has advanced enough that a photo can depict the authenticity of a watermarked cheque or if the cheque has been altered. Once the cheque is destroyed as required by my bank, there is no way of confirming its authenticity. Other than physically opening a bank account, customers may not even step foot in a bank, limiting the bank's ability to know its customer.

I believe in CYA and advise my clients accordingly. Should you choose to use mobile banking, keep the original cheque in case you need to produce it at a later date. If your customers use mobile banking to deposit their cheques, ask them to return them to you after the 90 day period or to retain them for at least a few years. While fraud and forgery may happen overnight, it may take years before it is discovered and much longer to figure out who will be out of pocket. Liability may be even harder to determine after the physical evidence has been destroyed. Should you need assistance in dealing with fraudulent activities, contact Wallace Law.