Adjudication Panel Meeting

25 May 2022

Institute and Faculty of Actuaries

Held by Video Conference

Respondent:	Joe Bronstein (Student member)
Category:	Student since 23 November 2018
Region:	Liverpool, UK
Panel Members:	Andy Scott FFA (Chair) Angela Brown (Lay member) Peter Ridges FIA (Actuary member)
Legal Adviser:	Graeme Watson
Judicial Committees Secretary:	Hinna Alim

Allegations:

The allegations against Joe Bronstein (the Respondent) are:

A1 On 15 January 2022 he sent emails containing unencrypted member data and/or company intellectual property (the Confidential Information) from his work email address to his personal email address;

A2 He intended to use the Confidential Information:

- A2.1 for purposes which were not related to his current employment;
- A2.2 to assist him in a new role at a different firm.

A3 His actions at A1 and/or A2 were in breach of his employer's:

- A3.1 Information Security Policy;
- A3.2 Personal Ethics Guide.

A4 His actions in paragraphs A1, A2 and/or A3 above were in breach of the Integrity principle of the Actuaries' Code (version 3.0).

A5 His actions in paragraphs A1, A2, and/or A3 above were in breach of the Compliance principle of the Actuaries' Code (version 3.0).

A6 His actions, in all or any of the above, constituted misconduct in terms of Rule 4.2 of the Disciplinary and Capacity for Membership Schemes of the Institute and Faculty of Actuaries (Effective 1 June 2021).

Panel's determination:

The Panel considered the Case Report and appendices submitted by the Case Manager and Investigation Actuary and the Respondent's response to the Case Report. The Panel also considered the advice of the Legal Adviser. The Panel determined that the Case Report disclosed a *prima facie* case of Misconduct.

The Panel accordingly invited the Respondent to accept that there had been Misconduct and the following sanctions:

- Reprimand
- Fine of £3,500 to be paid within 28 days of the Respondent's acceptance of the Panel's invitation

Background:

On 13 January 2022 the Respondent received offers for two new jobs. At that time, he was employed by "the Company", but he was working from home, having been on paternity/shared parental leave since 8 December 2021. The Respondent was due to return to work on 1 February 2022.

On 15 January 2022 the Respondent sent emails containing unencrypted member data and company intellectual property from his work email address to his personal email address. At the time the Respondent sent the emails on 15 January 2022, he had not accepted either new job offer.

The Company is a pensions advisory firm and was formerly Company B, before being sold in March 2020 and becoming an independent UK pensions advisory firm. The Respondent was transferred to the Company under the Transfer of Undertakings (Protection of Employment) Regulations (TUPE) and retained his original Company B terms and conditions of employment.

The Respondent's emails were flagged to the Company's management by their IT department on 17 January 2022 and the Respondent's manager spoke to him about the matter on 20 January 2022. The Company then carried out an investigation and commenced disciplinary proceedings against the Respondent. Following that investigation, the Respondent was dismissed on 31 January 2022 due to gross misconduct.

The allegations against the Respondent were received by the IFoA Disciplinary Team in an email from the Company on 22 February 2022.

Decision and Reasons on the Allegations:

Before commencing the discussions about the Allegations, the legal adviser instructed the Panel to ignore the "*Disciplinary Hearing Outcome*" which had been included in Appendix 2 of the Hearing documents. This instruction was based on recent Court judgements in which the outcome of a separate Hearing could be deemed as prejudicial to a subsequent Hearing.

The Panel felt that Appendix 2 could reasonably be ignored in their deliberations on this case and agreed to proceed accordingly.

Allegation A1

The Respondent has admitted that on 15 January 2022, he sent five emails containing a total of 43 attachments from his work email address to his personal email address.

The attachments contained unencrypted member data and company intellectual property including documents and spreadsheets created by other people for use in company projects. The unencrypted member data included, among other things, details of the Company's clients' age, sex, date of birth, service dates and pension details.

In mitigation, the Respondent advised the IFoA (Appendix 15) that, at the time of sending the emails to himself, he was physically and mentally exhausted from having a very young baby, looking after his wife [redacted], looking after their two older children (3.5 and nearly 2 years old), running the household and interviewing with a number of actuarial firms. The Respondent said that these circumstances resulted in him being in a state of fatigue that could be concluded to have contributed to his decision to send the emails. He said that had he been of clearer mind, he is confident he would not have sent them.

A list of all the attachments the Respondent sent to himself on 15 January 2022, and the nature of the data, was provided to the IFoA Disciplinary Team by the Company. The Respondent has accepted that this is an accurate summary of what was attached to the emails.

Given this evidence and the Respondent's admissions, the Panel believes that Allegation A1 is capable of proof.

Allegation A2

As noted above, two days before sending the Confidential Information to his personal email address, the Respondent had received two job offers.

The Respondent advised that he had been interviewing for a number of roles and that he was intending to use the information for his personal learning and as a prompt for any future work he may do elsewhere. The Respondent advised that he was interested in the formulae

rather than the data that was contained in the documents. He also advised that the data he sent to himself contained analysis that he had worked on personally and that this was his rationale for sending the documents to himself.

The Respondent subsequently admitted, however, that, having reflected on this logic, this was a highly inappropriate course of action and that if he had thought it through properly, he would never have sent himself the Confidential Information.

Given the above evidence and admissions, the Panel concluded that the Respondent intended to use the Confidential Information for his own use to assist him in his employment with his new Employer, and therefore that Allegation A2 is capable of proof.

Allegation A3

In the section entitled "*Protect information according to its value to the firm and our clients"*, the **Company's Information Security Policy** directs its staff to:

- Share [Company] and client information only with people authorised to use it
- Apply extra protection to [Company] or client information leaving the firm's trusted network and encrypt Highly Confidential information in transit and in storage.
- Personal data must be encrypted if leaving the firm's trusted network
- All the information you have obtained or created when working for the firm belongs to the firm (or our clients). You must not take it with you when you leave the firm.

The Panel further noted that in the section entitled "*Use email and the internet securely"*, the **Company's Information Security Policy** directs its staff;

- Don't email [Company] or client information to your (or someone else's) private email address, unless this is an approved part of your role in the firm (e.g. you work in recruitment)
- Use encryption if you're emailing Highly Confidential or personal information outside the firm's trusted network……

In the section entitle *"Intellectual Property",* the **Company's Personal Ethics Guide** instructs the staff:

- …when you leave [the Company] or cease to work on [a Company] account, you are prohibited from taking it with you and/ or reusing any form of confidential or proprietary information that you developed or became aware of in connection with your employment with [the Company] or your work on [a Company]account.

- Breaches of these policies may expose both you and [the Company]to legal actions and criminal penalties, including fines and imprisonment.

The Panel also noted that in the section entitled *"Protecting information*", the **Company's Personal Ethics Guide** instructs the staff to:

- Use information Assets and IT Assets for approved business purposes, and in a manner that does not compromise their confidentiality, integrity or availability.

Further, in the section "*Confidential information – Its uses and protection*", the **Company's Personal Ethics Guide** instructs the staff that:

- … you must not share with anyone else or use confidential information outside the engagement (unless given permission to do so by the client).
- Confidential information must be used for the engagement only unless otherwise agreed with the person who provided it. You must not use it for your own personal benefit.

The Respondent does not dispute this allegation and also acknowledged that he had attended extensive company training on data protocols and information security.

Given the above extracts of the **Company's Information Security Policy** and the **Company's Personal Ethics Guide**, and the admissions from the Respondent, the Panel believes that Allegation A3 is capable of proof.

Allegation A4

The Integrity principle of the Actuaries' Code (version 3.0 effective 18 May 2019) is as follows:

> *"Integrity*
>
> *1. Members must act honestly and with integrity.*
> *1.1 Members must show respect for others in the way they conduct themselves.*
> *1.2 Members should respect confidentiality."*

The Actuaries' Code Guidance for the Integrity principle states:

> *"3.3 Acting with integrity in a professional setting will generally mean being straightforward and honest in your professional and business relationships and dealing fairly with those around you.*
>
> *[...]*
>
> *3.9 Users and the general public are entitled to expect that sensitive information will not be misused, treated carelessly or, other than in exceptional circumstances, be*

shared without permission. This is reflected in the second amplification under the Integrity principle which provides that: "Members should respect confidentiality.

3.10 Confidential information to which a Member may have access includes personal data about third parties such as insurance or pension policy holders. It may also include communications from clients, such as emails, and some commercially sensitive information relating to businesses with which the Member interacts. Sometimes confidential information will not be labelled as such, and Members will need to exercise judgment as to whether there is a reasonable expectation that information should be considered confidential."

In responding to this allegation, the Respondent sent an email to the Case Manager on 11 March 2022, in which he states:

"I would argue that whilst the action I took lead to the potential for a breach in respect of confidentiality, as soon as it was made aware that I had done something wrong I took all reasonable steps to prohibit the possibility of data loss in line with requests made by [the Company]. Further, I would submit that I did not act dishonestly or without integrity - due to the circumstances mentioned above I would say that sending the emails constituted a serious error of judgement rather than a conscious and malicious action. As such, I would question whether I have breached the Integrity part of the Code."

The Panel felt, however, that, by emailing unencrypted data to himself, the Respondent had contravened Guidance Note 3.9, as it was not a level of behaviour that the general public are entitled to expect of a Member of the Profession and that it was treating the data carelessly. This could have had serious implications for the data subjects (if the Respondent's home IT system had been hacked) and also for the Company, who could have also been fined by the ICO (under GDPR regulations) with all the resultant reputational damage.

The Panel therefore concluded that the Respondent's actions in Allegations A1, A2 and/or A3 above were in breach of the Integrity principle of the Actuaries' Code (version 3.0) and therefore that Allegation A4 is capable of proof.

Allegation A5

The Compliance principle of the Actuaries' Code (version 3.0 effective 18 May 2019) is as follows:

"Compliance

.

.

4. Members must comply with all relevant legal, regulatory and professional requirements."

The Respondent's legal and professional requirements under the Company policies and his employment contract are set out in the **Company's Information Security Policy**, the **Company's Personal Ethics Guide** and the **[Company B] National Statement of Terms and Conditions,** and the Respondent does not dispute that his actions were in breach of the Compliance principle.

The Panel therefore considered that the Respondent's actions in paragraphs A1, A2 and/or A3, in particular the breaches of his company policies, amount to a breach of the Compliance principle of the Actuaries' Code.

Decision and Reasons on Misconduct:

The Panel then considered whether there was a *prima facie* case that the Respondent's actions in all or any of the above allegations constituted Misconduct.

For the purposes of the Disciplinary and Capacity for Membership Schemes, Misconduct is defined as *"any conduct by a Member, whether committed in the United Kingdom or elsewhere, in the course of carrying out professional duties or otherwise, constituting failure by that Member to comply with the standards of behaviour, integrity, competence or professional judgement which other Members or the public might reasonably expect of a Member having regard to the Bye-laws of the Institute and Faculty of Actuaries and/or to any code, standards, advice, guidance, memorandum or statement on professional conduct, practice or duties which may be given and published by the Institute and Faculty of Actuaries and/or, for so long as there is a relevant Memorandum of Understanding in force, by the FRC (including by the former Board for Actuarial Standards) in terms thereof, and to all other relevant circumstances."*

The Panel determined that there was a *prima facie* case that the Respondent's actions were sufficiently serious as to constitute Misconduct under the Disciplinary and Capacity for Membership Schemes.

The Misconduct was a serious breach of the Respondent's legal and professional responsibilities to his clients and the Company and could have had serious implications for them. As a result, the Panel was satisfied that there was sufficient evidence that the threshold for Misconduct had been met, given the importance which the profession properly attaches to ensuring compliance with the Actuaries' Code.

The Panel concluded, taking account of all the evidence available, that this was not so serious a matter as to require referral to a Disciplinary Tribunal Panel.

Decision and Reasons on Sanction:

In reaching its decision, the Panel had regard to the Indicative Sanctions Guidance (November 2021). The exercise of its powers in the imposition of any sanction is a matter solely for the Panel to determine and it is not bound by the Indicative Sanctions Guidance. The Respondent's misconduct was a serious breach of the Respondent's legal responsibilities as a citizen but did not arise from his professional practice. Overall the Panel was satisfied that there was sufficient evidence that the threshold for Misconduct had been met, given the importance which the profession properly attaches to ensuring compliance with the Actuaries' Code. However, the Panel concluded, taking account of all the evidence available, that this was not so serious a matter as to require referral to a Disciplinary Tribunal Panel.

The Panel was aware that the purpose of sanction is not to be punitive although it may have that effect. Rather, the purpose of sanction is to protect the public, maintain the reputation of the profession and declare and uphold proper standards of conduct and competence. The Panel is mindful that it should impose a sanction, or combination of sanctions necessary to achieve those objectives and in so doing it must balance the public interest with the Respondent's own interests.

In considering sanction, the Panel took into account the following aggravating factors:

- The amount of data emailed by the Respondent was substantial (43 attachments with extensive member data)
- The Respondent had received substantial training from the Company on data protocols and information security
- The Respondent had subsequently been dismissed
- The actions by the Respondent could have resulted in significant financial penalties and reputational damage for the Company, and could potentially have caused embarrassment and financial disadvantage to the members whose data had been transferred
- The Respondent could have asked the Company about emailing the data, but failed to do so
- The Respondent's actions were in breach of the Actuaries' Code and were not at a level that could reasonably be expected by the general public or the profession

The Panel also took into account the following factors in mitigation:

- The Respondent was a student member and was not an experienced actuary

- The Respondent was under a lot of pressure, looking after the family at home and carrying out a number of interviews
- The Respondent has admitted that his actions were inappropriate
- The Respondent did not intend to achieve any financial gain from his actions and wished to use the transferred information for “educational” purpose
- The Respondent has no previous disciplinary record and has apologised to the IFoA
- The Respondent has undergone substantial training at his new Employer on information security, data sharing and GDPR
- Given all of the above mitigations, the likelihood of the Respondent repeating his actions (and putting the public or his employer at risk) is extremely low

The Panel considered whether this was a case that warranted no sanction but was satisfied that the seriousness of the professional breach required the imposition of a sanction in order that an appropriate message could be given to the Respondent, the profession and the wider public.

The Panel considered whether to impose a Reprimand and determined that this should form part of the sanction, as there was evidence of a serious breach of the Actuaries’ Code, which could have had substantial consequences for the Company and the members whose data had been transferred unencrypted.

The Panel considered whether to impose a fine and decided that it would be an appropriate punishment in this case. The Respondent has taken responsibility for his conduct giving rise to the allegations, but he should have known better, given all of his training, and the potential ramifications of his actions were such that a fine should be imposed. The Respondent had provided information on his personal financial position and having taken all these factors into account, the Panel concluded that a fine of £3,500 was appropriate.

Finally, the Panel considered whether to impose a period of education, training or supervised practice and decided that it would not be appropriate in this case, given all of the training that the Respondent has received with his new Employer. The Panel felt that this training and his experience in this case meant that the likelihood of any repetition by the Respondent was extremely low.

Publication:

Having taken account of the Disciplinary Board's Publication Guidance Policy (May 2019), the Panel determined that, if the Respondent accepted the findings of the Panel, this determination will be published and remain on the IFoA's website for a period of five years from the date of publication. The Panel applied appropriate redactions to the published determination in accordance with the Publication Guidance. A brief summary will also be published in the next available edition of *The Actuary* Magazine.

That concludes this determination.