Fraudsters have you in their sights…our tips will help stop them stealing your card data
Continued from page 14

security systems and processes (employ a specialist firm to try to break into your network)

Maintain an information security policy: ISO 27001 is an excellent means to do this.

Matthew Bryars, chief executive of Aeriandi, a call centre software provider; matthew.bryars@aeriandi.com

Stay safe and save time and money

IT IS more than five years since the major providers in the payment card industry banded together to develop common standards to protect users from fraud.

The requirements for compliance with the PCI Data Security Standards are far reaching. They include voice recording where the rules make it absolutely clear that encryption is not acceptable and that recordings must not contain data such as the three-digit CVV number on the back of the card.

To many call centres, compliance audits represent budget and time that could be better spent elsewhere. However, non-compliance can be serious in terms of fines and litigation.

How can you meet the standards and still maintain the customer experience?

Our web-based product provides clients with PCI compliance. With no break in the conversation, callers input their card details with the telephone keypad, completely removing the risk of agent fraud.

Agents simply initiate each process via their PC and subsequently receive an on-screen update on whether the payment has been successful and the system automatically collects the payment for the client. In the event of a failed payment, the failure reason code is displayed.

It means that all sensitive data passed over the telephone – including bank details, personal identification data and credit/debit card transactions – are secure.

The benefits include: simple compliance adherence; improved experience and increased confidence for customers; and less time needed to monitor agents.

Joanne Hatherley, sales director, Ultra Communications; joanne.hatherley@ultraasp.net

New ways to stay safe...but look out for the cloud

THE PCI Security Council's new guidelines setting out recommendations for processing payment card data over the telephone are a welcome boost for all organisations and will provide clarity about the risks involved with data security in call centres.

Every year we share more and more of ourselves online and rely on third parties to keep our information secure.

But fraudsters are vigilant and resourceful. According to the UK National Security Strategy (October 2010), identity fraud costs more than £2.7 billion and affects over 1.8m people every year in the UK.

Despite card fraud falling by nearly £75m in 2010 to the lowest level for a decade (UK Card Associations, March 2011), thieves still managed to get away with approximately £1m per day last year.

For call centres, authentication technologies are not as established as those for online trading, but there are solutions emerging that will bring significant improvements.

For example, products that mask dual-tone multi-frequency signalling (DTMF) can help your agents from ever handling card information. This not only simplifies your security endeavours, but also provides for more employee-friendly security policies. Alongside the release of these new guidelines, new validation questionnaires have been introduced to simplify customer eligibility criteria.

The role of cloud computing will become increasingly important for call centre managers. A study by Cisco Systems in December 2010 projected that almost 12 per cent of all enterprise workloads will run in the public cloud by the end of 2013. It is not surprising that the key deciding factors for migration to the cloud are: data custody, control, security, privacy, jurisdiction, and portability standards for data and code.

Essentially, call centres will have to perform a balancing act of losing control gracefully, whilst maintaining accountability when the operational responsibility of handling and securing their assets lies with one or more third parties.

You can best achieve this by asking cloud providers for transparency and disclosure on how

"Customers should always feel that their data is completely secure when speaking to an agent"

assets are handled and secured, making sure they have good security credentials (and PCI DSS compliance at Level 1 is a good start) and, lastly, reviewing contractual obligations thoroughly.

Customers should always feel that their data is completely secure when speaking to a call centre agent.

There is still more to do to create security solutions that benefit call centres, notably in the area of VoIP, cloud computing and mobile security, but the acceptance of these guidelines is the first step to ensuring customer data remains secure and out of fraudulent hands.

Neira Jones, head of payment security at Barclaycard, is a board adviser with the PCI: SSC and was part of the team which created the new guidelines to protect telephone-based payment card data; Neira.Jones@barclaycard.co.uk

The risk-free way to take card payments... and at far less cost

THERE is a way for your agents to take payment calls without risk to card data – and at far less cost. In addition, it reduces call handling time, improves customer satisfaction and eliminates any opportunity for agent fraud.

Using services from Opal, and other major telecoms carriers, customers enter their card details with their telephone keypads.

Unlike an automated payment IVR, agents remain in conversation throughout. Agents and, more importantly, the recordings – whether hosted or on your own equipment – do not hear or capture the DTMF tones but only a flat monotone which cannot be reverse engineered back to the credit card number. Credit card details are sent directly from the carrier cloud to Commidea's payment gateway where they are sent onward for authorisation to the acquiring bank.

This approach avoids the need to adhere to up to 222 information security controls, mandated by PCI DSS, which can cost hundreds of thousands of pounds for small call centres and several millions for the very largest.

If your agents listen to credit card details, then the following could be required: card keys; CCTV; white boards only (no paper and pens); no access to email, web or mobile phones; a policy to protect card data; agent supervision; and background checks and lockers for every member of staff.

Call centres that have implemented these "clean room" environments have experienced increased attrition and decreased agent morale.

Most small contact centres cannot justify the expenditure of becoming PCI DSS compliant. They will have to look to hosted payment services which are far cheaper. In effect, they will be outsourcing their payment processing to their carrier who will need to be a PCI DSS Level 1 service provider and take the liability of PCI DSS.

The IT manager at Registration Transfers, Ian C. Clayton, said: "Using Semafone in Opal's cloud has allowed Registrations Transfers to remove all card data from our organisation and eliminate the need to be PCI DSS compliant within our contact centre. This allows our 45 agents to take card payments without ever hearing or seeing card data and eliminates any opportunity for agent fraud".

Graham Thompson, sales and marketing director, Semafone; graham.thompson@semafone.com