

In the Matter of the

***FINANCIAL INSTITUTIONS ACT*, RSBC 1996, c.141
(the “Act”)**

and the

**INSURANCE COUNCIL OF BRITISH COLUMBIA
 (“Council”)**

and

**BARZIN ASSADI
(the “Licensee”)**

ORDER

As Council made an intended decision on July 13, 2021, pursuant to sections 231, 236, and 241.1 of the Act; and

As Council, in accordance with section 237 of the Act, provided the Licensee with written reasons and notice of the intended decision dated August 27, 2021; and

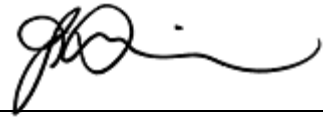
As the Licensee has not requested a hearing of Council’s intended decision within the time period provided by the Act;

Under authority of sections 231, 236, and 241.1 of the Act, Council orders that:

1. The Licensee is required to successfully complete the *Privacy Compliance – How to Protect Your Brokerage, Part 1 and Part 2* courses through the Insurance Brokers Association of British Columbia, or equivalent courses as acceptable to Council, by December 16, 2021;
2. The Licensee is required to successfully complete the Council Rules Course, currently available through the Insurance Brokers Association of British Columbia, by December 16, 2021;
3. The Licensee is fined \$2,000, to be paid by December 16, 2021;
4. The Licensee is assessed Council’s investigative costs in the amount of \$2,125, to be paid by December 16, 2021; and

5. A condition is imposed on the Licensee's general insurance licence that failure to pay the fine and investigative costs or to complete the required courses by December 16, 2021 will result in the automatic suspension of the Licensee's licence, and the Licensee will not be permitted to complete his 2023 annual filing until such time that the fine and costs are paid, and the course requirements met.

This order takes effect on the **17th day of September, 2021.**



Janet Sinclair, Executive Director
Insurance Council of British Columbia

INTENDED DECISION

of the

INSURANCE COUNCIL OF BRITISH COLUMBIA

(“Council”)

respecting

BARZIN ASSADI

(the “Licensee”)

1. Pursuant to section 232 of the *Financial Institutions Act* (the “Act”), Council conducted an investigation to determine whether the Licensee acted in compliance with the requirements of the Act, Council Rules, and Code of Conduct in relation to allegations made in April 2019 by the Licensee’s former employer (the “Former Employer”) to the effect that after the Licensee’s employment at the Former Employer had ended, the Licensee improperly possessed and used confidential information which the Licensee had obtained during the time of his employment at the Former Employer.
2. As part of Council’s investigation, on May 4, 2021, a Review Committee (the “Committee”) met with the Licensee and his counsel by video conference to discuss this matter. Prior to the meeting, a copy of an investigation report prepared by Council staff was provided to the Licensee and his counsel. The Licensee’s counsel made oral submissions in respect of the issues discussed in the investigation report, and the Licensee responded to questions of the Committee. After the Licensee and his counsel had left the meeting, the Committee deliberated on this matter and on its recommendations to Council. As part of the deliberation, the Committee reviewed and considered certain certificates that the Licensee had submitted through his counsel, which indicated that the Licensee completed various ethics courses in 2020.
3. The Committee’s report, along with the aforementioned investigation report prepared by Council staff and the certifications submitted by the Licensee, were reviewed by Council at its meeting on July 13, 2021, where it was determined that the matter should be disposed of in the manner set out below.

PROCESS

4. Pursuant to section 237 of the Act, Council must provide written notice to the Licensee of the action it intends to take under sections 231, 236, and 241.1 of the Act before taking such action. The Licensee may then accept Council’s decision or request a formal hearing. This

intended decision operates as written notice of the action Council intends to take against the Licensee.

FACTS

5. The Licensee was first licensed with Council in October 2010 as a Level 1 general insurance salesperson and is currently a Level 2 general insurance agent. In February 2019, the Licensee left the employment of the former employer (the “Former Employer”) and began working for his current employer (the “Current Employer”).
6. On March 15, 2019, the Former Employer commenced an action against the Licensee and the Current Employer in the Supreme Court of British Columbia (the “Civil Proceeding”) by filing a notice of civil claim (“NCC”). In the NCC, the Former Employer alleged, among other things, breach of contract and breach of fiduciary duties by the Licensee, and the Former Employer alleged that the Current Employer induced the Licensee to breach his contractual and fiduciary duties.
7. On or about March 21, 2019, the Current Employer and the Licensee took certain steps in agreement with the Former Employer to address the Former Employer’s concern that the Licensee had copied confidential and proprietary information from the Former Employer’s computer system onto a USB drive. Through counsel, the Licensee provided the USB drive to the Former Employer. Further, the Current Employer isolated a folder on its computer system which contained a copy of the files from the USB drive, and restricted access to the folder in accordance with a procedure agreed upon with the Former Employer. Finally, the Licensee and the Current Employer agreed to a forensic IT audit of the Licensee’s home computer and the Current Employer’s computing system.
8. On April 4, 2019, Council staff received the Former Employer’s complaint against the Licensee. This complaint was made by the Former Employer in parallel with the Civil Proceeding. In support of its complaint, the Former Employer provided a copy of the NCC, which set out the Former Employer’s version of events.
9. By letter dated July 25, 2019, counsel for the Licensee provided his response to the Former Employer’s complaint, and stated the following:
 - (a) Throughout his employment with the Former Employer, and for many years before that, the Licensee maintained a USB drive, which he used regularly.

- (b) The Licensee admitted that the USB drive contained some confidential and proprietary documents belonging to the Former Employer, along with many documents that did not belong to the Former Employer. The USB drive had two primary functions: to store personal documents and information necessary for the Licensee's non-work business and personal computing, and as a backup for his work computer. The Licensee backed up his work computer to the USB drive from time to time, with the result that documents on his work computer were copied onto the USB drive.
 - (c) The Licensee did not create the USB drive during his employment with the Former Employer or in anticipation of his departure to join the Current Employer. For six years prior to joining the Former Employer, when the Licensee worked at other insurance agencies, the Licensee similarly used the USB drive.
 - (d) The Licensee was particularly reliant on the USB drive as a backup of his work computer during most of his employment with the Former Employer because the Former Employer did not have a centralized system for storing policy documents until sometime in 2018. The Licensee believes that he backed up his work computer to the USB drive approximately five or six times during his employment with the Former Employer.
 - (e) Other individuals at the Former Employer were aware of the USB drive and that it contained information relating to the Former Employer and insurance clients served by the Licensee.
 - (f) The Licensee did not contact the Former Employer's clients on behalf of the Current Employer while employed by the Former Employer. In fact, when clients asked him where he was going after his employment at the Former Employer ended, he told them that he was not permitted to tell them.
 - (g) The Licensee recognized that he made errors with respect to the management of the Former Employer's documents. He respectfully proposed that the situation would be best addressed by a renewed commitment on his part to education and training.
10. By email dated December 13, 2019, Council staff requested that the Former Employer clarify whether the Licensee would have been authorized to access the client files that he copied to the USB drive, had he not left the Former Employer.

11. By email dated January 24, 2020, the Former Employer responded that if the Licensee had not left the Former Employer, he would have been authorized to access the client files found on the USB drive, but only for the purposes of providing services through and on behalf of the Former Employer; however, the Licensee should not have saved the client files to a personal USB drive.

12. At the meeting of May 4, 2021 with the Committee, the Licensee confirmed his view that there was no error in the investigation report. The Licensee also provided the following evidence in response to questions put to him by the Committee:
 - (a) the USB drive contained the Former Employer client files as well as unrelated information and documents which belonged to the Licensee;
 - (b) the information on the USB drive was not encrypted;
 - (c) the Licensee admitted to having used a laptop computer issued to him by the Former Employer for work as well as personal use;
 - (d) The Former Employer did not have a centralized backup system for documents until mid-2018, and even after that the centralized backup system was frequently down;
 - (e) the Licensee did not remember the Former Employer providing any training or policy for use and management of documents, and he recalls that other employees also took work documents home;
 - (f) the Licensee did not recall ever deleting documents from the USB drive;
 - (g) the Licensee did not save documents on the USB drive in anticipation of leaving the Former Employer;
 - (h) the last time that the Licensee backed up documents on the USB drive was in January 2019;
 - (i) the Licensee accepted that the client information which he collected and stored on the USB drive was obtained from clients who reasonably expected that their information would only be used for business purposes and would not be stored on the Licensee's personal devices.

ANALYSIS

13. Council found Council Rule 7(1), which requires licensees to hold in strict confidence all information acquired in the course of the professional relationship concerning the personal and business affairs of a client, to be relevant to this matter. Also of relevance are Code of Conduct sections 5 (“Competence”) and 7 (“Usual Practice: Dealing with Clients”). Additionally, Council found the Code of Conduct’s Client Confidentiality Guidelines for Insurance Agents, Adjusters, and Salespersons (the “Guidelines”) were relevant to the review of the alleged misconduct.
14. Council believes it is fair to describe the Civil Proceeding as a business dispute over revenues from insurance clients. The purpose of the Civil Proceeding is not to vindicate public norms or protect insurance clients *per se*. In contrast, this investigation was not concerned with the business dispute between the Former Employer, the Licensee, and the Current Employer. Rather, Council was concerned with whether the Licensee breached his ethical and professional regulatory obligations.
15. Council found the evidence provided by the Licensee regarding the use of the USB drive and its contents to be reasonable and not directly contradicted by any evidence provided by the Former Employer. To that end, Council found that the Licensee’s actions primarily offended section 5 of the Code of Conduct, and that he likely had not intended to disadvantage the Former Employer or otherwise act against their interests. In addition, by inappropriately dealing with client information, Council believes that the Licensee breached the minimum requirements set out at Council Rule 7(1) and section 7 of the Code of Conduct.
16. According to the Former Employer, if the Licensee had not left the Former Employer, he would have been authorized to access the client files found on the USB drive, but only for the purposes of providing services through and on behalf of the Former Employer. Council found this to have been a reasonable assertion by the Former Employer. As the Licensee has admitted, it is reasonable to believe that the Former Employer’s clients expected the Licensee to handle their information with care, and use the information only for authorized business purposes, and not store the information on his personal USB drive.
17. Council was troubled by the Licensee’s handling of client information in the following manner:

- (a) the Licensee's storage of client information on his personal device, notwithstanding the implied expectation of clients that the information would only be used for authorized business purposes;
 - (b) the Licensee's co-mingling of client information with his personal information and documents; and
 - (c) the lack of passwords or other reasonable safeguards to protect the client information on the personal USB drive from unauthorized access by others.
18. Prior to making the intended decision, Council took into consideration the following precedent cases.
19. *Jason Robert Verbeke* (April 2018) concerned a Level 2 general insurance agent licensee who took clients' information on a spreadsheet when he left an agency. The licensee's position was that the clients were his and that he had a right to the information. He also claimed to have the clients' verbal consent. Council accepted that the licensee genuinely believed that the clients were his own, but he had not obtained express consent from the clients to keep the client information. Council ordered that the licensee take the Privacy Course and Council Rules Course through the Insurance Brokers Association of British Columbia ("IBABC"). In addition, the licensee was fined \$2,500 and was assessed investigative costs of \$2,037.50.
20. *Dolores Gertrude Findlater* (February 2018) concerned a Level 2 general insurance agent licensee who took copies of client records and Insurance Corporation of British Columbia ("ICBC") documents while packing her belongings. The licensee stated that she inadvertently took the ICBC documents and returned them to the agency when she realized the mistake. In respect of the client records, the licensee defended her decision to take them as she thought that they belonged to her. Council determined that while there was no indication that the licensee had used client information inappropriately, she had improperly compiled, retained and stored confidential client information without the knowledge and consent of the clients. Council ordered that the licensee take the Privacy Course through the IBABC. In addition, the licensee was fined \$2,500 and was assessed investigative costs of \$1,118.75.
21. *Douglas Arthur Fredell* (December 2016) concerned a Level 2 general insurance agent licensee who represented his former agency for 15 years and had a contractual right to transition his clients from the former agency to a new agency. During the transition, the licensee emailed client information to his personal email account and saved information

on his personal computer. For 18 clients, the licensee transferred their information to the new agency without obtaining letters of brokerage. Council determined that the licensee's compilation, retention, and storage of confidential client information on his personal computer and then, subsequently, at the new agency, without knowledge and consent of the clients, was contrary to the usual practice of the business of insurance. Council ordered the licensee to take the Privacy Course and Council Rules Course through the IBABC. In addition, the licensee was fined \$2,500 and was assessed investigative costs of \$875.

22. *Miodrag Subin* (April 2016) concerned a Level 2 general insurance agent licensee who was found with a flash drive of confidential information relating to 136 customers he had serviced through his former agency. The licensee did not have consent from his former agency or customers. Council determined that the licensee's failure to consider the need for the customers' consent was inappropriate, and that the licensee's actions were aggravated by the fact that the information was kept on an unsecured memory stick and then subsequently left unsecured at the licensee's new agency, where it was discovered and copied. Council ordered that without express knowledge and consent of the nominee of any insurance agency, the licensee must not remove from the agency's offices any information about the agency's clients. In addition, the licensee was fined \$2,500 and was assessed investigative costs of \$1,000.
23. Council gave consideration to relevant mitigating and aggravating factors in this matter. The primary mitigating factor was that the Licensee was cooperative from an early stage of the investigation and he made reasonable admissions. The primary aggravating factor was that the carelessness with which the Licensee handled and kept client information, as described at paragraph 17 above, was a marked departure from the minimum standards for dealing with client information as set out at Council Rule 7(1) and sections 5 and 7 of the Code of Conduct. The Licensee's breach of the relevant standards was unacceptable particularly given his relative experience as an insurance agent.
24. Council also believed it was appropriate to assess costs against the Licensee. As a self-funding regulator, the cost to investigate the misconduct of a licensee should not be borne by members of the insurance industry unaffiliated with these matters. This is particularly true in instances when the evidence is clear that a licensee's actions have amounted to misconduct.
25. After weighing all of the relevant considerations, including the ethics courses which the Licensee took on his own accord in 2020, Council made the intended decision set out below.

INTENDED DECISION

26. Pursuant to sections 231, 236, and 241.1 of the Act, Council made an intended decision to:

- a) Require the Licensee to successfully complete the *Privacy Compliance – How to Protect Your Brokerage, Part 1 and Part 2* courses through the Insurance Brokers Association of British Columbia (“IBABC”), or equivalent courses as acceptable to Council, within 90 days of the date of Council’s order;
- b) Require the Licensee to successfully complete the Council Rules Course, available through the IBABC, within 90 days of the date of Council’s order;
- c) Fine the Licensee in the amount of \$2,000, to be paid within 90 days of the date of Council’s order;
- d) Assess Council’s investigative costs in the amount of \$2,125 against the Licensee, to be paid within 90 days of the date of Council’s order; and
- e) Impose a condition on the Licensee’s general insurance licence that failure to pay the fine and investigative costs or to complete the required courses within 90 days of the date of Council’s order will result in the automatic suspension of the Licensee’s licence, and the Licensee will not be permitted to complete his 2023 annual filing until such time that the fine and costs are paid, and the course requirements met.

27. Subject to the right of the Licensee to request a hearing before Council pursuant to section 237 of the Act, the intended decision will take effect after the expiry of the hearing period.

RIGHT TO A HEARING

28. If the Licensee wishes to dispute Council’s findings or intended decision, the Licensee may have legal representation and present a case at a hearing before Council. **Pursuant to section 237(3) of the Act, to require Council to hold a hearing, the Licensee must give notice to Council by delivering to its office written notice of this intention within 14 days of receiving this intended decision.** A hearing will then be scheduled for a date within a reasonable period of time from receipt of the notice. Please direct written notice to the attention of Executive Director. **If the Licensee does not request a hearing within 14 days of receiving this intended decision, the intended decision of Council will take effect.**

29. Even if this decision is accepted by the Licensee, pursuant to section 242(3) of the Act, the British Columbia Financial Services Authority (“BCFSA”) still has a right of appeal to the Financial Services Tribunal (“FST”). The BCFSA has 30 days to file a Notice of Appeal, once Council’s decision takes effect. For more information respecting appeals to the FST, please contact them by telephone at 250-387-3464, visit their website at www.fst.gov.bc.ca or view their appeal guide at www.fst.gov.bc.ca/pdf/guides/ICGuide.pdf.

Dated in Vancouver, British Columbia on the 27th day of August, 2021.

For the Insurance Council of British Columbia

A handwritten signature in black ink, appearing to be 'JS', written over a horizontal line.

For Janet Sinclair
Executive Director