CITATION: Sankreacha v. Cameron J. and Beach Sales Ltd., 2018 ONSC 7216
COURT FILE NO.: CV-17-129350
DATE: 20181203

ONTARIO

SUPERIOR COURT OF JUSTICE

BETWEEN:	)	
Bharath Sankreacha	)	
Plaintiff	)	James Jagtoo, Frances Jagtoo, for the Plaintiff
– and –	)	
Cameron J. and Beach Sales Ltd., John Cowan, JMC Legal Services Inc., and Rod Brennan	)	Martin A. Smith, Desneiges Mitchell, Marla Rosenblatt-Worth, for the Defendants, Cameron J. and Beach Sales Ltd. and Rod Brennan
Defendants	)	Andrew W. Graham, for the Defendants, John Cowan and JMC Legal Services Inc.
	)	**HEARD:** May 14-18, 22-25, 28-31, June 1, 4 and September 14, 2018

REASONS FOR JUDGMENT

TABLE OF CONTENTS

CHARNEY J.:

Introduction

[1] The plaintiff, Bharath Sankreacha, is a former Service Advisor at the Canadian Tire store in Markham, Ontario. He was dismissed from his employment on June 21, 2010, after being accused of installing spyware on his employer's computer and being charged by the police with unauthorized possession of credit card data.

[2] The charges against Mr. Sankreacha were withdrawn by the Crown on August 10, 2011.

[3] Mr. Sankreacha brought this claim for wrongful dismissal, inducing breach of contract, injurious falsehood, intentional infliction of mental distress, defamation, false imprisonment, malicious prosecution, and civil conspiracy.

[4] Named as defendants in this action are: i) Mr. Sankreacha's former employer and corporate owner of the Markham Canadian Tire franchise, Cameron J. and D. Beach Sales Ltd., ii) the Service Manager at the Markham Canadian Tire store's automotive department and Mr. Sankreacha's former manager, Rod Brennan, iii) the contractor retained by the franchise to provide security services in the Markham Canadian Tire store, John Cowan, and iv) the corporation owned and operated by Mr. Cowan to provide these security services, JMC Legal Services Inc.

A. Facts

The Discovery of the KGB Spyware - June 21, 2010

[5] On June 21, 2010, the defendant, Rod Brennan, the Automotive Service Manager at the Markham Canadian Tire store, arrived at work sometime around 6:45 a.m. He logged on to the computer in his office using his password and noticed a minimized tab at the bottom of the screen. When he clicked on the tab it brought up an email.

[6] The email appeared to be on Mr. Sankreacha's personal Hotmail email account. The email was from bharath_sankreacha@hotmail.com to bharath_sankreacha@hotmail.com. There is no dispute that this was the plaintiff's personal email address.

[7] In addition to the sender and recipient, there was other information on the screen. The email subject was "Rod" (Mr. Brennan's first name) and referenced "KGB monitoring system". It also showed the words "17/06/2010 4:41:12 PM Stop recording". The email was dated Sunday, June 20, 2010, at 8:53 a.m. and contained an attachment.

[8] Mr. Brennan was not sure what to make of this, but he was concerned. He called two other employees into his office to look at his computer screen and ask them their opinion. At about 8:00 a.m., he called in the General Manager, Sasha Issa, and the owner of the Markham Canadian Tire franchise, Cameron Beach. They too looked at the screen and all agreed that the image on the screen looked suspicious.

[9] Mr. Issa told Mr. Brennan that the image on his screen looked like Mr. Sankreacha was recording something on Mr. Brennan's computer with spyware, and Mr. Issa printed a copy of the screen and the 48-page attachment to preserve the information. Mr. Beach stated that it looked to him as though data was being sent via the email. He was particularly concerned because there were folders referencing "CTC mastercard" and "CTC0399", which he thought might relate to credit card information of the store or its customers.

[10] Mr. Issa reviewed the 48-page printout. Several items on the printout contained the letters "SCODEF" followed by numbers and "CREDAT" followed by numbers. Mr. Issa thought that this could relate to Bank of Nova Scotia credit cards. Several other items contained the words "Scotia OnLine Sign-On" followed by a series of numbers, or "Scotia OnLine", or "Scotia Bank".

[11] Mr. Brennan testified that he only looked at the first page of the 48-page printout.

[12] Mr. Sankreacha was not scheduled to start work until 2:00 p.m. Mr. Brennan's first thought was to call Mr. Sankreacha to ask if he could explain what was on the computer screen. Mr. Sankreacha worked in the automotive department and reported to Mr. Brennan. Mr. Brennan described Mr. Sankreacha as his "right-hand man"; he trusted Mr. Sankreacha, and had given Mr. Sankreacha the password to his computer so that Mr. Sankreacha could do the employee scheduling and check his personal emails from work. There is no dispute that only Mr. Brennan and Mr. Sankreacha knew the password to Mr. Brennan's computer.

[13] Mr. Brennan called Mr. Sankreacha at home at about 7:00 a.m. to ask if he could explain the email, but Mr. Sankreacha did not answer. Mr. Brennan left Mr. Sankreacha a voicemail message telling him that there was something serious involving an email on the computer in his office.

[14] Mr. Sankreacha called Mr. Brennan back at about 7:30 a.m., but there was no answer. Mr. Sankreacha then stopped by the store at about 9:00 a.m., but was told by Mr. Brennan that everything was fine and to return to the store for his scheduled shift at 2:00 p.m.

[15] Mr. Brennan called the defendant, John Cowan, who is under contract with the Markham Canadian Tire store to provide security services, including loss prevention and corporate investigations. Mr. Cowan arrived at the store at about 9:15 a.m. and viewed the email on Mr. Brennan's computer screen and the printout of the attachment. He believed that there was banking information on the printout and he advised Mr. Beach to call someone with computer expertise.

[16] Mr. Beach called in his IT contractor, Allan Valencia, at around 9:30 a.m. to come in and look at the computer screen.

[17] Mr. Valencia provides sales, installation, support and services to his clients' electronic systems, including telephone, surveillance and computer systems. He attended the store

that morning, sometime between 10:30 – 11:00 a.m., and went to see the computer in Mr. Brennan's office.

[18] Mr. Valencia observed that he was looking at an email to a Hotmail account from the plaintiff's email address to the plaintiff's email address. He noted the reference to the KGB Monitoring Software, which he knew was a type of spyware. It is used to record all keystrokes on a computer and take screen shots of the websites the computer is visiting. KGB continuously and secretly monitors the activity of the computer, and the data is collected and put in a log. A password is required to access the data collected by KGB after installation. This data can be used to access bank accounts because the website information will reveal the bank and the keystrokes can be used to figure out the account numbers and password.

[19] Mr. Valencia testified that KGB spyware must be installed on the computer intentionally and manually by a person downloading it from the internet or bringing it in on a CD or USB drive. Since he had installed Sonicwall on the store's computers to protect them from viruses and malware, it was unlikely that the KGB spyware had been installed from the internet.

[20] When Mr. Valencia looked at the email on the computer, there was a banner at the top which read: "Please sign in again. To help protect your personal information, we periodically sign you out (for example, after 24 hours or when you sign in to a different account)." Mr. Valencia explained that this banner appears when the account has "timed out" due to inactivity. After 24 hours, Hotmail signs the user out automatically as a safety feature. Notably, that banner was not present when Mr. Brennan had opened his computer and printed the screen that morning.

[21] Mr. Valencia believed that Mr. Sankreacha had sent the email from himself to himself. Mr Valencia explained that since the Hotmail account had been logged out, he was looking at cache memory. He could not click on or open any of the attachments because the account had been timed out. Based on this information Mr. Valencia was of the opinion that the email account was opened on Mr. Brennan's computer the day before, and less than 24 hours before Mr. Brennan had opened it that morning. Mr. Valencia believed that Mr. Sankreacha had opened it the day before and had likely forgotten to close it and sign out.

[22] Mr. Valencia isolated the computer from other computers on the network and conducted a virus scan. The scan confirmed that there was KGB spyware on Mr. Brennan's computer. There was a KGB folder in the computer's hard drive, but Mr. Valencia could not open it and view the contents because he did not have the password to open the spyware. He then shut the computer down so it could be used as evidence.

[23] Mr. Valencia concluded that whoever installed the spyware on the computer was sending an email with the data captured by the spyware to himself. He told Mr. Beach that the spyware could have been installed on the computer in the hope of harvesting credit card, banking, and personal identification information that could be used or sold. He advised Mr. Beach that the spyware had captured numbers that could potentially relate to bank

accounts. He did not, however, advise Mr. Beach, Mr. Issa, Mr. Cowan, or the police, that the printout contained any credit card or Mastercard information.

[24] Mr. Cowan left the store at about 10:30 a.m. for about 3 hours in order to deal with other matters. While away he called a "contact" who informed him that Mr. Sankreacha's previous employer had accused Mr. Sankreacha of stealing a hard drive from the employer's computer. Mr. Cowan believed that Mr. Sankreacha had previously been charged with computer related offences.

[25] Mr. Cowan returned to the store at about 1:00 p.m., and spoke to Mr. Issa who relayed Mr. Valencia's opinion that there was spyware on the computer. Mr. Issa told Mr. Cowan that there appeared to be credit card data on the printout. Mr. Cowan thought, incorrectly, that Mr. Issa's information regarding credit card data had come from Mr. Valencia.

The Arrest of Mr. Sankreacha

[26] At 2:00 p.m., Mr. Sankreacha arrived at the store to begin his shift. He was escorted by Mr. Cowan to Mr. Issa's office to be questioned about the email and see if he had any explanation. Messrs. Issa, Cowan, Beach and Brennan were present for some or all of the interview. Mr. Cowan advised Mr. Sankreacha that he was opening an investigation, but that Mr. Sankreacha was not under arrest, did not have to speak to him, and was free to go at any time. The door to the office was left open.

[27] They showed Mr. Sankreacha the printout of the email and he responded that he did not know anything about it.

[28] They asked Mr. Sankreacha to open his Hotmail account from Mr. Issa's computer, which he did. The email from Mr. Sankreacha to Mr. Sankreacha with the subject "Rod" that was on the printout was not in Mr. Sankreacha's email or in his trash. Mr. Sankreacha had no explanation for the email that Mr. Brennan had found on his computer that morning.

[29] Mr. Cowan suspected that Mr. Sankreacha deleted the email after he received Mr. Brennan's telephone call that morning at about 7:00 a.m.

[30] Mr. Beach and Mr. Cowan decided to call the police. Mr. Beach and Mr. Brennan left and returned to their respective offices.

[31] Mr. Cowan advised Mr. Sankreacha that he could either leave or wait for the police. Mr. Sankreacha chose to remain.

[32] Mr. Cowan called the police at about 2:58 p.m. A transcript of this phone call was made an exhibit to the trial and forms the basis of several of Mr. Sankreacha's claims. In this phone call Mr. Cowan introduced himself as security for the Markham Canadian Tire store and made the following comments:

> We have an employee…it appears at this point he accessed an internal computer and downloaded some spyware on it and collected a whole

> bunch of personal information regarding the manager's, all of the manager's bank accounts as well as internal CTC Mastercard accounts and all of that. He has got a bit of a history of it from his past employer as well so I would like the police to come in.
>
> ...
>
> He basically downloaded a whole bunch of information like tons of CTC Canadian Tire account numbers, everything that would be on a computer from the mainframe he downloaded and sent it to his email. The forensic computer, forensic auditor came in today and confirmed that he was in fact in possession of it and when he is cautioned and then questioned about it he denied having using his account so he is definitely responsible for it and he has got a past before from doing the same thing in another company.
>
> ...
>
> I'm just going to give you the information in a second...he is not detained or anything, he is cooperating at this point.
>
> ...
>
> I don't know I have never been faced with this type of investigation but I know where there is possession of all this stuff that went to him well it's all in the paper so what basically happened is that the forensic computer guy came in and confirmed that all of this stuff went to his email address and it was the result of him installing software on the computer so there would be no other way for him to send all of this stuff to him unless you know he was the one who installed the software because it's going to his email account so he is definitely responsible for the theft of the information so they may call the detectives and there may be enough evidence to bring him in for it right because this involves all kinds of accounts.

[33] Police Constable Marshall of the York Regional Police came to the Markham Canadian Tire store at about 3:16 p.m. and spoke to Mr. Cowan, who showed him the email and the 48-page printout. P.C. Marshall then spoke with Mr. Sankreacha at 3:45 p.m. Mr. Sankreacha was calm and cooperative. P.C. Marshall placed Mr. Sankreacha under arrest for unauthorized possession of credit card data contrary to s. 342(3) of the *Criminal Code*. Mr. Sankreacha was handcuffed in the office and taken out to the police vehicle where he was read his right to counsel.

[34] P.C. Marshall testified that the decision to arrest and handcuff Mr. Sankreacha was his decision, and no one at the Canadian Tire store encouraged him to do this. He made this decision based on his review of the 48-page printout, which he believed included credit card information. He decided that there were reasonable and probable grounds to arrest Mr. Sankreacha.

[35] Prior to coming to the store, and pursuant to his usual practice, P.C. Marshall ran a Canadian Police Information Centre (CPIC) check on Mr. Sankreacha and discovered that Mr. Sankreacha had previously been charged with theft of data/mischief to data, but the charges had been withdrawn. P.C. Marshall testified that this factor did not have much weight in his decision to charge Mr. Sankreacha.

Discovery of the Thumb Drive on the Key Chain

[36] At this point Mr. Sankreacha's evidence differs markedly from the evidence of Mr. Cowan and P.C. Marshall, This difference is significant to each of the claims made in the Statement of Claim.

[37] Mr. Sankreacha testified that Mr. Cowan asked Mr. Sankreacha to turn over his store I.D. and his store key. Mr. Sankreacha was nervous, so he gave Mr. Cowan his entire wallet and his entire key chain, including his house key and his car key. He testified that when he gave the key chain to Mr. Cowan there was no USB key or "thumb drive" on the key chain.

[38] Mr. Sankreacha testified that Mr. Cowan gave the key chain to P.C. Marshall. When P.C. Marshall took Mr. Sankreacha to the police vehicle, he asked Mr. Sankreacha if that was his key chain. Mr. Sankreacha confirmed that it was. Mr. Sankreacha did not know that a thumb drive had been placed on the key chain, likely by Mr. Cowan, before it was handed to P.C. Marshall.

[39] Mr. Sankreacha testified that the thumb drive was not his and that he had never seen it before.

[40] Mr. Cowan testified that he was not aware that Mr. Sankreacha had a store key and denied asking Mr. Sankreacha for the store key. He denied receiving Mr. Sankreacha's wallet and key chain, and denied giving them to P.C. Marshall. Mr. Cowan testified that he did give P.C. Marshall an empty plastic shopping bag in which to place Mr. Sankreacha's personal items.

[41] P.C. Marshall testified that he took the key chain with the thumb drive on it directly from Mr. Sankreacha, although he was not certain whether that occurred in the office or at the police car. He asked Mr. Sankreacha whether these were his keys, and Mr. Sankreacha responded in the affirmative. P.C. Marshall returned the keys, but he seized the thumb drive and completed a Seized Property Report. Mr. Sankreacha was released at the scene on a "Form 9 Appearance Notice" (promise to appear) with a court date of July 27, 2010.

[42] P.C. Marshall's evidence in this regard was consistent with his contemporaneous notes, which state: "Asked accused if he drove to work today – Accused says yes. Pick up car key and say with these? Accused says yes. Take Thumb drive from car keys and lodge in property bag. Thumb drive black/silver."

[43] P.C. Marshall's evidence was also consistent with the report he prepared at the end of the day, which indicates that "the accused was searched before entering the police vehicle

and police located 1 thumb drive, black/silver in colour. The thumb drive was placed in evidence bag..."

[44] P.C. Marshall's only other involvement in the case was to request a warrant to search the thumb drive on February 14, 2011. He was not the officer in charge of the investigation, and his involvement in the case ended at that stage.

[45] The search of the thumb drive revealed that the KGB spyware was on the thumb drive and it could have been used to install the KGB spyware on Mr. Brennan's computer.

[46] After the charges against Mr. Sankreacha were withdrawn by the Crown in 2011, the thumb drive was not claimed by anyone and it was eventually destroyed by the police.

Mr. Sankreacha is Dismissed

[47] Mr. Beach testified that he believed that Mr. Sankreacha was responsible for downloading the KGB spyware after discussing the matter with Mr. Valencia. This belief was based on the fact that the email with the data captured by the KGB spyware appeared to have been sent from Mr. Sankreacha's personal Hotmail email account to Mr. Sankreacha's personal Hotmail email account on Mr. Brennan's computer.

[48] Mr. Beach decided to dismiss Mr. Sankreacha on June 21, 2010 when he learned that Mr. Sankreacha had been charged by the police.

[49] The following day Mr. Beach received a telephone call from Mr. Sankreacha's lawyer, who asked about Mr. Sankreacha's employment status. Mr. Beach told the lawyer to tell Mr. Sankreacha that he was no longer employed at the Markham Canadian Tire store.

Installation of the KGB Spyware

[50] The defendants called Mr. Jason Green as an expert in computer forensic examination in relation to hard drives. He was asked to examine Mr. Brennan's computer hard drive to determine whether spyware had been installed, how the spyware program got there, and where the information went.

[51] In order to conduct the examination, Mr. Green was given the whole computer and he made an image of the hard drive so as not to change the original.

[52] After examining the hard drive, Mr. Green confirmed that the "KGB Keylogger" had been installed and used to extract data from the system. He was, however, unable to conclude who had installed the program on the basis of his examination of the computer hard drive.

[53] Mr. Green determined that the KGB spyware had been installed on the system using a USB key on May 21, 2010. The USB key used to install the spyware was inserted at 14:56:21, and the KGB spyware was installed at 15:01:00. Mr. Green testified that it might take only one minute to install the program. The spyware program was then run at 15:35:33 on the same day, meaning that it was fully installed at that time. Nothing was

going on between 15:01 and 15:35 – the spyware was just sitting on the computer and waiting to be used.

[54] These times are important to the central issue in this case. The plaintiff argues that these times prove that he could not have been the person who installed the KGB spyware, while the defendants argue that these times prove that he was the person who installed the spyware. I will return to this question later in these Reasons.

[55] The KGB spyware is designed to be covert; there is no KGB icon on the screen, so a person using the computer would not know that it was installed. The KGB spyware can be purchased and downloaded from the internet.

[56] Once installed and running, the spyware acts as a "keylogger" by registering all keys pressed by a user and captures all data entered on the keyboard. The spyware also records all websites visited on the computer.

The Pin Pad Fraud – June 22, 2010

[57] On June 22, 2018, Canadian Tire Corporation Ltd. corporate security received a fraud alert from Moneris, which operated the credit card "pin pads" (the hand held electronic device used in debit and credit card transactions) in the Canadian Tire franchise stores. Canadian Tire Corporation Ltd. is a separate legal entity from the franchise stores, such as the Markham Canadian Tire store, the franchise owned by Mr. Beach.

[58] The fraud alert indicated that a pin pad in the automotive department at the Markham Canadian Tire store had been compromised. Corporate security advised the Markham store by telephone and the pin pad was immediately taken out of operation.

[59] Geoff Lawson, the Corporate Security Manager for Canadian Tire Corporation Ltd., attended the store on June 23, 2010. He met with Francis Tzigeris, the HR Manager of the Markham store, who gave him the automotive department pin pad. Mr. Lawson did not meet with or talk to anyone else in the store, and, in particular, did not meet with or talk to any of the defendants in this case. Mr. Lawson completed an integrity inspection of all the pin pads in the store, including the one in the automotive department. His inspection found obvious signs of tampering on the automotive department pin pad, including a foreign device (a skimming mechanism) behind the access panel located at the bottom of the pad. This device would record and transmit information collected by the pin pad, including the user's Personal Identification Number ("PIN") and the information contained on the card's magnetic strip. Both these pieces of information are necessary to make a counterfeit debit or credit card.

[60] Mr. Lawson noted that there was video surveillance at the store, but the camera did not provide a field of view of the pin pad station at the automotive department. There was, therefore, no video to show who might have installed the skimming mechanism on the pin pad. Mr. Lawson removed the pin pad and sent it for inspection. He also contacted the York Regional Police and filed an occurrence report.

[61] While Mr. Lawson was at the store on June 23, 2010, he was advised by Ms. Tzigeris that an employee of the store was arrested on June 21, 2010 in relation to an allegation that he put spyware on the automotive manager's computer. Mr. Lawson noted this in his report. He was not advised of the name of the employee or any other details surrounding the incident.

[62] The investigation by Moneris revealed that the skimming device was installed on the pin pad on or before May 21, 2010. The skimming began on May 21, 2010 and continued until June 21, 2010. The fraud activity took place on June 22, 2010, when the information collected from the pin pad was used to withdraw approximately $85,000 from several bank accounts across the GTA.

[63] The Moneris report was not communicated to anyone at the Markham franchise because the financial losses associated with the pin pad fraud are those of the credit card company and the bank; the franchisee has no liability for credit card fraud.

[64] On June 24, 2010, Mr. Lawson emailed a contact at the York Regional Police to alert them to the pin pad fraud and a possible connection between the spyware incident and the pin pad fraud. He stated:

> Hi Andrew, wanted to let you know about the incident with our Markham store. See the summary at the bottom and feedback from our financial services folks for risk to our Canadian Tire branded cards. The interesting note is that the store one day earlier had YRP [York Regional Police] attend and arrest of one of their employees was made as it is alleged that he put spyware software on the automotive manager's computer. Ironically this employee worked in the automotive service area, the same area that the compromised pin pad was located.

[65] Mr. Lawson took no further steps to identify the person who had tampered with the pin pad in the automotive department. He had no evidence that Mr. Sankreacha or any other employee at the Markham Canadian Tire store had been involved. Indeed, he had no evidence other than the compromised pin pad.

[66] It is fair to say that the staff at the Markham Canadian Tire store that heard about the pin pad fraud suspected that Mr. Sankreacha was involved. Their suspicion stemmed from several coincidences:

a) the coincidence of timing between Mr. Sankreacha's dismissal on June 21, 2010 and the discovery of the pin pad fraud on June 22, 2010;

b) the coincidence that the KGB spyware was installed on an automotive department computer and the skimming device was installed on an automotive department pin pad; and

c) the coincidence that the KGB spyware was installed on May 21, 2010, and the skimming activity on the pin pad also began on May 21, 2010.

[67] Mr. Sankreacha was not, however, ever questioned by the police with regard to the pin pad fraud and he was never charged in relation to that incident.

[68] In the end, no one was ever charged with the pin pad fraud, and Canadian Tire Corporation Ltd. does not know who was responsible. There was no evidence that any store employee was responsible for the pin pad fraud. The crime remains unsolved.

[69] The plaintiff called as an expert witness Mr. Len McGowan, a Senior Fraud Investigator of TD Bank Financial Group who is responsible for VISA and eBank investigations. He was qualified as an expert on counterfeiting of credit cards and skimming devices and schemes. He was involved in the investigation of the pin pad fraud at the Markham Canadian Tire store.

[70] Mr. McGowan testified that 103 bank cards had been compromised by collecting data ("skimming") from cards used on the Markham Canadian Tire store's automotive department's pin pad between May 21 and June 21, 2010. All of the money withdrawn was from various accounts across the Greater Toronto Area (GTA) in a "fraud run" on June 22, 2010.

[71] Mr. McGowan explained that this type of credit card fraud is a very involved process that is rarely, if ever, committed by one person acting alone. The scheme has three distinct parts: i) acquisition of data, ii) manufacture of cards, and iii) use of cards.

[72] In order to acquire the data, a person with technical knowledge and skill would have to obtain the pin pad from the store because it takes between one to two hours to install the skimmer. Usually the pin pad would be taken at the end of the day and replaced with a dummy pin pad, and then returned the next morning when the store is not busy.

[73] Once installed in the pin pad, the skimmer is capable of capturing the PIN entered by the customer, as well as the information that is encoded on the magnetic strip on the back of the debit or credit card. For the scheme to work, both the PIN number and the information on the magnetic strip are required – one is useless without the other.

[74] After acquiring the data from the skimmer, the perpetrator would have to manufacture a card with a magnetic strip containing the information skimmed from the pin pad. This would create a card that can be used at an ATM machine to obtain funds from the customer's account. This was a common scam between 2010 and 2012, before the introduction of chip technology on bank cards.

[75] Once the data was collected and the card manufactured, the perpetrator can use the completed counterfeit card to remove funds from the customer's account at an ATM machine. The perpetrators have a limited period of time to conduct a "fraud run" to acquire funds from bank ATM machines because the bank's computer will identify the fraud run and shut the cards down within about five minutes. As a result, the fraud run requires a number of people to use their cards at the exact same time at different locations. The perpetrators withdraw as much money as fast as they can on each card until the cards are shut down by the banks.

[76] In Mr. McGowan's opinion, the pin pad fraud incident in this case was not perpetrated by one person acting alone.

[77] Mr. McGowan testified that the information obtained from Mr. Brennan's computer and listed on the 48-page printout could not be used to manufacture fraudulent bank cards. In his view, the 48-page printout did not contain sufficient information, standing alone, to allow anyone to monetize or profit from it.

[78] Mr. McGowan testified that, in his experience, 99.5% of pin pad frauds are committed without involvement of employees, and that it would be very rare to have an employee involved. These frauds are usually perpetrated by a group of criminals external to the employer. In his opinion, the employees of the Markham Canadian Tire store were likely unaware that a device had been installed in the store.

[79] Mr. McGowan could offer no opinion as to the identity of the individual or individuals who tampered with the pin pad. He did not examine the pin pad device or interview any of the employees. He was never asked to investigate who committed the pin pad fraud.

B. Analysis

[80] The plaintiff relies on eight separate causes of action. I will address each one in turn. There is considerable overlap among the essential elements of each cause of action and certain factual findings are common to more than one of the claims raised.

1) Wrongful Dismissal

[81] The plaintiff takes the position that he was not responsible for the installation of the KGB spyware on Mr. Brennan's computer. He argues that the KGB spyware was actually installed by Mr. Brennan and Mr. Cowan, acting in concert. He alleges that Mr. Brennan and Mr. Cowan installed the KGB spyware on Mr. Brennan's computer and framed Mr. Sankreacha for one of two reasons:

i. to fabricate a cause to dismiss Mr. Sankreacha because he refused to "upsell" to customers in the automotive department; or

ii. to set Mr. Sankreacha up as a "decoy" or diversion for the pin pad fraud of June 22, 2010, which, the plaintiff alleges, was actually orchestrated by Mr. Brennan and Mr. Cowan. He alleges that Mr. Brennan and Mr. Cowan installed the KGB spyware on Mr. Brennan's computer and made it look like Mr. Sankreacha had installed it in order to cast suspicion for the June 22, 2010 pin pad fraud on Mr. Sankreacha.

[82] During the trial, the plaintiff's conspiracy theory was expanded to include Mr. Beach as a co-conspirator.

[83] This conspiracy theory is central to all of the claims made by the plaintiff. To a certain extent, the success of each cause of action hinges on the court's acceptance of one of these two theories.

[84] The defendant argues that Mr. Sankreacha was dismissed for installing KGB spyware on Mr. Brennan's computer, and that this, in itself, constituted just cause for the dismissal.

[85] While Mr. Beach and Mr. Cowan initially believed that the 48-page printout contained confidential customer credit card and Canadian Tire Mastercard information when they first reviewed it on June 21, 2010, there is no dispute that this was an error. The printout did not contain any customer credit card information or any Canadian Tire Mastercard information, although it did contain confidential banking information of one Canadian Tire employee. Accordingly, theft of confidential customer credit card and Canadian Tire Mastercard information is not advanced as a ground for dismissal.

[86] In addition, the defendants' Statement of Defence included a claim of "after-acquired cause", which alleged that Mr. Sankreacha was responsible for or involved in the June 22, 2010 pin pad fraud. This defence was formally withdrawn by the defendants at a pre-trial conference in April 2017, more than a year before the trial began. The defendants acknowledge that, notwithstanding the suspicions raised by the coincidences listed at para. 66 of these Reasons, there is no evidence linking Mr. Sankreacha to the pin pad fraud.

[87] By all accounts, Mr. Sankreacha was a valuable and dedicated employee who was well liked by Mr. Beach and Mr. Brennan. The only reason he was dismissed was the discovery of the KGB spyware on Mr. Brennan's computer and the conclusion that Mr. Sankreacha had installed it.

[88] Accordingly, there are only two issues in relation to the wrongful dismissal claim:

i. Have the defendants proven, on a balance of probabilities, that Mr. Sankreacha was responsible for the installation of the KGB spyware on Mr. Brennan's computer? and

ii. If the answer to the first question is yes, is the installation of KGB spyware on an employer's computer just cause for dismissal?

Who installed the KGB Spyware?

[89] Counsel for the defendant employer acknowledges that the burden of proof is on the employer when dismissal for cause is alleged. The employer must demonstrate, on a balance of probabilities, that it had just cause to terminate the employee's employment without notice or compensation in lieu of notice: *McKinley v. BC Tel,* 2001 SCC 38, [2001] 2 SCR 161, at para. 49*; De Jesus v. Linamar Holdings Inc. (Camcor Manufacturing)*, 2017 ONCA 384, at para. 7.

[90] The employer relies on the following evidence to support just cause:

[91] The password to Mr. Brennan's computer was known only to Mr. Brennan and Mr. Sankreacha.

[92] The email that opened on Mr. Brennan's computer when he logged on in the morning of June 21, 2010, was Mr. Sankreacha's personal Hotmail email account. The email displayed was from bharath_sankreacha@hotmail.com to bharath_sankreacha@hotmail.com. There is no dispute that this was the plaintiff's personal email address.

[93] The email account was opened on Mr. Brennan's computer the day prior, on the morning of Sunday June 20, 2010. Mr. Brennan was not at work on June 20, 2010. Mr. Sankreacha was at work from 8:30 a.m. to 12:00 p.m. and from 12:30 p.m. to 5:00 p.m. Mr. Sankreacha was the only Service Advisor at work from 8:30 a.m. until 10:00 a.m. This supports the defendant's position that it was Mr. Sankreacha who logged on to Mr. Brennan's computer on the morning of June 20, 2010, opened his Hotmail account and sent the email containing the attachment to himself.

[94] Since Mr. Brennan was not at the store on June 20, 2010, he could not have been the one to open his computer, log onto the plaintiff's personal email account, and then leave his computer on for 24 hours. There was no evidence that Mr. Brennan had remote access to his workplace computer or that any of these acts could have been performed remotely by Mr. Brennan. Moreover, it defies logic that Mr. Brennan would send the email on the morning of June 20, 2010 and leave the email open on his computer all day knowing that the plaintiff was at work that day and had access to Mr. Brennan's workplace computer throughout the day on June 20, 2010.

[95] In addition, if Mr. Brennan had sent the email to Mr. Sankreacha's email address on June 20, 2010, Mr. Sankreacha would have received the email and, not knowing what it was, brought it to someone's attention. Mr. Sankreacha's position is that he never received the email.

[96] The email included an attachment containing data collected on June 17, 2010. The data was collected using KGB spyware that had been installed on Mr. Brennan's computer using a USB key on May 21, 2010. The USB key used to install the spyware was inserted on May 21, 2010 at 14:56:21, and the KGB spyware was installed at 15:01:00. That program was then run at 15:35:33 on the same day.

[97] Both Mr. Brennan and Mr. Sankreacha were at work on May 21, 2010. Mr. Brennan was at work from 7:00 a.m. to 5:00 p.m. Mr. Sankreacha was at work from noon to 3:00 p.m., when he left for a 30 minute break to pick up his daughter from day care, and returned to work from 3:30 p.m. until 9:00 p.m.

[98] The defendants argue that the time of installation and running of the KGB spyware are critical. The timing suggests that Mr. Sankreacha inserted the USB key and installed the KGB spyware just before his 3:00 p.m. break, but was interrupted and had to leave the store. He returned to work at 3:35 and ran the spyware. Since Mr. Brennan was in the office from 7:00 a.m. to 5:00 p.m., there was no reason for a gap from 3:00 p.m. to 3:35 p.m., as he could have installed and run the spyware at any time without interruption.

[99] The plaintiff argues that the gap supports his theory of the case. He argues that Mr. Brennan waited until Mr. Sankreacha was on break to install and run the spyware.

[100] Based on the evidence I have reviewed, I find the defendants' theory more credible and consistent with the timelines provided.

[101] When Mr. Sankreacha was arrested by the police on June 21, 2010, the police found a USB key with the KGB spyware on his key chain. There are two explanations as to how the USB key got onto the key chain. P.C. Marshall testified that the USB key was on the key chain when he took it from Mr. Sankreacha. Mr. Sankreacha testified that the USB key was not his and that it must have been surreptitiously placed on his key chain by Mr. Cowan when he gave Mr. Cowan his key chain.

[102] Mr. Sankreacha's allegation that the USB key was planted by Mr. Cowan was not pled and particularized in the Amended Statement of Claim, but was raised for the first time at trial.

[103] Based on the evidence, I am satisfied on a balance of probabilities that the USB key was on Mr. Sankreacha's key chain when it was taken from Mr. Sankreacha by P.C. Marshall. There are three reasons for this conclusion. First, it is consistent with the evidence of P.C. Marshall, who testified that he took the key chain directly from Mr. Sankreacha. P.C. Marshall is not a party to this litigation, and there is no reason for him to not tell the truth about this. On the whole, I found P.C. Marshall's evidence to be credible. He acknowledged when he could not remember certain details, and his evidence on this point was consistent with the report he made at the end of the day.

[104] Second, I find Mr. Sankreacha's evidence on this point to strain credulity. Even if I accept Mr. Sankreacha's evidence that he was asked by Mr. Cowan to return his store key, it is unlikely that Mr. Sankreacha would have given Mr. Cowan his entire key chain, including his car and house keys, when asked only for his store key. Moreover, there is no way that Mr. Cowan could have anticipated that Mr. Sankreacha would hand over his entire key chain when asked for his store key. As such, it strikes me as very unlikely that Mr. Cowan would have been in a position to surreptitiously put the USB key on the key chain.

[105] The evidence indicates that Mr. Brennan called Mr. Sankreacha at approximately 7:00 a.m. on the morning of June 21, 2010 to ask him for an explanation about the email. Mr. Brennan testified that he called Mr. Sankreacha because he trusted him and thought that Mr. Sankreacha might have an innocent explanation for what Mr. Brennan saw on his computer.

[106] The defendants suspect that this "heads up" inadvertently gave Mr. Sankreacha an opportunity to erase the email before he came to work that day. That is why the email was no longer in Mr. Sankreacha's Hotmail account when he opened it from Mr. Issa's computer when confronted that afternoon by Messrs' Beach, Issa and Cowan.

[107] Mr. Sankreacha takes the position that Mr. Brennan's telephone call that morning was also part of the conspiracy. He takes the position that the email was never on his Hotmail

account, and that Mr. Brennan called him at 7:00 a.m. so that Mr. Brennan, Mr. Cowan and Mr. Beach would have an explanation as to why the email was not found when Mr. Sankreacha opened his Hotmail account in Mr. Issa's office. The difficulty that I have with this rather convoluted theory is that there is no dispute that the screen shot printed and made an exhibit is indeed an image of Mr. Sankreacha's Hotmail account. It includes all of the folders that he acknowledges were in his Hotmail account. No explanation or expert evidence was offered for how the screen shot could be an image of Mr. Sankreacha's Hotmail account, but the email was never in his Hotmail account.

[108] Some of these questions might have been answered if Mr. Sankreacha had retained his personal computer, but six months after he was dismissed he had his personal computer "recycled" and it was long gone by the time he issued his Statement of Claim. Mr. Sankreacha also acknowledged that he never contacted Hotmail to see if they could determine how or from where his Hotmail account was accessed on June 20, 2010.

[109] The plaintiff points out that while his email account was opened in Mr. Issa's office, the defendants did not ask him to open any of his folders. They were focused exclusively on finding the email. Had they opened the folders they would have discovered that the contents were innocuous and did not include any confidential credit card information as the defendants suspected. He argues that their failure to ask him to open the folders is evidence that they were setting him up – they did not ask to open the folders because then it would be known that there was no credit card data in Mr. Sankreacha's Hotmail account, and they would have no reason to call the police.

[110] The defendants argue that, at the time, they either did not know that they could open the folders or simply did not think of asking Mr. Sankreacha to open any of the folders other than his inbox and trash.

[111] In my opinion, it is hardly surprising that their exclusive focus was finding the email and that they did not think of asking Mr. Sankreacha to open other folders in his account. I accept the defendants' evidence in this regard and I do not agree that their failure to ask Mr. Sankreacha to open the other folders in his account is evidence that the defendants were involved in a conspiracy to set Mr. Sankreacha up as a patsy or decoy.

[112] Mr. Sankreacha's theory also begs the question of why Mr. Brennan, Mr. Cowan and Mr. Beach would want to delete all traces of the email from Mr. Sankreacha's account if they wanted to frame him. One would have thought that the better strategy would be to make sure that the email was in his account when he opened it in Mr. Issa's office that day.

[113] There is also considerable evidence that Mr. Sankreacha has a sophisticated knowledge of computers, and the requisite knowledge to download and operate the KGB spyware. He has taken computer science courses and has a diploma in AutoCAD and Computer Science from Farnborough College of Technology in England. He also worked with computers as a Systems Administrator at his previous employer. He acknowledged that he bought and sold computer parts on eBay. Furthermore, two former Canadian Tire employees testified that Mr. Sankreacha openly discussed his knowledge about computers and offered to assist co-workers with their computer problems.

[114] One former employee, Mr. Gavin Chow, testified that when his laptop could not boot up, he told Mr. Sankreacha and Mr. Sankreacha said he knew how to fix it. Mr. Chow gave the laptop to Mr. Sankreacha, and the laptop worked when Mr. Sankreacha returned it. Mr. Chow paid Mr. Sankreacha for his services. Mr. Chow had no reason to fabricate this story. In 2010 he was a student working part-time as a Service Advisor at the Canadian Tire store, but currently has no connection to Canadian Tire or any of the defendants. Mr. Sankreacha denied that this ever happened.

[115] A second employee, Mike Sue, testified that Mr. Sankreacha built him a home computer. Mr. Sue did not actually see the plaintiff build the computer, but Mr. Sue testified that the plaintiff told him he was going to build him a computer and then provided him with a computer. Mr. Sankreacha denied building the computer.

[116] In my opinion, Mr. Sankreacha deliberately understated his knowledge of computers during his testimony.

[117] In contrast, the evidence indicates that Mr. Brennan lacked the computer skills necessary to accomplish the elaborate conspiracy postulated by the plaintiff. Mr. Sue and Mr. Chow both testified that, in their experience working with Mr. Brennan, he had limited computer skills.

[118] Another important conflict in the evidence relates to the plaintiff's evidence that when he was in the Canadian Tire store on Sunday June 20, 2010, he could not have accessed Mr. Brennan's computer because another employee, Mr. Chow, was assigned by Mr. Brennan to prepare the store's promotional flyer using Mr. Brennan's computer. According to Mr. Sankreacha, Mr. Chow was in Mr. Brennan's office preparing the promotional flyer for 6 or 7 hours.

[119] Mr. Chow testified that while he would occasionally use Mr. Brennan's computer to print school assignments if he was working right before school, he was never asked by Mr. Brennan to prepare or print promotional flyers. He stated that he never prepared a promotional flyer for Canadian Tire because the flyers are professionally printed and are not prepared or printed "in-house" or in Mr. Brennan's office. He testified that he would have remembered if he had sat for 6 or 7 hours to make flyers. Again, Mr. Chow would have no reason to fabricate this evidence.

[120] Finally, for the plaintiff's position to make any sense at all there would have to be some motive for Mr. Brennan, Mr. Cowan and Mr. Beach to engage in an elaborate scheme to frame an employee who earned slightly more than minimum wage.

[121] As indicated above, the plaintiff has advanced two possible motives for the defendants wanting to frame him.

The "Upsell" Theory

[122] In his Amended Statement of Claim the plaintiff alleged that Mr. Brennan's compensation package included a profit sharing component that was based in part on the automotive department's sales. In order to increase sales, automotive department staff,

including Mr. Sankreacha, were encouraged to "upsell" to customers. The Amended Statement of Claim defines this as actively persuading customers they need additional services that may not be necessary. Mr. Sankreacha alleges that he refused to "upsell" and that this refusal jeopardized Mr. Brennan's ability to generate profit sharing revenue.

[123] The plaintiff alleges that as a result of his refusal to upsell, Mr. Brennan wanted to get rid of Mr. Sankreacha. In order to fabricate grounds for dismissal, Mr. Brennan, in combination with Mr. Cowan, devised the following plot: Mr Brennan gave Mr. Sankreacha his computer password in 2009 and permitted Mr. Sankreacha to use the computer at work. Mr. Brennan then downloaded the KGB spyware on to his own work computer, opened the plaintiff's Hotmail account with the plaintiff's user name and password somewhere away from the office using the internet, and attached the data generated by the KGB spyware to the plaintiff's Hotmail account to make it appear as though Mr. Sankreacha had sent an email to himself with the data. Mr. Brennan then pretended to find the email on his computer when he came to work on the morning of June 21, 2010. At the same time Mr. Brennan erased all traces of the email from Mr. Sankreacha's Hotmail account so that when Mr. Sankreacha accessed his Hotmail account in Mr. Issa's office on the afternoon of June 21, 2010 there would be no trace of the email that was on Mr. Brennan's computer in the morning. Mr. Brennan called Mr. Sankreacha at 7:00 a.m. so that when no trace of the email could be found on Mr. Sankreacha's Hotmail account, Mr. Cowan could claim that it was Mr. Sankreacha who erased it.

[124] In closing submissions, the plaintiff all but abandoned the upsell theory as Mr. Brennan's motive to frame him. In closing submissions, Mr. Jagtoo, counsel for Mr. Sankreacha, stated that upselling was a "small factor", "not an important factor", and "if it is a reason it is insignificant". Since it was not abandoned completely, I will address it.

[125] The plaintiff's evidence is that there was one source of disagreement between him and Mr. Brennan: upselling. The plaintiff points to his employee review of February 2007 as evidence of this disagreement. The employee review, which was prepared by Mr. Brennan, was generally positive. Mr. Sankreacha was rated "Superior" or "Good" in all categories. His "strengths" were listed as "customer service, very patient with customers and staff, handling issues". His "three areas to improve upon" were listed as "upselling, work on less time explaining to the customer, more overseeing on what is going in the garage when being duty manager".

[126] The 2007 employee review is the only reference to "upselling" as a weakness. For example, the 2010 employee review, also prepared by Mr. Brennan, lists Mr. Sankreacha's strengths as "excellent customer service, very personable and calm, reliable", and lists "three areas to improve upon" as "needs to keep time with customers shorter, leadership".

[127] I found Mr. Sankreacha's testimony on the issue of upselling to be very confused and confusing. Mr. Sankreacha worked at the service desk. His job was to act as a liaison between the customer and the mechanic. He would write down why the customer brought the car in for service and would communicate the mechanic's recommendations for

vehicle repair and maintenance to the customer. Mr. Sankreacha is not a mechanic and did not look at the cars.

[128] Mr. Sankreacha testified that there were two types of vehicle repair and maintenance: required repairs and maintenance and recommended repairs and maintenance. It was the mechanic's job to indicate which repairs and maintenance were required and which were recommended. For example, if a customer brought the car in for an oil change, the mechanic would conduct an inspection, and might recommend that the customer also get new brakes or new tires if the brakes or tires were worn. These could be "recommended" rather than "required" because they did not have to be done immediately, but might have to be done soon. This is what we would usually think of as preventative maintenance. Whether something was required or recommended was the decision of the mechanic based on his or her expertise. It would be up to the customer whether he or she wanted to proceed with the repairs and maintenance recommended by the mechanic.

[129] Mr. Sankreacha initially suggested that upselling was telling the customer that the recommended repairs or maintenance were required, and that he refused to do this. He then explained that communicating the recommendation was upselling, and Mr. Brennan told him that he had to communicate both the required maintenance and the recommended maintenance. He later changed this to mean that upselling meant trying to persuade customers to accept recommended repairs and that he refused to persuade customers, although he did communicate the mechanic's recommendations. He stated that he would only tell the client what the mechanic had recommended, but "would not go beyond that". He explained that telling customers what was recommended by the mechanics was not upselling, so he would tell the client what the recommendation was, but would not explain why the recommendation was made. For example, if the mechanic recommended that the vehicle needed an alignment, he would communicate that information to the customer, but refuse to explain to the customer why the additional service is recommended. He then stated that making the recommendation was not upselling, but convincing or explaining to the customer was upselling. He explained that he always recommended, but did not go beyond that by encouraging the customer.

[130] Mr. Sankreacha acknowledged that there was no record of what he did or did not do to "persuade" customers to accept recommended service or maintenance. The work order would set out what was necessary and what was recommended and indicate whether the customer accepted or declined the recommended service/maintenance. There was, however, no report or tracking of "upsell" activity as Mr. Sankreacha defined it. There were no records of whether any Service Advisor tried to "convince" a customer to accept recommended repairs or maintenance, and no report that tracked the success or failure rate of any employee with respect to customer acceptance of recommended repairs or maintenance.

[131] Mr. Sankreacha's evidence with respect to the meaning of "upselling" was inconsistent with the evidence of all the other current and former automotive department employees who testified. They testified that "upselling" meant communicating the mechanic's maintenance recommendations to the customer. If the customer had questions about the recommendations, the customer would often speak directly to the mechanic who made it.

None of the witnesses were aware that Mr. Sankreacha refused to "upsell" as they understood the word.

[132] Mr. Brennan explained that his reference to upselling in Mr. Sankreacha's 2007 employee review related to a single incident in which a customer complained that his tires wore out prematurely and that Mr. Sankreacha had failed to recommend a wheel alignment when he brought his car in for service. Apart from this incident, Mr. Brennan was unaware that Mr. Sankreacha had ever failed or refused to make the appropriate recommendations or "upsell". There was no reference to upselling on Mr. Sankreacha's subsequent employee reviews and Mr. Brennan thought that since 2007 Mr. Sankreacha had done a good job of upselling.

[133] Mr. Brennan noted that there were no targets for upselling and no way to track or record whether any Service Advisor was upselling. Both Mr. Beach and Mr. Brennan testified that if an employee refused to upsell he would not be dismissed, but the employee would be transferred to a different department within the store. The Markham Canadian Tire store had approximately 100 employees and Mr. Sankreacha worked in three different departments during his four years at the store. If Mr. Sankreacha had refused to upsell, it would be a simple matter to transfer him back to one of these departments.

[134] The evidence does not support Mr. Sankreacha's definition of "upsell" and it does not support his contention that he refused to "upsell", whatever definition is used. Assuming that Mr. Sankreacha's definition of "upsell" is correct, and he was refusing to explain to customers why the mechanic was recommending service such as a wheel alignment or coolant change, and assuming that Mr. Brennan had any knowledge of this refusal, I would fully expect to see some reference to this refusal on Mr. Sankreacha's 2010 employee review. Instead, the 2010 employee review, written by Mr. Brennan, commends Mr. Sankreacha for "excellent customer service". If Mr. Brennan was intent on dismissing Mr. Sankreacha, a negative employee review would be a much easier tack than the convoluted computer conspiracy advanced by Mr. Sankreacha.

[135] In my view, the evidence does not support the allegation that Mr. Brennan had any concern, let alone knowledge, of Mr. Sankreacha's alleged refusal to upsell. Nor does the evidence support the allegation that this alleged refusal had anything to do with his dismissal, or that it could have provided any motive for Mr. Brennan or Mr. Cowan or Mr. Beach to conspire against Mr. Sankreacha.

The Pin Pad Fraud Diversion Theory

[136] The second motive alleged by the plaintiff was to set Mr. Sankreacha up as a "decoy" or diversion for the pin pad fraud of June 22, 2010, which the plaintiff alleges was actually committed by Mr. Beach, Mr. Brennan and Mr. Cowan. The plaintiff argues that to help get away with the pin pad fraud, Mr. Beach, Mr. Brennan and Mr. Cowan installed the KGB spyware on Mr. Brennan's computer and made it look like Mr. Sankreacha had installed it in order to cast suspicion for the June 22, 2010 pin pad fraud on Mr. Sankreacha and "inoculate Messrs. Cowan and Brennan from blame or investigation".

[137] In his closing submissions the plaintiff alleged that Mr. Brennan, Mr. Cowan and Mr. Beach "were motivated by an improper purpose – to earn money from the sale of debit and credit card data to organised crime".

[138] This allegation is not in Mr. Sankreacha's Amended Statement of Claim. The Amended Statement of Claim, at para. 45e(xv), alleges only that Mr. Beach had knowledge of the pin pad fraud on June 23, 2010 and failed to tell the police that the plaintiff was not involved. The conspiracy alleged in the Amended Statement of Claim, at para. 45e(xvi), is the alleged conspiracy of the defendants to withhold exculpatory evidence from the police.

[139] Nowhere in the Amended Statement of Claim does Mr. Sankreacha allege that Mr. Brennan, Mr. Cowan, and/or Mr. Beach had any involvement in, or foreknowledge of, the pin pad fraud. Mr. Beach is not named as a defendant in the action. The defendants object to Mr. Sankreacha making this allegation as part of his case without having pled it. They argue that they were ambushed by this new theory at the beginning of the trial.

[140] The issues in a civil action must be decided within the boundaries of the pleadings. In *Musicians' Pension Fund of Canada (Trustees of) v. Kinross Gold Corp.*, 2014 ONCA 901, the Ontario Court of Appeal held, at para. 84:

> As this court has consistently emphasized, it is central to the litigation process that issues in a civil action be decided within the boundaries of the pleadings. Fundamental fairness and the efficacy of the civil litigation process demand no less.

[141] Similarly, in *Wilson v. Beck*, [2013] ONCA 316, leave to appeal to S.C.C. refused, [2013] S.C.C.A. No. 300, at para. 27, MacPherson J.A. set out the principle that "[i]t is fundamental to the litigation process that lawsuits be decided within the boundaries of the pleadings." This principle is frequently repeated: see *Holmes v. Hatch Ltd.*, 2017 ONCA 880, at para. 7, and *460635 Ontario Limited v. 1002953 Ontario Inc.*, 127 O.A.C. 48 (C.A.), 1999 CanLII 789 (ON CA), at para. 9.

[142] The same principle has been affirmed by the Supreme Court of Canada in *Lax Kw'alaams Indian Band v. Canada (Attorney General)*, 2011 SCC 56, at para. 43:

> Pleadings not only serve to define the issues but give the opposing parties fair notice of the case to meet, provide the boundaries and context for effective pre-trial case management, define the extent of disclosure required, and set the parameters of expert opinion. Clear pleadings minimize wasted time and may enhance prospects for settlement.

[143] I agree with the defendants that the allegation that Mr. Brennan, Mr. Cowan and Mr. Beach committed or orchestrated the pin pad fraud, and that they framed the plaintiff on June 21, 2010 in order to use him as a decoy or diversion from the fraud run on June 22, 2010, is not pleaded in the Amended Statement of Claim. Accordingly, it would not be fair to make any finding of liability and resulting damages against a defendant on a basis that was not pleaded in the statement of claim.

[144] That said, I should add that in my view, the plaintiff has advanced no evidence to support his allegation that Mr. Brennan, Mr. Cowan or Mr. Beach, together or individually, had any involvement in the pin pad fraud. In the absence of such evidence, there is no basis to conclude that involvement in the pin pad fraud provided the defendants with a motive to frame or conspire against Mr. Sankreacha.

[145] This finding is relevant to a number of the causes of action raised by Mr. Sankreacha, that rely on a finding of bad faith or malice as an element of the claim. To the extent that the plaintiff's claims are premised on his pin pad fraud diversion theory, each of these claims must fail, even if the pin pad fraud diversion theory were properly pleaded.

Conclusion Re: Proof of Just Cause

[146] Based on the foregoing analysis, I find that the defendants have proven, on a balance of probabilities, that Mr. Sankreacha was responsible for the installation of the KGB spyware on Mr. Brennan's computer.

Was Installation of the KGB Spyware Just Cause for Dismissal?

[147] The second question is whether the installation of KGB spyware on an employer's computer is just cause for dismissal?

[148] In closing submissions, plaintiff's counsel acknowledged that, if the allegation were true, downloading and installing spyware on an employer's computer was sufficiently serious to warrant dismissal. His position is that the employer had not met its onus of proving that Mr. Sankreacha was responsible.

[149] In *Dowling v. Ontario (Workplace Safety and Insurance Board)* (2004), 246 D.L.R. (4th) 65 (C.A.), at paras. 49-50, leave to appeal to S.C.C. refused, [2005] S.C.C.A. No. 25, the Ontario Court of Appeal, following the Supreme Court of Canada's decision in *McKinley v. BC Tel*, 2001 SCC 38, held that the core question in wrongful dismissal claims is whether the employee's misconduct was sufficiently serious that it struck at the heart of the employment relationship. To answer this question, the court must:

1. determine the nature and extent of the misconduct;

2. consider the surrounding circumstances; and

3. decide whether dismissal was warranted.

[150] See also *Fernandes v. Peel Educational & Tutorial Services Limited (Mississauga Private School)*, 2016 ONCA 468.

[151] In *McKinley*, at para. 48, the Supreme Court stated that one way to express the test is "that just cause for dismissal exists where the dishonesty violates an essential condition of the employment contract, breaches the faith inherent to the work relationship, or is fundamentally or directly inconsistent with the employee's obligations to his or her employer."

[152] The Supreme Court mandated a "contextual approach", which involves an examination of "both the circumstances surrounding the conduct as well as its nature or degree": *McKinley*, at paras. 34 and 51. When examining whether an employee's conduct – including dishonesty – justifies the employee's dismissal, the question to be addressed is whether, in the circumstances, the behaviour was such that the employment relationship could no longer viably subsist: *McKinley*, at para. 29. The Supreme Court stated, at para. 57:

> I favour an analytical framework that examines each case on its own particular facts and circumstances, and considers the nature and seriousness of the dishonesty in order to assess whether it is reconcilable with sustaining the employment relationship. Such an approach mitigates the possibility that an employee will be unduly punished by the strict application of an unequivocal rule that equates all forms of dishonest behaviour with just cause for dismissal. At the same time, it would properly emphasize that dishonesty going to the core of the employment relationship carries the potential to warrant dismissal for just cause.

[153] In certain contexts, the court directed at para. 51, that this contextual approach leads to a "strict outcome":

> Where theft, misappropriation or serious fraud is found, the decisions considered here establish that cause for termination exists.

[154] The Supreme Court noted: "[a]n effective balance must be struck between the severity of an employee's misconduct and the sanction imposed": *McKinley* at para. 53.

[155] In my view, the surreptitious installation of spyware on an employer's computer constitutes a clear breach of faith or trust inherent in the work relationship. It "violates an essential condition of the employment contract" and "breaches the faith inherent to the work relationship": *McKinley*, at para. 30.

[156] This was not a case of an employee simply using a work computer to access his personal email or the internet for personal purposes. This is not even a case in which an employee uses his credentials to access confidential information for personal purposes: see *Steel v. Coast Capital Savings Credit Union*, 2015 BCCA 127, 383 D.L.R. (4th) 481; *Carias v. CIBC,* 2003 BCSC 587. In this case, the employee surreptitiously installed spyware on the employer's computer that had only one purpose: the wholesale collection of the employer's or his co-workers' confidential information.

[157] It matters not in these circumstances that most of the information collected on June 17, 2010 was inconsequential. The evidence indicates that the spyware was running for one month prior to the date of its discovery by Mr. Brennan, and we cannot know what other information was collected. We do know that the data collected on June 17, 2010 included the confidential banking information of one of Mr. Sankreacha's co-workers.

[158] The evidence indicates that this was neither a single incident nor a momentary lapse of judgment. The installation of the spyware took considerable planning and subterfuge. It