

12581
35

Court File No. CV-14-507120

ONTARIO
SUPERIOR COURT OF JUSTICE

BETWEEN:

THE CATALYST CAPITAL GROUP INC.

Plaintiff

- and -

BRANDON MOYSE and WEST FACE CAPITAL INC.

Defendants

AFFIDAVIT OF KEVIN LO
AFFIRMED APRIL 2, 2015

I, Kevin Lo, of the City of Toronto, SOLEMLY AFFIRM AS FOLLOWS:

1. I am a managing director with Froese Forensic Partners LLP ("**FFP**"). FFP was engaged by Paliare Roland Rosenberg Rothstein LLP ("**Counsel**"), on behalf of Mr. Brandon Moyse ("**Moyse**"), to provide our professional services in relation to this matter. A copy of my curriculum vitae is attached as **Exhibit "A"** to this affidavit. I attach a signed Acknowledgment of Expert's Duty, which I signed prior to swearing this affidavit, as **Exhibit "B"**.
2. As a result of the work done by FFP in this engagement, I have knowledge of the matters set out in this affidavit. To the extent that my knowledge is based on information and belief, I identify the source of such information and believe the information to be true.
3. I worked directly on the matters described in this affidavit. I was assisted throughout the process by my colleague Barry Kuang, a managing consultant with FFP.

4. For the purpose of our review and obtaining an understanding of the matter, we were provided with the report of the Independent Solicitor Supervisor ("ISS"), dated February 17, 2015, and the affidavits/reports of Marty Musters ("**Musters**") at Computer Forensics Inc., who I understand to be the forensic expert retained by the Catalyst Capital Group Inc., the plaintiff in this matter.

5. We understand that Digital Evidence International Inc. ("**DEI**") was retained by the ISS to assist with the collection, analysis, and reporting of the relevant electronically stored information ("**ESI**").

6. FFP was provided with the forensic images of relevant devices belonging to Moyse (i.e., desktop computer and mobile devices) for the purpose of our analysis.

The "Secure Delete" Issue

7. In its report, the ISS noted that Moyse apparently purchased two software products in July 2014: one called "RegClean Pro" and the other called "Advanced System Optimizer 3" ("**ASO**"), both of which are created by Systweak Software.

8. The ISS also noted the existence of a folder called "Secure Delete" on Moyse's computer. A program called "Secure Delete" is one of many programs packaged into the ASO product, which can be described as a "software suite". The ISS reported as follows with respect to the folder, at paragraph 45 of its report:

On July 20, 2014 at 8:09 p.m., a folder entitled "Secure Delete" was created, which suggests that a user of Moyse's computer took steps to make the use of that function available at that point in time.

9. The ISS ultimately reached the following conclusion with respect to the existence of the "Secure Delete" folder on Moyse's computer, at paragraph 48 of its report:

...DEI cannot determine whether or not the Secure Delete function may or may not have been used to delete an individual file or files and this report accordingly cannot express any conclusion on that possibility other than to note that it exists.

10. In his affidavit of February 15, 2015, Musters concluded that the existence of a "Secure Delete" folder would indicate that someone had executed Secure Delete and that files and folders were deleted as a result:

- (a) "In my own experience using the Secure Delete feature, merely downloading and installing the software on one's computer does not lead to the creation of a folder entitled "Secure Delete". That folder is only created when a user runs the Secure Delete feature to delete a file or folder from his computer." [para. 12]
- (b) "Based on my own experience using this software, it is my opinion that someone using Moyse's computer on July 20, 2014 deleted one or more files or folders beginning at 8:09 p.m. Based on my experience using this software, there is no other explanation as to why a "Secure Delete" folder would be created on Moyse's personal computer on that date." [para. 13]

138²⁵⁹⁴

-4-

11. Counsel asked FFP to conduct our own independent analysis and to provide an opinion on the conclusions Musters and the ISS reached with respect to the "Secure Delete" folder on Moyse's computer.

12. As part of our independent analysis, FFP purchased and installed the ASO and RegClean Pro software on a Microsoft Windows computer ("**Test Computer**").

13. We launched Secure Delete on the Test Computer. We observed that a folder named "Secure Delete" was created in the following file path: *\Users\Brandon Moyse\AppData\Roaming\Systweak\ASO3\Secure Delete*, as soon as we launched Secure Delete. In other words, the Secure Delete folder was created as soon as we clicked Secure Delete on the ASO menu, but before it was used for any other purpose. Therefore, contrary to the statement at paragraph 12 of Musters' affidavit, simply launching Secure Delete creates a "Secure Delete" folder. We did not have to take any other step, including deleting a file, in order to create a "Secure Delete" folder.

14. Next, we attempted to determine whether we could reach any conclusions as to whether or not Moyse used Secure Delete to delete any files from his computer.

15. In order to do so, we used Secure Delete on the Test Computer to delete a number of files. As we deleted the files, we observed that Secure Delete created a "log" which maintained records of the files deleted (the "Secure Delete Log"). A copy of the Secure Delete Log generated by our use of Secure Delete on the Test Computer is attached as

Exhibit "C" to this affidavit. The Secure Delete Log was located in the user registry at the following location:

HKEY_CURRENT_USER\Software\Systweak\aso3\Secure Delete

The Secure Delete Log records the following information when Secure Delete is used to delete one or more files:

- (a) NumOfItemsWiped
- (b) NumOfItemsWipedTillDate
- (c) LastWipeDateFileFolder
- (d) SpaceOfItemsLastWiped
- (e) FileFolderWipeStatusLine1
- (f) FileFolderWipeStatusLine2
- (g) WipeSettingMethod

16. We then analyzed the forensic image of Moyse's computer. As an initial matter, we confirmed the finding from the ISS's report that a "Secure Delete" folder existed on Moyse's original computer. Moyse's computer has a "Secure Delete" folder in the same location as the Test Computer, that is:

\Users\Brandon Moyse\AppData\Roaming\Systweak\ASO3\Secure Delete

We were also able to confirm the ISS's report that the "Secure Delete" folder appears to have been created on Moyse's computer on July 20, 2014 at approximately 08:09 p.m.

17. We then searched Moyse's computer for the existence of a Secure Delete Log, which we would have expected to see if someone had in fact used Secure Delete to delete any files from Moyse's computer.

18. Based on our review, no Secure Delete Log exists on Moyse's computer. Attached as **Exhibit "D"** to this affidavit is a screenshot of the "System Summary" from Moyse's computer which confirms that Secure Delete was not used to delete any files from Moyse's computer. As described below, we ran additional tests and we were not able to use RegClean Pro to delete the Secure Delete Log.

19. Therefore, contrary to Musters' conclusion, we found no evidence that a user used Secure Delete to delete any files or folders from Moyse's computer.

20. Our observations and analysis with respect to the Secure Delete issue can therefore be summarized as follows:

- (a) someone using Moyse's computer clicked on the "Secure Delete" program on July 20, 2014 at approximately 8:09 p.m., resulting in the creation of a "Secure Delete" folder on that computer; and
- (b) the "Secure Delete" program on Moyse's computer was not used to delete any files or folders from that computer.

Use of the "RegClean Pro" Software

21. Counsel also asked us to attempt to determine whether the "RegClean Pro" program was ever run on Moyse's computer.

22. Again, the first step of our analysis involved performing a simulation by running the RegClean Pro software on the Test Computer, and recording our observations.

23. We observed that when the RegClean Pro program is run, a log is created in the user registry at the following location:

\\KEY_CURRENT_USER\\Software\\systweak\\RegClean Pro

It appears that some of the notable program activities that are captured by that log are as follows:

- (a) StrLastScan
- (b) StrLastScanResults
- (c) StrLastOptimizeTime
- (d) StrLatestRegDefrag
- (e) StrLastestRestorePoint

24. We then applied this information to the analysis of Moyse's computer. We located a log that recorded that someone ran the RegClean Pro product on Moyse's computer. It appears that RegClean Pro "optimized" the registry on Moyse's computer on July 12, 2014, and that it performed a scan on July 20, 2014. A copy of the log confirming the use

2598
142

-8-

of the RegClean Pro product on Moyse's computer is attached as **Exhibit "E"** to this affidavit.

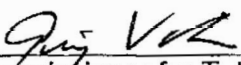
Use of RegClean Pro to delete Secure Delete's Registry

25. Counsel also asked us to determine whether it was possible to use RegClean Pro to delete the Secure Delete Log. As described above, the Secure Delete Log is located in the computer's registry.

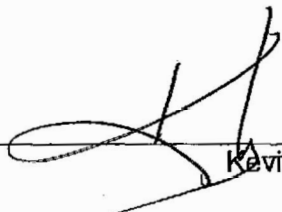
26. In order to determine whether it was possible to delete a Secure Delete log, we first deleted a number of files on the Test Computer using Secure Delete. We then ran all possible scan options from RegClean Pro. RegClean Pro identified a number of "registry errors", which did not include the Secure Delete Log. We instructed the program to "Fix Issues". We then checked the Secure Delete Log and found it had not been deleted.

27. We repeated the tests using a clone copy of Moyse's computer image. We again found that RegClean Pro did not delete Secure Delete's registry logs.

AFFIRMED BEFORE ME at the City of
Toronto, in the Province of Ontario on
April 2, 2015



Commissioner for Taking Affidavits
(or as may be)



Kevin Lo

Ainsley Claire Vaculik, a Commissioner, etc., Province of Ontario,
for Froese Forensic Partners Ltd., limited to process serving
and documents required pursuant to the Private Security and
Investigative Services Act, 2005 only. Expires March 14, 2016.