SMALL CLAIMS COURT OF NOVA SCOTIA
Citation: *Campbell v. Asaph*, 2024 NSSM 48

Date: 20240611
Docket: 525466
Registry: Sydney

Between:

Carl Christopher Campbell

Claimant

v.

Michael Leon Asaph

Defendant

DECISION

Adjudicator: Raffi A. Balmanoukian

Heard: December 28, 2023, by Teams

Counsel: Carl Christopher Campbell, self-represented claimant
Michael Leon Asaph, self-represented defendant

By the Court:

[1] The Claimant did work for the Defendant. The Defendant paid the bill, but through a scam the funds went to a third party who, incredibly, has been identified. The funds have not been recovered. Nobody is holding their breath for them to materialize. Who bears the loss?

[2] The Claimant provided two invoices; the first was paid without issue. The second, issued in May 2023, was 'paid' in the sense that funds were transferred from the Defendant; but they were not received by the Claimant.

[3] Although the parties disagree on fault, they do not disagree on the fundamental facts. The Defendant sent two e-transfers to pay the second invoice, both requiring a fairly simple password, which the Defendant says he sent separately by email (at least one email appears to have been diverted, as will appear). When the Claimant could not retrieve the funds (he was not set up, at that time, for autodeposit), he called the Defendant, who said that he received an email "from me, to me." The Defendant clicked on a link in that email and, the Claimant testified, the Defendant realized immediately that he had fallen into the proverbial trap. The Defendant denies clicking on any such link. The Defendant was able to stop the second, but not the first, transfer.

[4] The Claimant's bank (which is different from the Defendant's) has no record of the transaction.

[5] A criminal investigation ensued, apparently at the Defendant's initiative (the Claimant said he did not contact police or insurance). The perpetrator of the malicious email was identified as one Joshua Daley, apparently a Saskatchewan resident. The Claimant communicated with him, and promises of reimbursement (to either of the parties) not surprisingly went unconsummated. There is no indication that recovery through either the civil process or other restitutionary remedies is likely. There is no indication that Mr. Daley has been charged with any offence, or that criminal proceedings are ongoing. The Claimant testified, however, that he had no knowledge that the investigation was in fact suspended.

[6] The Claimant admits, quite candidly, that he could have been hacked; however, his computer is password protected, has (unspecified) antivirus protection, and has limited accessibility (he and his wife); his email is also password protected. He says that his bank account is "automatic sign in" but he has received "hundreds" of e-transfers without incident.

[7] The Defendant provided evidence that the hacker was able to answer the security question / password to obtain the misappropriated e-transfer. It was never established, to my satisfaction and on a civil standard, how the perpetrator was able to receive both the e-transfer notification and separate password. It may be that the nefarious link provided access to both, but whether it was from the Claimant's computer being hacked, the Defendant's clicking on the impugned link, or some combination or third option was never proven.

[8] The Claimant also referred to material from Interac and another website advising that e-transfers should be bolstered with strong passwords, safely shared (and not by email). It was not clear when these materials were created or accessed, but the implication is that the Defendant is the author of his own misfortune by emailing a weak password (the Defendant admits emailing the password, but "in reply" to an email purporting to come from the Claimant). The Claimant did not provide payment instructions to the Defendant.

[9] The Defendant denied clicking on any links, saying instead that he replied to an email from the Claimant. As for Mr. Daley, the Defendant says his (Daley's) story is another fourth party accessed his electronics and is the ultimate perpetrator.

[10] The Defendant had a tech-savvy "friend" trouble shoot his computer, who found a virus on his machine, embedded in Hotmail "rules." Both parties have Hotmail addresses. It appears Mr Daley had a Gmail address.

[11] The Defendant testified that although other payment methods were available, the parties agreed to use e-transfer for payment.

[12] In brief, while the Claimant admits that it's possible his computer was hacked, he denies negligence and submits that banking 'best practices' were not followed by the Defendant and, as such, the loss lies with him. The Defendant submits that passwords are not an infallible "protective device" and submits that the recipient has a responsibility to protect against malicious links or other compromising items.

[13] Adjudicator Darling recently dealt with a "hacking" case in *Jane Group Limited v. Heritage Gas Limited*, 2022 NSSM 36. As here, a payor's remittance was misdirected due to a hack; there was no evidence that the hack originated from the Creditor's computer or system. As such, Adjudicator Darling found that there was no negligence by the Creditor and was entitled to be made whole, notwithstanding the good-faith and misappropriated payment by the Debtor.

[14] Adjudicator Darling concluded that there was no evidence of negligence by the Creditor, concluding that the adjudicative framework can be broken down as follows:

> The decision maker in this case described what I consider to be a helpful test in circumstances where, as in the case before him, the identity of the party that had been hacked was known:
>
> > 56. As noted at the outset of these reasons, the issue in this case can be restated as follows: Where a computer fraudster assumes control of Victim A's email account and, impersonating Victim A, issues instructions to Victim B, who then transfers funds intended for Victim A (or a third party) to the fraudster's account, is Victim A liable for the loss?
> >
> > 57. In my view, the answer is "no", <u>unless</u>:
> >
> > a. Victim A and Victim B are parties to a contract which (i) authorizes Victim B to rely on email instructions from Victim A and, (ii) assuming compliance with the terms of the contract, shifts liability for a loss resulting from fraudulent payment instructions to Victim A;
> >
> > b. There is evidence of willful misconduct or dishonesty by Victim A; or
> >
> > c. There is negligence on the part of Victim A. [emphasis in original]

[15] Notably, there were several "red flags" in the emails in question in *Jane Group*, even without the benefit of hindsight (Adjudicator Darline considered there to be none on the part of the Claimant; I am not sure I agree at least insofar as the

Defendant was concerned in that case). The email requested a deposit to a third party account in Ontario. It is also worth noting that the payor was a sizeable corporation rather than an individual consumer, such as we have here. It also appears that a strong password was in use, which was not the case here.

[16] I, too, consider the above framework to be helpful. Applying it,

(a) We do not know who was hacked. The Claimant admits that it might be he. Neither party impressed me as being especially tech-savvy.

(b) The contract does not provide for method of payment, although I accept that e-transfer was agreed upon and indeed was used to pay the first invoice.

(c) There is no evidence of wilful misconduct or dishonesty by either party;

(d) Although the Claimant (to repeat) admits he might be the victim of a hack, he denies negligence. I accept that a successful hack is not in itself proof of negligence or that the standard of care for a business accepting e-transfers was breached by him. It appears that his computer has limited accessibility and at least consumer-level protections.

[17] It is common knowledge that even the most robust systems are subject to compromise. Governments and large corporations are crippled by private and sometimes by state acts. As I write (on a computer), I admit to looking forward to

the next reboot of Battlestar Galactica and its increasingly timely warning to maintain technological advance within our capacity to manage it.

[18] With that said; it falls to the Claimant to prove his case on a balance of probabilities. He has easily done so in the sense that he has proven that there was work done and he has not received all of his money for it. What makes matters complicated is that while the contract was performed and the money paid, the contractual elements then require a negligence analysis to determine whether the Claimant has any responsibility for the misdirected funds.

[19] I repeat, again, that the Claimant has admitted that his computer may have been compromised. I also repeat that this is *in itself* not conclusive of negligence. Weighing all of the evidence, while I conclude that the Claimant did not have the military-grade security, he did not fail to take reasonable security precautions in all of his circumstances; it follows that the Defendant has not established that the Claimant was electronically negligent. It will be recalled that the Claimant's invoice did not provide for terms of payment; the parties then agreed on e-transfer; the first was without incident; the Defendant created a weak password; and while there was conflicting evidence on whether the Defendant clicked on a compromising link, there was no evidence that this was created through the negligence of the Claimant – that is to say, that he failed to take reasonable security precautions in the circumstances of his business, or to address a previously known vulnerability.

[20] I have considered whether contributory negligence applies. When deliberating,

my first instinct was that each side should bear a portion of the loss; perhaps even equally (s. 3(1) of the *Contributory Negligence Act*, RSNS 1989, c. 95 providing that where a Court cannot determine who is more at fault than another, the loss shall be allocated equally). However, that disregards the fact that for there to be *some* negligence, there first must be *any* negligence; that is for the Defendant to establish, to a civil standard. He has not done so; the mere acknowledgement that the Claimant's *reasonable* efforts with respect to virus protection and passwords may not have been successful (and I find that they were reasonable, in the circumstances), is not enough.

[21] It follows that the Defendant remains liable for the $2,499.81 claimed. In the circumstances, I award neither prejudgment interest nor costs.

Balmanoukian, Small Claims Court Adjudicator