On 21 February 2022 Vision West was a victim of a ransomware attack. It resulted in much of our database being encrypted and with a request from the hackers for payment to unencrypt the files. Fortunately, Vision West has a robust backup system, which made it possible to ignore the request from the hackers and restore the database that morning.

The reason for this notice is to inform anyone that had personal information in our database before the day of the attack, of the possibility that their information could also have been extracted. However, we have not received any notification or evidence of any files being uploaded from our database and we received further reassurance from three separate professional opinions who suggest that the nature of this breach is usually only to seek a ransom for encrypted files. Any personal information about our clients is also embedded in proprietary optical software, adding one further layer of complication for anyone viewing our database. As far as individual financial details, Vision West does not store records of bank account or credit card details of any of our clients.

Professional opinion suggests the malware entered our system via an email. For this reason, we have updated all passwords and added even further layers of security and early warnings to hopefully eradicate the possibility of ever receiving another breach.