Andrew Gould
Detective Chief Superintendent
National Cybercrime Programme
NPCC

25th November 2020

Dear Mr Moore

I write on behalf of the National Police Chiefs' Council. We refer to your previous engagement with the Police CyberAlarm team, and the blog post you published yesterday entitled 'CyberAlarm: An independent security review... and why you should avoid it' at the following url, which was tagged with the terms 'CyberAlarm', 'Police', 'Security', 'Vulnerability', 'Pervade', 'Pervade Software' and 'SME':

https://paul.reviews/cyberalarm-an-independent-security-review-and-why-you-should-avoid-it/

We also refer to your Tweets to the 3651 followers of your Twitter account @Paul_Reviews

(https://twitter.com/Paul_Reviews) concerning your blog post, including but not limited to:

>   https://twitter.com/paul_reviews/status/1330976174084923397?s=21
>   https://twitter.com/Paul_Reviews/status/1331258549289312263?s=20
>   https://twitter.com/Paul_Reviews/status/1331268271937638400?s=20
>   https://twitter.com/i/status/1331342205030715393
>   https://twitter.com/Paul_Reviews/status/1331376181292228609?s=20

As you knew at the time of publication, or should have known (including having regard to your professed expertise in the area of Information Security), it is patently false for you to state that you uncovered *"critical #security issues with #CyberAlarm"*. As had been repeatedly explained to you prior to publication, you had not examined any code, which was pertinent to the launched Police CyberAlarm tool. The sensational conclusions you reach concerning your purported findings are entirely unfounded.

You have also mischaracterised the communications that took place between you and both the Police CyberAlarm team and Pervade. Any and all legitimate security concerns are taken with the utmost seriousness and are thoroughly investigated. It is not the case that the response to your concerns was merely that these were not a *"deal breaker"*, as you suggest, or that your advice that the Police CyberAlarm ought to be withdrawn was simply rejected without further investigation. Rather, and as you know, the concerns you raised were investigated and found to be unfounded.

Police CyberAlarm has been, and continues to be subjected to, independent external security reviews. The most recent of these, undertaken by a CREST STAR and NCSC-approved CHECK consultancy considered the issues you had flagged. Unsurprisingly, the independent analysis did not find any of the

issues you had raised in Police CyberAlarm. Nor did the review find any other significant security issues with Police CyberAlarm.

Nor was it merely the case that you were asked to give "feedback". Steps were taken to engage with you in an effort to understand your concerns. These were investigated and when they were found to be irrelevant to the Police CyberAlarm as launched, you were informed of this. You, unjustifiably, maintained your position. You were also informed of the outcome of the external security review. You were invited to provide further feedback should you have any, notwithstanding the unfounded concerns you had previously raised.

We should make clear that at no time were you engaged to conduct a review of Police CyberAlarm and therefore you have not had access to the code underlying the system.

Your tweets and your blog post contain false and misleading information, and should never have been published. Your assertions to the effect that entities should avoid engaging with Police CyberAlarm on the basis that the system is fundamentally insecure are strongly refuted and wrong.

Regrettably, however, your publications are liable to cause significant and irreparable damage to the Police CyberAlarm brand and to its further rollout, harming efforts to improve the cybersecurity of organisations in the UK and requiring the further expenditure of public funds. We also consider that they are likely to have caused harm to Pervade, but we will leave it to them to take any legal action that they may consider appropriate. By taking the steps requested below, you may be able to mitigate at least some of the damage already caused.

We note in this regard that your tweet publicizing your blog post (https://twitter.com/Paul_Reviews/status/1331258549289312263?s=20) has received, at the time of writing, some 36 retweets and 32 quote tweets, reaching a potential audience of in excess of 300,000 individuals and entities. You also took deliberate steps to bring your allegations to the largest possible audience, directing your blog post to a number of journalists and influential technology professionals.

As to your suggestion that you have published this information "responsibly" to allow the public to decide for themselves whether to engage with Police CyberAlarm, in circumstances where you have published information which you have been repeatedly informed is wrong, there can be no basis for any suggestion that your post and Tweets are in the public interest. In this regard, it is notable that you failed to include due, or indeed, any reference to the position of the Police CyberAlarm team or Pervade, of which you were well aware. Indeed, to any one in possession of the facts, it would appear that your efforts are merely intended to increase your own traction, and to malign and cause damage to both the Police CyberAlarm product and the supplier and developers behind it.

Finally, we note that you have utilised the PoliceCyberAlarm logo without permission.

In the circumstances, we request that you immediately delete the blog post and tweets concerning the post and Police CyberAlarm and that you publish a correction in the following terms on both your blog and on Twitter:

From 23 November 2020, I published a series of Tweets and a blog post concerning Police CyberAlarm, a tool developed by Pervade Software, to improve the security ok UK businesses. I alleged that Police CyberAlarm was insecure, and should not be utilised, and referred to my analysis of code that I suggested was used in Police CyberAlarm.

As I knew at the time of my publications, the code to which I referred does not form part of Police Cyber Alarm and the conclusions I reached cannot legitimately be based on the analysis to which I referred. I have therefore deleted my publications.

I have been asked to clarify by the National Police Chiefs' Council that Police CyberAlarm has been independently and externally tested by a professional cyber security organisation, that the issues I raised were not found to exist in Police CyberAlarm, nor were any significant cyber security issues identified. I had been informed of this prior to my publications.

Given the damage already caused and which will continue to be caused unless remedied, we request that you take these steps by noon on Friday 27th November 2020.

We also request that you cease and desist publishing the same or similar falsehoods in future.

It is regrettable that it has proven necessary to write to you in these terms, but your actions have left no other option.

Yours sincerely

Andrew Gould
Detective Chief Superintendent
National Cybercrime Programme
NPCC