Fraudsters have you in their sights...our tips will help stop them stealing your card data

Credit card criminals are now targeting call centres. Jeremy King, of the PCI Security Standards Council, explains the new guidance on how to protect your customers

THANK S to technological advances, industry collaboration and greater vigilance, face-to-face fraud is being reduced significantly.

But, as we've seen, when we push criminals away from one type of fraud they quickly go looking for another. It is therefore increasingly important to address not just the technologies but also the people and processes that are essential to help secure payment card data.

For merchants and service providers, the PCI Security Standards are designed to protect card data. They require measures to protect any systems that store, process and/or transmit cardholder data.

And this applies to call centres where credit card information processed over the phone may be recorded and stored.

In cooperation with Barclaycard, and other organisations, we have produced a new document to help provide guidance on securing card data for those who take payments by phone.

As you may be aware, a number of regulatory bodies require companies to record and store phone conversations at call centres. In addition, calls are often recorded for training and dispute resolution. These calls can include card payment data.

However, the Payment Card Industry Data Security Standard (PCI DSS), stipulates that the three-digit or four-digit card verification code or value printed on the card (CVV2, CVC2, CID, or CAV2) cannot be retained after authorisation, and full primary account numbers (PANs) cannot be kept without further protection measures.

Call recording potentially exposes cardholder data to unnecessary risk.

This problem is challenging for all markets, because those committing card fraud have become focused and organized. They are no longer opportunist criminals but organised gangs specifically targeting your sector as they know there is a lot of card data to be obtained. These are targeted attacks, looking for easy data.

For example, last year the hospitality industry became the most targeted for data breaches according to a global security report from Trustwave. The situation has grown in such a way that recently, one of the largest hospitality industry associations put forward guidance on how to mitigate credit card fraud targeting the industry.

These incidents of fraud aren't specific to call centres, but they do illustrate the ways that criminals will move around to find the data and steal, whether through an unprotected POS system or call centres.

So what has the PCI Council done to help you maintain the integrity and security of card data in your call centre?

The Protecting Telephone-Based Payment Card Data Information Supplement provides actionable recommendations to merchants and service providers for securely processing payment card data over the telephone. The council developed the information supplement to assist merchants and service providers with meeting PCI DSS requirements to secure payment data captured by recordings. It provides tactics and best practices on how to secure recorded data, with information drawn from resources developed by PCI SSC board of advisor member Barclaycard.

Hopefully, with this new guidance in place, we will have better consistency and improved security among merchants, service providers and the assessor community, by providing a common set of best practices for the interpretation and implementation of PCI DSS requirements for the protection of payment card data in call centre operations. Together, with the PCI Standards and supplemental guidance documents, we can continue to reduce fraud rates globally.

Do check out the new supplement and the rest of the resources we have in place for you in our documents library on the PCI SSC web site.

Take action now and you can help make your organisation more secure. And, if you'd like to participate in providing meaningful feedback to help evolve the PCI standards and supplemental guidance, please do consider joining us as a participating organisation. Being involved in this way gives you the chance to shape the future of payment card security – this includes early access to any documentation and a review of proposed changes.

Plus, you get two free tickets for this year's European Community meeting in London in October and a substantial discount on our training courses.

- You can get more details at https://www.pcisecuritystandards.org/get_involved/index.php.

Jeremy King, European regional director, PCI Security Standards Council; jking@pcisecuritystandards.org

Are you doing enough to protect your data?

WITH a string of high profile breaches in data security, I do not believe that PCI compliance and its threat of heavy fines is enough.

Getting data protection right has never been more important. We are increasingly asked to complete transactions online and provide our personal details. Real data security can only be achieved by companies treating security with the importance it deserves, and this means from the board down.

PCI compliance is the minimum requirement for securing card holder data, but this should be supported through rigorous testing and company wide policies, certified through the likes of ISO 27001. Many companies are doing the minimum to comply and are not as secure as they could be, failing to actually test any safe measures and monitor them regularly.

In my opinion PCI compliance is a MUST for all call centres that regularly handle financial transactions. However in addition to this companies should have regular procedures written up to test and monitor.

We work with a number of charities and banks to provided hosted call centre solutions and here are some of the additional measures and tests we put in place:

Have the design of your network ratified by a specialist, including firewall rules

Implement strong access control: restrict access to all data, including cardholder by business need-to-know; assign a unique ID to each person with computer access; restrict physical access to cardholder data

Audit: track and monitor all access to network resources and cardholder data (is someone logging on at 2am, for example); regularly test

Please turn to page 16 ➲

Our tips in a nutshell

OUR new supplement builds on a previous FAQ by providing specific, actionable payment security advice for implementing PCI DSS requirements to protect card data processed over the telephone, including:

- How PCI DSS applies to cardholder data stored in call recording systems
- Recommendations for merchants when assessing risk and applicable controls of call centre operations
- Quick reference flow chart that provides a step by step process for determining necessary controls to meet PCI DSS requirements for voice recordings
- Specific guidance addressing storage of sensitive authentication data: including suggested methods for rendering data unavailable by query

The hints and tips for call centres section in the paper offers guidance on key considerations you face when implementing PCI DSS requirements, including specific recommendations and best practices. Examples include:

If you don't need it, don't store it! Make sure payment card data is only stored when absolutely necessary and that disposal procedure is put in place

Don't share passwords Customer service representatives, sales agents and administrators should all have unique log-in credentials

Limit access Allow access only on need-to-know basis; segment call-centre operations so that a limited number of sales agents have access to payment card data