**IN THE MATTER OF** A complaint under s 74 of the Private Security Personnel and Private Investigators Act 2010 against **ARGYLE SECURITY GROUP (NZ) LTD** and **CRAIG ANDREW CAMPBELL**

**HEARD**
by audio visual hearing on 2 November 2023

**APPEARANCES**
Mr SW
Mr Campbell

**DECISION**

(i) Complaint upheld: Mr Campbell is guilty of unsatisfactory conduct.
(ii) Mr Campbell is officially reprimanded.
(iii) Mr Campbell is to apologise in writing to Mr SW and provide confirmation that he has done so to the Authority no later than 31 December 2023.
(iv) Mr Campbell must undergo training in the area of privacy law within the next twelve months and provide evidence of his having done so to the Authority.

## REASONS

[1] In July 2023 Craig Andrew Campbell, under the employment of Argyle Security Group (NZ) Ltd (Argyle), installed a security system for Andrew SW. Shortly afterwards he replaced one of the cameras upon Mr SW's request. There were ongoing issues with several of the cameras, particularly the 'boat' camera. Mr Campbell and Mr SW disagreed over whether the issue was with the cameras or the environment that was being filmed. In the end, Mr SW replaced several cameras himself with cameras of different specifications which resolved the issue.

[2] Mr SW subsequently laid a complaint against Mr Campbell and Argyle regarding his actions whilst installing their security system. Mr SW alleges Mr Campbell is guilty of misconduct or unsatisfactory conduct by installing a faulty security system and not dealing with their concerns adequately or professionally. He also alleges that Mr Campbell logged into their security system remotely and viewed the SW's personal cameras and downloaded footage without permission, thereby invading their privacy.

[3] Mr Campbell denies the allegations and says he was working diligently to resolve the issues Mr SW was facing. He submits that he only accessed the cameras in attempts to troubleshoot and the complaint is vexatious.

[4] Mr Campbell holds a Certificate of Approval (COA) that is valid until 19 February 2024. He is one of two directors of Argyle. Argyle holds a company license in the classes Crowd Controller, Property Guard, Security Consultant, Security Technician, Repossession Agent, Monitoring Officer, Document Destruction Agent and Personal Security Guard that is valid until 27 November 2025.

*The questions for the Authority*

[5] The issues I therefore need to decide are whether Mr Campbell is guilty of misconduct or unsatisfactory conduct by:

- Without permission or knowledge accessing Mr SW's security system, and/or
- Changing Mr SW's access password, and/or
- Generally acting unprofessionally.

[6] If Mr Campbell is guilty of misconduct or unsatisfactory conduct, I then need to decide what is the appropriate penalty in accordance with the Private Security Personnel and Private Investigators Act 2010 (the Act).

[7] Misconduct is defined in s 4 of the Act as being:

> *Conduct by a licensee or certificate holder that a reasonable person would consider to be disgraceful, wilful, or reckless or conduct that contravenes this Act or any Regulations made under this Act*

[8] Unsatisfactory conduct is conduct that falls short of the standard that a reasonable member of the public is entitled to expect from a reasonably competent licensee or certificate holder; or conduct that is incompetent or negligent; or conduct that would reasonably be regarded by private security personnel of good standing as being unacceptable.

[9] I discuss each of the grounds of complaint separately below. Further, since the hearing Mr SW alleges that Mr Campbell has sent him abusive messages, and this concern will be addressed as well.

*Did Mr Campbell unlawfully and without permission log remotely into Mr SW's security system?*

[10] It is accepted that at times post-install Mr Campbell did log into an application which allowed him to view the SW's security camera footage. The question therefore becomes about permission and purpose.

[11] Mr Campbell says that he made Mr SW aware he had the ability to log in remotely and would do so for the purposes of checking the system. In particular he notes the following occasions of disclosure:

[i] In a phone call when they were discussing the ongoing problems Mr SW was having with his system, Mr Campbell said he told him he would sporadically "check in" and see how it was going. Mr Campbell says it would have been clear that by him "checking in" he would be accessing the system remotely.

[ii] At the visit on 20 July when he asked Mr SW to sign the service check list. He says he read out the last paragraph to Mr SW before he signed which says: *I'm happy for the tech/company to periodically check-in on my remote-view details 24/7 (if applicable) to verify no issues with my system.*

[iii] At the visit on 23 August when he read out the same paragraph on the service check list for that visit and again Mr SW signed the document.

[iv] On 23 August when he showed Mr SW how to access the system remotely, he did so through an application on his phone.

[v] An email on 24 August he said to Mr SW: *I did the same in "search" on your boat camera and back door over the last 3 weeks and they seemed to work fine?*

[12] Mr Campbell says he had no need to access Mr SW's system other than to try and help him with the issues he was experiencing. His evidence is that to access a client's security system, he firstly needs to scan the QR code on their system and then login remotely. He says his company only ever does so if troubleshooting is required.

[13] Mr Campbell accepts that the only place in his documentation that there is reference to remote access is on the service check lists they use when they are investigating problems clients are having. This is because they do not access a system unless they need to, to troubleshoot. He says he was only logging in to help Mr SW and each time he did it was only brief to ascertain if the cameras were working.

[14] Mr SW is adamant that he was not aware that Mr Campbell had remote access until an email from him on 14 September which indicated he had 'inside' knowledge as he knew the names of his cameras. At which point he logged in and saw that the administrative account which they had previously not had access to (see the below discussion) had been logging in on numerous occasions. He could then see that the admin account had viewed the cameras on 21 different days between 15 August and 14 September.

[15] He says he specifically asked Mr Campbell at the install if anyone else could access the system and Mr Campbell said no. He says that at no point did Mr Campbell say he would be accessing the system himself which is supported by him sending Mr Campbell videos of the issue which he would not have had to do had he knew Mr Campbell could access it himself.

[16] Mr SW acknowledges the relevant wording on the service check list but says it was not read out to him and he was not left with a copy. He agrees he should have read the fine print but was focussed on getting the issue resolved and just signed where Mr Campbell pointed out to him to do so. He says he would never have given consent for others to access his system; this is his private home and they have children in the house. He submits that it would completely defeat the purpose of a security system for it to be accessible by others.

[17] Mr SW's understanding of the discussion on the 23rd of August about the ability to access the system remotely was only with reference to him being able to. It did not occur to him, or come up in the conversation he says, that Mr Campbell would use the system for his own access.

[18] Mr SW has been so upset over this process that he has filed a complaint with the Police over the issue as well as the Authority.

[19] Having considered the evidence thoroughly, I find it more likely than not that Mr Campbell did not make Mr SW clearly aware of his ability to login remotely. I do not find it proven that he read the specific section of the service sheet aloud to Mr SW when he went through it with him, as he was focussed on the tasks they had completed. Furthermore, he had already accessed the cameras prior to the service attendances where the service sheets were signed. All other references were implicit in nature.

[20] In a situation such as this that involves privacy issues, I consider that a reasonable and prudent security technician is obliged to clearly and explicitly state what access, if any, an external person could have to the client's newly installed security system. Further, if a security system is to be accessed, I consider it reasonable and prudent that the client is

advised before that access occurs. This is especially so when the cameras are at a private residence.

[21] I find it established that Mr Campbell accessed Mr SW's security system without his knowledge or permission. He was doing so in an effort to help Mr SW and I do not find it substantiated that he used it for any illicit purpose.

[22] I consider that a failure to clearly explain the access before it was undertaken is unsatisfactory conduct of a security technician. Accordingly, Mr Campbell has engaged in unsatisfactory conduct by failing to explicitly advise Mr SW that his system could be remotely accessed and by failing to advise him that he would access the cameras before he did so.

*Did Mr Campbell change the SW's password?*

[23] There were two accounts associated with the security system. Mr SW says that at one point Mr Campbell changed the password on the 'admin' account which meant that the SWs could not access that account which had more settings such as account permissions, but Mr Campbell could. When they realised this, they had to re-set the entire system to delete the account he had access to.

[24] Mr Campbell says that there was an issue with the login at one point, so he changed the password to get access and he did this on an occasion he was at the home with Mr SW trying to resolve the issues. He says this was standard practice and no underhand behaviour.

[25] I do not find it established in evidence that Mr Campbell changed the password surreptitiously to have covert access to Mr SW's system. While he should have provided Mr SW with this password there was nothing materially superior about the admin account to the alternative account which disadvantaged the SWs. The fact that Mr SW could delete the admin account from his own supports this finding.

[26] Accordingly, I do not find it established in this instance that Mr Campbell's actions were materially improper.

*Did Mr Campbell act in a professional manner?*

[27] Mr SW says that Argyle's job was unsatisfactory, and they were left with a malfunctioning security system and poor workmanship. They have had to spend many hours themselves trying to fix the problem which he considers should have been Mr Campbell's responsibility. They have had to purchase three replacement cameras themselves which has now repaired the system.

[28] Mr SW says that's Mr Campbell responded to their complaints with a lack of regard or motivation to resolve them. It felt to him, he says, that Mr Campbell had no interest in fixing the problems for them and sent them off to research online themselves and try different settings.

[29] Mr Campbell says he never told Mr SW to change the settings, but he did so of his own volition which made their troubleshooting challenging. He also says he never told them to research online, a task Mr SW also undertook on his own. Mr Campbell is clear he was attempting to work as hard as possible to resolve the issue for Mr SW which was challenging.

His evidence is that the problem was the specifications of the cameras. He had only quoted for 4-megapixel cameras but given the particular things Mr SW was videoing, they needed 8-megapixel cameras. He says he suggested this change himself to Mr SW.

[30] There was disagreement over the way some parts of the install were completed but the evidence does not substantiate that they amount to a finding of unsatisfactory conduct or misconduct. I do not find it proven in evidence that Mr Campbell was reluctant to resolve the issue for Mr SW, in contrast he did engage to sort it out for him.

[31] The communication however between the parties at the end of the relationship was acrimonious. Mr Campbell certainly used an inappropriate tone at times, telling Mr SW that he was 'full of it', telling him to 'get over it' and calling his allegations 'crap', 'lies and BS". I do not consider this professional dialogue.

[32] This allegedly continued after the hearing. Mr SW provided a screenshot of messages Mr Campbell allegedly sent him calling him a liar. They also said that he did not "give a shit what PSPLA say".

[33] I find it established that these comments that Mr Campbell made are unsatisfactory, and not what one can expect from a professional security technician. I also find the disregard Mr Campbell has shown to the Authority concerning. The Authority is the regulatory body for his chosen profession and a disregard for such regulation is not appropriate. Breaches of the Act are offences and punishable upon conviction by fine. These comments were unsatisfactory conduct.

[34] Mr Campbell questions the genuineness of the complaint saying that Mr SW has been stimulated to file it upon the encouragement from another security company that, for some reason, has a vendetta against him.

[35] Mr SW clearly understands that there is no financial gain for him in lodging this complaint or going through this process; he says he is just doing this so that others do not suffer the same issues he has. He explained he is going through a difficult personal time in other ways which is why he has not taken the matter through the Disputes Tribunal. However, he considered it important that he complete this process.

[36] As the complaint has been established in part, I do not consider the complaint was made in bad faith, or that it is frivolous or vexatious. It clearly took a personal toll on Mr SW to file the complaint at a time of difficulty for him, and he had nothing to gain from it.

*Conclusion*

[37] Having considered all of the evidence carefully, I am satisfied that Mr Campbell is guilty of unsatisfactory conduct. I have come to this conclusion, based on the following findings:

- [i] Mr Campbell did not make Mr SW aware that he could, or would, access his camera footage remotely before he did so.
- [ii] Mr Campbell engaged in inappropriate dialogue with Mr SW on various occasions after he filed his complaint.
- [iii] Mr Campbell appears to have little regard for the Authority or governing Act.

[38] The Authority's disciplinary powers upon the upholding of any complaint are to be found in section 81(1B) of the Act. In determining the appropriate penalty, I need to consider the gravity of the unsatisfactory conduct, the impact of any penalty and any other relevant factors in relation to Mr Campbell's competency, experience, and character.

[39] In this light I note the lack of remorse from Mr Campbell and his insistence at the hearing that he had not done anything wrong. There is no evidence that Mr Campbell lacks technical ability, as it is his subsequent (to his installation) interactions that are at issue. I also note the disregard Mr Campbell has for the Authority and law.

[40] Having considered all the relevant factors, I consider it appropriate to make the following orders:

[a] Mr Campbell is officially reprimanded[1].
[b] Mr Campbell is to apologise[2] in writing to Mr SW and provide confirmation that he has done so to the Authority no later than 31 December 2023
[c] Mr Campbell must undergo training in the area of privacy law[3] within the next twelve months and provide evidence of his having done so to the Authority.

*Other*

[41] A further issue was dealt with separately but is relevant to note in this decision for clarity and public education. On some official documentation of Argyle's the following emblem was included:


[42] Licence holders are not authorised to use the Ministry of Justice logo. In fact, no one is permitted to use the Ministry of Justice Logo without authorisation. In addition, it is legally wrong, as the Private Security Personnel Licensing Authority (PSPLA) is an independent Licensing Authority administratively supported by Ministry of Justice. It is the PSPLA that has granted Argyle's licence and not the Ministry of Justice. The PSPLA is not a part of Ministry of Justice.

[43] Mr Campbell was unaware of this and has undertaken to remove any such reference in Argyle's documentation. He is therefore not criticized for this action and this information is included in the decision for public education.

*Should any of the decision be redacted when it is published?*

[44] Pursuant to section 96C of the Act, this decision must be published unless there is good reason not to do so.

[45] Mr SW does not wish his details to be published as he says they are not relevant to the issues discussed. He says the concerns are about Argyle and Mr Campbell, and who he is,

[1] Section 78(1B)(d) of the Act
[2] Section 78(1B)(e) of the Act
[3] Section 78(1B)(a) of the Act

is irrelevant to their conduct. I agree with this submission. I also consider it inappropriate to deter members of the public from making a complaint regarding security personnel. Accordingly, I direct that Mr SW's details are to be redacted from the published order.

[46] Mr Campbell does not wish his details to be published either because he says this was a one-off situation which should not reflect badly on him with his other customers. He considers Mr SW's complaint disingenuous and as such says he should not suffer because of his "buyer's remorse".

[47] I do not accept Mr Campbell's submission as the complaint has been upheld, and I consider it of public interest that his details be published. Accordingly, his application for suppression is dismissed.

**DATED** at Wellington this 27th day of November 2023


K A Lash
**Deputy Private Security Personnel Licensing Authority**