Court File No. CV-14-507120

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N:

THE CATALYST CAPITAL GROUP INC.

Plaintiff

- and -

BRANDON MOYSE and WEST FACE CAPITAL INC.

Defendants

AFFIDAVIT OF HAROLD BURT-GERRANS
(Sworn March 9, 2015)

I, HAROLD BURT-GERRANS, of the City of Kitchener, in the Province of Ontario, MAKE OATH AND SAY:

1. I am the Director of eDiscovery and Litigation Support at H&A eDiscovery Inc. ("**H&A**"), a consulting company that specializes in electronic discovery ("**eDiscovery**") and advanced digital forensics.

Expertise

2. H&A is a leader in providing consulting services related to eDiscovery and computer forensics. We are regularly called upon to review and analyse data from electronic devices, including desktop and laptop computers, network servers and personal electronic devices like smartphones and tablets.

3. Since graduating with an Honours Bachelor degree in Computer Science in 1984, I have developed over 30 years of experience in application development,

technology management, computer forensics and electronic discovery. In my position as Director of eDiscovery and Litigation Support, I manage all facets of computer forensic investigations for our clients. My experience includes preservation of electronic data, analysis of computer hardware (including hard drives and portable storage media such as USB drives) and data found thereon, and recovery of deleted electronic data from all manners of storage media.

4. On behalf of H&A, I have acted as an independent eDiscovery specialist by *amicus curiae* before the Quebec Superior Court of Justice in relation to two major inquiries. I have also instructed the Institute of Law Clerks of Ontario's course on "eDiscovery—Advanced Theory and Practices for Litigation Support Personnel". A copy of my curriculum vitae is attached as **Exhibit "1"** to my affidavit.

5. In making this affidavit, I have reviewed the affidavits sworn by Martin Musters, Director of Forensics at Computer Forensics Inc. on June 26, 2014 and February 15, 2015 (the "**Musters Affidavits**"). I have also reviewed the draft and final reports of the Independent Supervising Solicitor, Stockwoods LLP (the "**ISS**").

Our Retainers

6. On January 23, 2015, Dentons Canada LLP, counsel for the Defendant, West Face Capital Inc. retained H&A to act as a computer forensic expert in this matter. A copy of our retainer letter is attached as **Exhibit "2"**. Pursuant to our retainer, H&A has made forensic images of Mr. Moyse's desktop computer hard drive, hard drives from West Face's servers accessed by Mr. Moyse, and West

Face's email traffic from March 27, 2014 to January 13, 2015. My analysis of the data thus preserved is set out below.

7. Before our retainer by Dentons, H&A had been retained in July 2014 by Mr. Moyse's counsel, Grosman, Grosman & Gale LLP ("GGG"), to make a forensic image of Mr. Moyse's personal electronic devices (laptop, iPad and Samsung Android smartphone device), as well as capture the contents of two personal email accounts of Mr. Moyse. I did not analyze the data that I had preserved other than to ensure that the imaging software had confirmed that the images were accurate. We were directed by Jeff Hopkins of GGG to provide the forensic images created to the forensic expert for Stockwoods LLP on December 18, 2014, which we did. The other copy of the forensic image was provided to GGG on December 22, 2014. We did not retain any copies of the images created, as instructed. A copy of H&A's retainer letter with GGG (the "GGG Retainer") is attached **Exhibit "3"** to my affidavit.

My Investigations on Behalf of West Face

8. Our forensic analyses of West Face's computer systems included: Mr. Moyse's desktop computer, West Face's network servers, cloud storage services, and West Face's mail system. I will first explain my preservation work in respect of these various sources of data. I will then discuss my analyses of the data so preserved.

(a) Forensic Preservation

9. On January 29, 2015, I created a forensic image of the hard drive of Mr. Moyse's desktop computer at West Face. Chap Chau, West Face's Head of Technology, identified Mr. Moyse's computer for me and confirmed that Mr. Moyse's computer had not been assigned to another user after he was placed on indefinite leave on July 16, 2014. We created the forensic image by physically removing the hard drive from Mr. Moyse's computer and capturing a forensic image of the hard drive using a "write blocker" device that ensures that the process of copying the entire contents of the hard drive does not alter any of its contents.

10. Whenever a user of West Face's computer system opens certain file types (most commonly Microsoft Office documents and Adobe PDF documents), the computer system will create a link on the user's hard drive. This process is automatic and invisible to the user. This "link file" contains information about what file was accessed, where on West Face's servers the file was stored, and the time and date of access. This lets a forensic expert identify documents that were accessed by the user. Using these link files, I extracted from forensic images of West Face's servers documents that Mr. Moyse had accessed, created or modified during his employment at West Face.

11. As a safeguard for the search I just described, I performed a second search. The most common document types (again, like Microsoft Office or Adobe PDF documents) contain "metadata" that tells, among other things, who authored or last edited the document. I therefore searched the West Face file servers for

metadata that identified any documents created or modified during the period June 23 to July 16, 2014 by Mr. Moyse.

12. West Face uses a "cloud-based" email system. All emails are stored remotely on Microsoft servers and are accessed by West Face over the Internet. When a user opens Outlook, a file called an "OST" is created on the user's computer. The OST contains the current contents of the user's email folders. As email comes in and out of Microsoft's email servers, the OST synchronizes and ensures the user's email folders remain up to date so long as Outlook is running.

13. I attended at West Face's offices on January 29, 2015 and watched as Mr. Chau logged in to a Microsoft administrator's tool only accessible to IT department employees. Mr. Chau then downloaded all the items for all then-active West Face users for the period of March 27, 2014 to January 13, 2015. The items were stored in a file called a "PST" for each mailbox on the West Face system. Once the download was completed, I created a forensic image of the PST files in question. Mr. Moyse's email account was included in this forensic image as an active user, because West Face has not deactivated his email account.

14. Finally, I understand that for a number of former West Face employees, Mr. Chau extracted PST files at the time of their departure and saved the PSTs to West Face's backup server. Mr. Chau also gave me the PST files from West Face's backup server for Alex Singh, West Face's former general counsel; Alex Goston, a former summer intern; Sara Yarmand, an administrator who performed risk management services; and Heather Miles, a receptionist.

(b) **Mr. Moyse's Desktop Computer**

1. **Log In Data for Desktop Computer**

15. As a preliminary matter, it is important to explain how I was able to identify when Mr. Moyse accessed documents on the West Face computer system, and how I checked to see if anyone else had accessed his computer. As at most workplaces, all West Face employees have a unique user ID and password. I am advised by Mr. Chau that West Face's policy requires all users to keep their password confidential and to not share it with anyone. To log in to West Face's computer system, either at the user's computer or remotely from outside the office, a user must enter his or her unique user ID and password. Every log-in is recorded on the computer from which the log-in occurs so that it can be determined who logged in, and at what time and date, for any particular computer on the West Face network.

16. My first step in analyzing the forensic image of Mr. Moyse's computer hard drive was to determine who had logged in to his computer from June 23, 2014 to July 16, 2014 (the period that I am advised Mr. Moyse worked at the office of West Face). I extracted this log-in data from the records maintained on Mr. Moyse's computer as described above. According to the log-in data, the only users who logged onto Mr. Moyse's computer were the user ID issued to Mr. Moyse and the user ID issued to Danny Yu who, I have been advised by Mr. Chau, is a West Face IT analyst. Attached as **Exhibit "4"** is a spreadsheet listing all log-ins recorded at Mr. Moyse's computer.

17. After July 16, 2014, no user logged in to Mr. Moyse's computer until December 15, 2014 when the user ID issued to Mr. Chau was used to log in. I am advised by Mr. Chau that he logged on to Mr. Moyse's computer on that date in order to create a backup of Mr. Moyse's profile. At that same time, various outstanding software upgrades occurred which had not previously occurred, most likely because the computer had been turned off since August 28, 2014. A user profile consists of documents located in default file locations (such as "My Documents"), system settings, and Internet browser bookmarks and history. I am advised by Mr. Chau that he logged on to Mr. Moyse's computer again on January 14 and 26, 2015 to confirm that the system was still working, that data has been properly preserved, and that no one else had logged on.

18. Based on my analyses, other than these three log-ins by Mr. Chau, I have found no evidence that any other users have logged in to Mr. Moyse's computer since July 16, 2014.

2. No User Deletion of Data

19. I have also analysed Mr. Moyse's computer to assess Mr. Chau's representation to me that nothing had been deleted from Mr. Moyse's computer since June 23, 2014. I did this by using forensic tools to analyze records that are left on a computer when files are deleted. Those records did not indicate that any user had deleted any files on Mr. Moyse's computer. The only record of deleted files were system and temporary files that are automatically created and deleted by standard operating system and application software like Microsoft Office and Windows. These deletions are not initiated by the user.

20. While it is possible to delete files without leaving any record of doing so, it requires an extremely sophisticated computer technician to do so. In my experience, the average computer user does not have the requisite level of sophistication.

3. No Copying of Data from or to Storage Media

21. I searched the forensic image of Mr. Moyse's computer for any evidence that a user copied data from or to an external storage device (such as a USB key, external hard drive, or smartphone) during the period of June 23, 2014 until July 16, 2014.

22. When an external device is plugged into the USB port of a computer for the first time, it creates a digital "footprint" on the hard drive that records the serial number of the device, as well as the date of the first use. Again, while such records can be deleted without leaving a record of doing so, in my experience only the most sophisticated users know how to do so. I conducted a forensic analysis of the hard drive from Mr. Moyse's computer looking for those footprints. I found no evidence that any external drive or storage media was connected to the USB port of Mr. Moyse's computer.

23. Similarly, when a device like an internal hard drive or a CD/DVD-ROM is added to a computer, it creates a "footprint" on the computer's hard drive. My forensic analysis of the hard drive from Mr. Moyse's computer found no evidence that any such devices were mounted on Mr. Moyse's computer on or after June 23, 2014.

4. Documents Accessed from Mr. Moyse's Desktop Computer

24. I have provided to West Face's counsel at Dentons Canada LLP via secure Internet link all documents with evidence of having been created, modified or accessed by Mr. Moyse, as identified by the two distinct processes I have described above in paragraphs 10 and 11.

(c) No Access to Dropbox from Desktop Computer

25. In addition to storing data on servers, computers or removable storage devices it is now possible to store files by using so-called "cloud" storage. Cloud storage just means that data is stored remotely from the user on a third party's server. The advantage of cloud storage is that users can access their data from anywhere with an Internet connection, and that specialized cloud storage providers can often provide better security than a typical employer. There are a number of web-based applications that offer this service, one of which is called Dropbox. If a document in the Dropbox folder on the hard drive of a computer is changed, Dropbox will automatically synchronize the computer files with the other devices that are associated with the Dropbox account.

26. I analysed Mr. Moyse's computer using three methods to determine if any user accessed a Dropbox account between June 23 and July 16, 2014. First, I looked for any evidence that the Dropbox program had been installed on the computer. Second, I searched the hard drive of Mr. Moyse's computer for any evidence of a Dropbox folder on the hard drive. Third, I reviewed Internet history records and conducted keyword searches for "dropbox", "box.com", "box.net", "onedrive", "googledrive" and "iCloud", looking for any record of accessing any of these services over the Internet from June 23, 2014 to July 16, 2014. With one

exception that I explain below, I found no record of any access to any of these services from Mr. Moyse's computer during the period in question.

27. In the course of my forensic review of the Internet history records for Mr. Moyse's computer, I found evidence that on July 10, 2014 or July 11, 2014, a web file sharing service called "Box.com" was accessed from the computer. I am unable to determine the content of the account or what documents were accessed. I am informed by Philip Panet, internal counsel to West Face, that emails relating to Mr. Moyse's use of this Box account have been provided to counsel to the plaintiff and will be attached to the affidavit of Tony Griffin.

(d) Emails to or From West Face from Moyse' Accounts

28. As noted above, West Face uses a "cloud" based email system offered by Microsoft, which hosts West Face's email. I have described above in paragraphs 13 and 14 how Mr. Chau and I extracted emails from West Face's email accounts. All existing emails to or from Mr. Moyse's West Face email account were preserved in a single PST file as a result of the extraction process.

29. In addition, using the PST files of other users extracted from the West Face email system as described above, I searched for all existing West Face email traffic involving Mr. Moyse's known personal email addresses on gmail.com or Hotmail.com. I have provided the emails identified using this search to West Face's counsel.

30. Attached as **Exhibit "5"** is a signed Acknowledgment of Expert's Duty form, which I signed prior to swearing this affidavit.

SWORN before me at the City of Toronto in the Province of Ontario this 9th day of March, 2015)

Commissioner for Taking Affidavits, etc.
Matthew McNamara

HAROLD BURT-GERRANS

THE CATALYST CAPITAL GROUP INC. Plaintiff/Moving Party	and	BRANDON MOYSE and WEST FACE CAPITAL INC. Defendants/Responding Parties	Court File No. CV-14507120

ONTARIO
SUPERIOR COURT OF JUSTICE

Proceeding commenced at Toronto

AFFIDAVIT OF HAROLD BURT-GERRANS
(Sworn March 9, 2015)

DENTONS CANADA LLP
77 King Street West, Suite 400
Toronto, ON M5K 0A1

Jeff Mitchell LSUC#40577A
Andy Pushalik LSUC#54102P

– AND –

DAVIES WARD PHILLIPS & VINEBERG LLP
155 Wellington Street West
Toronto ON M5V 3J7

Matthew Milne-Smith LSUC#: 44266P
Andrew Carlson LSUC#: 58850N
Tel: 416.863.0900
Fax: 416.863.0871

Lawyers for the Defendant/Responding Party,
West Face Capital Inc.