Memo

DATE:	July 18, 2025
TO:	BE-Law (Equibit Group v. AGC et al)
FROM:	Chris Horlacher, Executive Director, Equibit Group Ltd.
SUBJECT:	Marc Godard Experience
PRIVACY:	This document and its contents are confidential and protected by solicitor-client privilege, to be only possessed and read by the author and recipient. No decision made herein shall be announced publicly or privately to the affected parties, as it could jeopardize the ongoing personal safety of individuals still working for Equibit, as well as affect the outcome of litigation the company is actively prosecuting.

This memo serves as the official recounting of events relating to my complete experience with Marc Godard and Equibit Group Ltd.'s ("Equibit") conclusions based on the preponderance of evidence, knowledge of strategies employed by intelligence agencies, the context in which Equibit ultimately failed, and actions the firm will take to protect itself.

TIMELINE

Fall 2011	Marc initiated contact with me at the Mises Institute of Canada (a Canadian registered charity I volunteered at) booth during a Cambridge House event in 2011. I had been very politically active on Facebook at this point and big supporter of Ron Paul's 2008 Presidential campaign, which may have made me a person of interest to CSIS. I was also talking openly about the newly emerged Bitcoin technology and how it could be adapted for securities and other intangibles.
2012	For a couple of years little happened as we got to know each other. On a trip visiting him in Montreal, where he lived at the time, Marc confessed he once set up secret cameras in his bedroom to film himself having sex, unbeknownst to the women. I now know this to be a typical spy tactic for gathering blackmail, at the time I thought it was simply perverse. He also once indicated he felt he may be a psychopath. Marc never appeared to have a shortage of money for whatever he wanted to do, though he never worked a steady job the entire time. He explained that he was living off the profits he made rescuing and selling a Pita Pit restaurant, but the huge profits needed to sustain such a lifestyle, from such a small business, do not add up. He frequently spoke of a large amount of gold bullion he invested the proceeds of the business sale in, and that he kept it stored in a Brinks vault. Whenever he needed money, he would sell some of it to Kitco, a large Montreal-based precious metals dealer. A 2020 Maclean's article

revealed that law enforcement uses Brinks to pay undercover officers and informants, rather than via bank transfers.

I learned he studied Cognitive Science at Queen's University but stopped only a few credits short of graduating. A strange thing to do for such a high-level program that would take you into a promising career, unless he had already secured a job for life somewhere. He met Brent in the same program.

He maintained multiple birthdates, a "real" one he only told certain people (May 15, 1979) and a "fake" one, which I think was the 17th of May. He is the only person I've ever met to do this.

One of Marc's favorite movies, one I've seen him express to several people, is The Adjustment Bureau, which is about a group of quasi-supernatural beings directing and orchestrating all worldly affairs. It centers on their attempts to tear apart a genuine, loving relationship in the hopes that the separated victims will have more impressive careers. People's highest calling, according to these beings, was to be economically productive.

2013

Marc demonstrated an early interest in helping me develop my ideas, many of which required a coder to realize. Together we developed one of the very first location-based social media apps with proprietary search and user ratings algorithms. However, this company fell apart shortly after launch due to Marc's inability to maintain cohesion with the two junior developers we had hired. I noted then that he became irritated and abusive when others did not conform to his expectations.

Around this time Marc also began a work contract with Iris Software Inc. (Canada Corporation #851415-1), a Toronto-based startup from the same year that somehow managed to secure a huge contract building a secure document signing/storage system for Telus. The man he reported to, Amin Hamedani, is listed in the Federal Registry as having his residence in Tehran, Iran. How an Iranian-led startup managed to get a contract from a giant Canadian Telcom, which almost certainly would have raised national security concerns, has never been explained by anyone. The company was later administratively dissolved in 2025 for failing to meet its statutory obligations.

2014

After his contract with Iris Software wrapped up, Marc pushes for another business idea of mine and was interested in Equibit, which at this point I felt the market was ready for. We started working on it and he immediately recommends bringing in Brent Kievit-Kylar.

2015

Additional partners (Christian and Nathan) are brought into the newly created Equibit Development Corporation (later renamed Equibit Group Ltd.), an Angel Investor (Mario Malt) is located, developer hired (David Cauz) and other initial milestones setting up the company are achieved.

	Marc attends my wedding as the best man in September. His son Elliott is also born just prior to this on August 11.
2016	As we progress with development, we realize our vision is fully achievable and the decision to do a coin pre-sale is made after meeting with the OSC in December. At the meeting were Marc, David and me. More details of this meeting are in the OSC memo provided already to the case files.
Feb 2017	The Equibit pre-sale begins, and we start sourcing more developers. Kiarash Narimani and Sergei Sachkov are presented via Compustaff, a tech recruiting agency, as soon as funds start coming in. Brent administered a coding challenge and recommended Sergei, and Marc signed off without ever attending Sergei's interview. An offer letter is sent to Sergei on the 23rd and he accepts the day after. But as Equibit begins to crumble, Marc gaslights "I told you not to hire Sergei."
August 14, 2017	Marc suddenly quits Equibit just as things are really moving into high gear, but also just in time to avoid the OSC's onslaught. No reasons are specified in his resignation letter, and the most he would give in conversation was that he wanted to spend more time with his family. This did not seem strictly true to me, as he soon after partnered with Nathan to work on another initial coin offering. Marc claims he was paid 50 BTC for this job. A search of corporate records around this time reveals that Marc incorporated Token List Inc. (Canada Corporation #1032771-9) only a month before quitting Equibit, on July 18th. He later posted sentiments that he knew the company would collapse from the very beginning in the company Discord group in 2018 as the collapse was happening, to the group's great consternation.
June 28, 2018	Marc returns to Equibit as a contractor just as the ordeal with Sergei is taking place, and just after we concluded our dealings with the OSC (see OSC Experience memo) and their enforcement action. Perhaps after the failure of the OSC Sergei was then used to sabotage the company to ensure our collapse, with Marc returning to oversee the fallout.
Dec 13, 2018	After holding meetings online with the shareholders and EQB holders, Marc, Christian and I convene in the company offices for a strategy meeting, which consisted primarily of me sitting silently in a chair observing what I now understand to be a theatrical performance. Christian and Marc's behaviours were exaggerated and contrived, completely out of line with what I had previously seen of them. Christian's collaborative attitude was gone, while he obstinately insisted I help him embezzle the remaining company funds, lest he and our remaining coder quit the company. Marc's plan was my own; downsize the staff and shut down the office, stretch the remaining funds to a coin release, and pray the market supports us enough that

	we can continue financing the project out of the EQBs held by the company.
Dec 2018-2019	Marc taking over as CEO to deal with investor relations, and help with the ultimate winding down of Equibit, could be construed as an attempt to butter me up with gratitude for him so that he can later try entrapping me with yet another business idea– *which he attempted to do not long after the dust cleared*.
2019-2020	Shortly after the collapse of Equibit, Marc tried to get me involved in a scammy feeling mutual fund company called YourTimeFS, being spearheaded by a man named Dino Delellis. He had a prior conviction by the OSC, had been permanently expelled from the capital markets, and they wanted me to take a director/officer role. I never took to the idea and felt like this was another entrapment scheme to draw me back into the OSCs crosshairs. The thought that Marc and Brent could be the CSIS agents was alive and well in my mind by this point.
Summer 2020	Marc initially discourages me from filing lawsuits against CSIS, Christian, et al. Then reverses and asks to be added as a plaintiff in the lawsuit against Christian. I hide my surprise at and grant his foolish request. I knew if Marc and Christian were secretly allied that he would eventually have to betray me and this lawsuit. We agree that Christian violated the shareholder agreement and that his shares are rescinded. We encounter extreme difficulty serving Christian as even professional investigators are unable to find him. Christian had gone into hiding at this point, was being assisted in his hiding, and we were unable to find and serve him with our Statement of Claim for years. It was impossible for us to notify him of the share clawback.
December 2020	Upon providing Marc the reports showing that someone on my home network trying to access my "Equibit-DEV" honeypot, Marc has a "friend" look at it and immediately downplay the evidence. George Plytas, a far more illustrious security professional and someone I'd known and worked with at the Canadian Automobile Association, and several other companies over the years, *ceases all contact with me immediately after I inform him of the same*.
2021	While laying on my living room couch, browsing the web for information on VPN's and the Tor network, Marc begins messaging me about the exact same subject matter. He was attempting to steer me towards using Tor, which I later learned is not actually an anonymous network, and easily broken by targeted attacks like what Marc knew how to deploy (packet correlation). Here Marc demonstrated real-time knowledge of my web browsing activity, indicating a deep infiltration into my computer systems. Marc

	also repeatedly advised me to sell all my Bitcoin, which would have been financially catastrophic. The lawsuits proceed very strangely (the AG and Sergei both default, and Christian cannot be located even by professional investigators) and I'm feeling extremely uneasy knowing my network is compromised, that the government is cheating in court, and all the support systems I'd built up over the course of my career were being threatened into abandoning me. I leave Canada on June 8.
Feb 24, 2022	I completely cease communications with Marc. His behavior post-departure became strange and abusive, and this was done to gauge his reaction; friend or foe.
2022-2024	Marc tries numerous times to re-establish a dialogue with various forms of bait, including yet another "business idea" now in Mexico he wants me to be a part of in 2024. At no point do any of his messages contain anything to indicate any sadness, regret, or loss in the face of my sudden and unexplained departure from his life. He is cold and transactional in nature.
July 2025	After years of silence and complete disinterest in the status of the lawsuits, as I had predicted back when he asked to be a plaintiff, Marc takes actions whose only object is to stall the progress of the libel case against Christian et al. He also attempts to call a meeting of the shareholders of Equibit Group AG, the defunct Swiss parent company. He includes Christian in the call, whose shares he had already decided to claw back in early 2021. Marc is a plaintiff in the case being actively litigated against Christian for defrauding the company and libelling Marc and I, of which he is contributing absolutely nothing towards financially or otherwise. The meeting seeks to seize control of the litigation process at a time where the company's victory is all but certain in both the case against Christian et al, as well as CSIS et al.
July 19, 2025	Only a day after this document is created, I observe it suddenly being shared to the public via a OneDrive link. I never created this link, which would negate the entire privacy statement and ultimate purpose of this memo. I've experienced my computer taking unauthorized actions only once before, immediately after installing Keybase. This application is owned by the same company that owns Zoom and features several individuals on their board linked to the military-industrial-complex. I even wrote a lengthy post to Reddit about it. The only document of interest was the one with "Marc Godard" in the title, the other memo being actively worked on for Nathan Wosnack

was of no interest, nor the OSC memo, nor any of my other case files stored on OneDrive that are pertinent to our prosecution of CSIS.

July 20, 2025

What begins as my inability to access certain services (ProtonMail and Calendar, for example) in the morning, but only from my home network (everything returns to normal once I change IP addresses), expands to a complete block of all the internet on all my and my wife's devices (laptops and mobile) by the evening. This, even though the front panel of our router is showing all systems normal and operational.

July 22, 2025

After unplugging the modem/router for a day I reconnected it and things appeared fine for about 45 minutes, During the time it was functioning I was able to get into the router and see that some of the administrative settings had been changed, custom firewall rules and other items had been put into place. The admin section of the router also ran very slowly.

I did a reset on the router's configuration (which restored my internet access), and downloaded the router's logs, which reveal some incredibly strange behaviors over the last few days, including many entries backdated to Jan 1, 1981, which is impossible unless a hacker was covering their tracks. The log files are sent to a highly experienced cybersecurity professional for analysis and they conclude that the logged events represent hacking via the TR-069 protocol and denial-of-service attacks.

July 30, 2025

An email is sent by Marc to our lawyers appointing himself the sole legal liaison for the company, demanding the immediate termination of all legal proceedings against Christian, and a prohibition on filing any new libel actions.

August 5, 2025

While driving, I notice the clock on my car is suddenly an hour and fifteen minutes behind the actual time. The system is set to "Use network-provided time" and thinks the date is now January 1, 2019. Photos have been taken of this.

This issue corrects itself within an hour, and photos have also been taken. For decades it has been known that hackers, especially state-sponsored ones, can invade an automobile's electronics, even taking complete control of the drive-by-wire systems.

August 14, 2025

The day before the CSIS examination I receive two strange emails from unknown sources. They each contain a PDF file that, when analyzed by VirusTotal.com, come up with several disturbing MITRE signatures.

Specifically:

- Execution (TA0002)
- Defense Evasion (TA0005)
- Credential Access (TA0006)
- Discovery (TA0007)

- Command and Control (TA0011)
- Impact (TA0040)

August 18, 2025	After obtaining proxy rights to vote Mario's shares (I can now vote 50% of the shares) I held a shareholder's meeting with Ilya to vote on a resolution regarding Marc and Brent. The full meeting was recorded. A few days prior to this meeting I undertook a controlled disclosure – telling Ilya that I had isolated a DNS man-in-the-middle attack that Marc was using to determine my web browsing activities in real-time. Ilya admitted he was in communication with Marc and Brent but claimed he did not tell Marc about this specific matter. He also informed me that Marc reiterated to him his original determination from years ago that Christian breached the Shareholder Agreement. Only the company lawyers and Ilya knew I had accomplished this, and within 48 hours of the disclosure to Ilya we observed that the false DNS servers had been removed, as confirmed by our cybersecurity professional. A detailed analysis is available in a separate memo written by the cybersecurity specialist.
August 26, 2025	The day after another sham meeting was held (this time Marc included Nathan, who he later admitted was not a shareholder at all), Brent sends out the meeting notes in another PDF file. That PDF contained all the same MITRE signatures as the two previous emails I received from anonymous sources.
August 27, 2025	While looking at my computer screen, the file containing our cybersecurity professional's analysis of Marc's DNS man-in-the-middle attack spontaneously appeared on my desktop. It's conceivable that Marc has access to my OneDrive and mistakenly copied it to my desktop instead of his own.
February 23, 2026	I send hundreds of emails out to my list of journalists in North America. It includes a link to a file hosted on WeTransfer. Almost immediately after sending the email, before anyone could have reasonably read it, I receive a notification from WeTransfer that someone has downloaded the file. This is suggestive of an automated system having been wrapped around my email account (hosted by ProtonMail) that is at the very least checking all embedded links.

ANALYSIS

Marc has a track record of behaviours that raise serious questions regarding his true agenda in my life. His attempts to manipulate the record of history regarding the hiring of Sergei are particularly telling and a clear attempt at gaslighting. Were he an agent on a multi-year entrapment scheme (see *Nuttall*), now trying desperately to stop his identity from being made public, this is precisely how he would behave.

His immediate involvement of Brent with Equibit was only somewhat fruitful and, like Marc, Brent was very difficult to keep engaged in the project after things got moving. Once the whitepaper was published and Sergei hired, Brent's activities with the company all but ceased and my attempts to get his participation again as a significant shareholder were in vain. Marc even once suggested the company claw back half of Brent's shares because of his lack of participation. I naively defended Brent.

Marc's sudden departure from a promising startup on the rise, that just finished a significant fundraising round, for shockingly vague reasons are precisely what would be done by an agent looking to avoid being caught up in the impending charges. The only displeasure Marc ever expressed to me in the months leading up to his departure, was when I realized his HSM wallet idea would only work for enterprise and high-net-worth customers and would be impractical to use for personal wallets. His return and eventual appointment to CEO (well after the OSC had fled) allowed him to observe and manage the destruction of the company, while setting me up for the next scheme. When Marc initially left, we never replaced the CTO and it was his job to have back. The duration of his time away from the company was entirely of his own design. We also note that his reasons for leaving are contradicted by the fact that he worked at another startup during the interim.

When the scheme involving Equibit failed to produce any charges that could stick from the OSC, and the company was destroyed, he quickly introduced a new "business idea" that appeared shady on its face.

It's noteworthy that Nathan undertook a similar departure from a company he was previously involved with, called BitNation. I recall speaking with that project's founder, Suzanne Tarkovsky-Templehof, on Facebook and she accused him of being a spy. Just as the BitNation pre-sale was to begin, Nathan left very publicly and began casting aspertions on that project. He would then launch a similar system with another departing employee, David Mondrus, whom he initially brought to Equibit. However, Mondrus mysteriously disappeared for an extended period, which is when Nathan introduced another colleague of his, Christian Saucier, from his other venture, The Blockchain Factory. After leaving the firm, Nathan exhibited many of the same baiting strategies Marc tried and would even play off things that happened between Marc and I, demonstrating knowledge he ought not to have.

Marc's repeated and varied attempts to re-establish contact with me, including the offer of yet another "business idea" he wanted to partner with me on in Mexico, were a transparent attempt to re-gain access to my life, to assess my situation and state, and begin manipulating me into yet another entrapment scheme, or courtroom defeat by delivering privileged information about our strategy to the defense.

As discoveries approached, I noticed the connection with my computer's VPN (Mullvad) became unstable, it could not maintain a connection for any length of time or sometimes simply not establish one at all. Internet connectivity has been, in all my time in Mexico, excellent. Even with power outages, the internet fiber connection persists, and a UPS would often keep me online through the entire duration of a power outage. Sometimes I would not even notice the power had gone out. A service ticket was opened with Mullvad, but not even they could diagnose the problem. I immediately suspected Marc had returned to try hacking my systems, but that the VPN was a problem for him. I noticed it only misbehaved when I was at home, and it stands to reason he had

figured out the IP address of my router and had started doing something that would impact the VPN's ability to function on my computer, which improper firewall settings would indeed do.

Once I disabled my computer's VPN, as anticipated, many things got much weirder. It appeared like an intelligence had then gained control of my internet connectivity, shutting off my connection whenever I was doing something, or talking to someone, about CSIS and Marc being the hacker. My lawyers witnessed my entire internet being disabled during our calls several times. Many such events have been logged, including the termination of my internet connection mere minutes before Sergei's discovery session began on July 18, 2025. These cannot be explained by chance, especially when changing IP addresses causes these problems to vanish. A security professional examined the router's logs in detail and concluded that it had been attacked by a hacker.

It was upon Marc's re-emergence in real space, trying to subvert the course of our lawsuit against Christian et al, and extract privileged information about our strategy against CSIS et al, that another test was put into place, the creation of this memo and the one for Nathan. To see what interest, if any, the hacker would take. This is no different a tactic from a classic honeypot but allowed me to glean information on the hacker's identity, to which they fell into previously with similar alacrity. There is only one hacker in the world who would risk exposing themselves to obtain a copy of this memo. It is of no use to an industrial spy, and trying to steal all my case files would have been much too noticeable (he'd have to activate public sharing on an entire folder). It's undeniable this file was chosen very deliberately by someone with a big stake in its contents.

CONCLUSION

Equibit concludes that the balance of probabilities weighs heavily on Marc and Brent being the two intelligence agents mentioned by Sergei as having met him just prior to his own sabotage of the company's operations. It is likely that Christian Saucier and Nathan Wosnack also were spies/informants themselves. Both are similarly Canadians, but they had been primarily active in the United States. The concurrent timing of Marc and the hacker's re-emergence cannot be discounted. Combined with yet other experiences out of this memo's scope, it does appear as though more than one agency may have been involved. Many strange incidents with Nathan are deserving of a separate, similar memo.

Spies are incapable of legally contracting since a meeting of the minds is impossible, and Marc's true intentions are now plain to see. The nature and timing of Marc's most recent acts (he knows nothing of the upcoming discoveries for Sergei and CSIS) bear far more resemblance to attempts to irreparably harm the company's chances at a court victory against CSIS, than any other possible agenda. The intentions behind attempting a shareholder coup with a non-shareholder that he himself is actively prosecuting for fraud cannot be ignored.

Marc has now taken multiple, deliberate actions all invariably geared towards one object, obstructing the process of law and harming the company. It is also true Marc has never contributed any financial resources to Equibit, while I am personally out-of-pocket over $200,000 just in these lawsuits. Yet, as we drag the Attorney General of Canada into discoveries in just a few weeks, he is now doing anything he believes he can to gain inside knowledge of our strategy against the AG, including openly collaborating with someone he is suing for $20 million in a fraud case. These acts, taken together, communicate a state of absolute panic. Coupled with the recent resumption of

technical problems I experienced in Canada, it can only be concluded that Marc is representing the AG's interests, not Equibit's.

Therefore, Marc and Brent's shares are retroactively canceled on the day they were first issued, the issuance itself being null and void due to them lacking the capacity to contract.

APPENDIX

The issued and outstanding shares of Equibit Group Ltd. are as follows:

Name	Number of Shares	Share (%)
Chris Horlacher	29,750,000	86.8%
Mario Malt	4,250,000	12.4%
Ilya Fadeev	255,000	0.8%
Total	**34,255,000**	**100.0%**