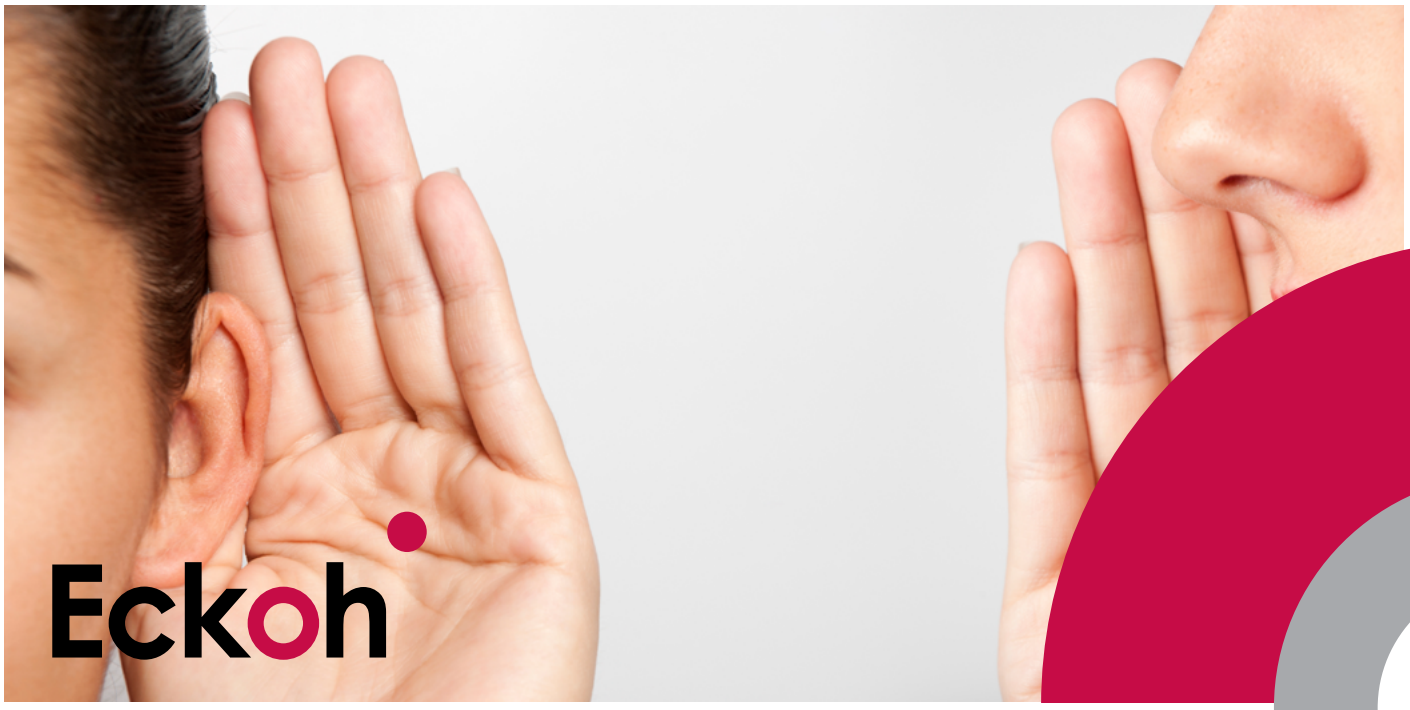

Five urban legends about PCI DSS and call recording

As the PCI DSS directive has established itself, inevitably urban legends have also evolved, causing confusion for organisations and individuals alike. One of Veritape's core values is to deliver straightforward technology which is easy to both understand and use and in our opinion, the confusion around PCI DSS isn't necessary. We think that it diverts attention away from its primary objective of protecting customers and payment card data.

In an effort to set the record straight, here are clarifications to five common urban legends about PCI DSS and call recording.

1. We can encrypt the call recordings

It is a fact that if the PAN (that's the long number of the front of the card) is stored in call recordings, it must be encrypted. However, once a payment has been authorised, the three- or four-digit CV2 security number on the card must not be stored at all.

Encryption is not an adequate tool to prevent the CV2 from being stored because, by design, every call recording system which uses encryption also uses decryption to give supervisors, trainers and other staff members the ability to listen to calls. Yes, encryption is used in some of your other payment processes, like the secure payment connection used in web browsers. But it's the fact that both encryption and decryption abilities sit side by side in the same environment (i.e. your contact centre) which makes encryption for sensitive authentication data inappropriate. Point 3.2 of the PCI DSS Requirements and Security Assessment Procedures make this very plain: "Do not store sensitive authentication data after authorization (even if encrypted)"

2. I don't have to comply yet; I'm a small business so I don't have to comply

All deadlines for compliance have passed. All organisations, irrespective of their size, are now required to be PCI DSS compliant.

3. PCI DSS isn't an issue for us as you can't mine data from audio recordings

The reality is that card data is easily mined from audio recordings, using any number of free or paid-for tools. As technology becomes more sophisticated, it is becoming easier to do so - there are plenty of speech recognition software tools available which will index and locate card data from within audio recordings.

4. Using an IVR system will make me PCI DSS compliant.

Not necessarily. While there are PCI DSS compliant IVR systems on the market, many of them do not comply. Using an external IVR to handle card payments may just move the problem around.Sometimes calls handled in this way are recorded too!

Furthermore, sometimes the IVR does not prevent card data from being sent back to your site which means that your on-site recording systems still capture the card data.

You may still need to employ a method of making call recordings associated with payments PCI DSS compliant. (On a practical note, you also need to consider the impact on customer service satisfaction levels caused by IVRs – many customers do not like them.)

5. Audio data breaches in contact centres don't happen so the risk of a fine is minimal.

The simple fact is that if you were to suffer a data breach as a result of information stored in call recordings, you would leave your business open to fines from your card acquirer.

It's true that contact centre data breaches involving audio are not in the public eye, but they certainly do happen. The UK's largest two acquiring banks have separately reported to us that their customers have suffered audio data breaches and been fined for doing so. In addition, in some US states, where data breach notification is being introduced, data breaches are becoming more widely reported.

Strict confidentiality agreements between card issuers, acquirers and merchants, coupled with a lack of mandatory data breach requirements, largely account for why audio data breaches aren’t in the public eye – but they do occur. So there you go: clarification on five urban legends about PCI DSS and call recording.