Contact centres — A new opportunity for card fraudsters?

Fraud and compliance challenges for contact centre payments and the new technologies helping firms beat crime and stay legal

Received: 6th August, 2011

Mike Havard

has been involved in the customer management industry as practitioner and adviser for over 25 years. He remains involved as director and adviser for a range of technology, operations and consulting businesses, and is a non-executive director at Semafone, a leading technology company for securing voice transactions and payments in contact centre environments.

Graham Thompson

has a long career in technology marketing and sales and is currently the Sales and Marketing Director at Semafone, and a specialist in PCI DSS, payment fraud issues and resolutions.

Mike Havard, Semafone, 120 Bridge Street, Chertsey, Surrey KT16 8LA, UK
Tel: +44 (0)845 543 0822; E-mail: mike. havard@semafone.com; website: www.semafone.com
Graham Thompson, Semafone
E-mail: graham.thompson@semafone.com

Abstract

This paper looks at the challenges contact centres face in meeting the rigorous compliance regulations for taking payments over the phone and in protecting both their customers' card data and themselves from fraudulent card usage. Technology is creating new ways to help combat the risk of data breaches, improve customer satisfaction and gain greater efficiencies and effectiveness within the contact centre. The paper shows how removing customer card data from the infrastructure using secure voice transactions can reduce the risk of fraud and take the contact centre out of scope for the Payment Card Industry Data Security Standard (PCI DSS).

Keywords: *PCI DSS, agent fraud, data masking, tone masking, phone payments, contact centre payments, reputation risk*

MANAGEMENT IMPLICATIONS

- PCI DSS compliance and why it matters.
- Why card data is vulnerable and at risk of fraud within the contact centre.
- PCI DSS requirements.
- Cutting risk by reducing the scope of PCI DSS.
- The benefits of removing card data from call centres.
- Using technology to improve customer satisfaction.
- Opportunities for offshore outsourcers and home workers.
- New advances in tackling card fraud.
- Financial and reputational risks for organisations exposed to card and payment fraud.

INTRODUCTION

Today's contact centres risk data breaches from many potential sources both internally

and externally. Fortunately, technology is creating new ways to combat these risks and help firms meet compliance regulations for taking payments via their contact centres.

The modern contact centre presents two opportunities for fraudsters — a source from which to harvest card data and a target where these stolen cards can be used. Both these risks are increasing as criminals target the 'weak link' in the payment chain. While chip and pin protects bricks and mortar establishments and 3D Secure (Verify by Visa and MasterCard Securecode) does the same for online transactions, phone payments remain vulnerable.

It is this phone element that presents two challenges for contact centres — how to protect their customers' card data and how to protect themselves from fraudulent card usage. Each of these challenges can be addressed using new technology and systems.

PCI DSS COMPLIANCE AND WHY IT MATTERS

The Payment Card Industry Data Security Standard (PCI DSS) is the card schemes' compliance programme to combat fraud and protect consumer card data. It applies to all organisations that store, process or transmit cardholder information, from any of its members' cards (Visa, MasterCard, American Express, Discover and JCB). Larger organisations must have their annual compliance assessment carried out by an independent Qualified Security Assessor (QSA), while smaller companies can use a Self-Assessment Questionnaire (SAQ). The current version of the standard (v2.0 since 28th October, 2010) specifies 12 requirements organised into six 'control objectives' — see Figure 1.

Control objectives	PCI DSS requirements
Build and maintain	1. Install and maintain a firewall to protect cardholder data 2. Do not use vendor-supplied defaults for passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use up-to-date anti-virus software on all systems commonly affected by malware 6. Develop and maintain secure systems and applications
Use strong access controls	7. Need-to-know access to cardholder data 8. Give a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a business-wide policy that addresses information security

Figure 1: The PCI's current control objectives and requirements

Historically, the main source of card data for fraudsters has been non-encrypted card data at rest. Fraudsters have mined this low-hanging fruit predominantly using a technique called SQL injection. Trustwave's SpiderLabs in their 2011 Global Security Report[1] stated: 'While SQL injection is not the most common vulnerability we encounter (7 per cent), the potential for the bulk extraction of sensitive data makes it the number one threat of 2010'.

PCI DSS is slowly eliminating this card data source by having merchants either remove card data within their environment or protecting this 'at rest' data through encryption. As ever, fraudsters are therefore moving on to the next-lowest-hanging fruit — card data in transit. Major frauds have already happened by harvesting data in transit such as with Heartland Payment Systems[2] (although SQL injection was initially used to penetrate their network and then sniffer software used to harvest the data in transit).[3]

The contact centre, like the point of sale and ecommerce applications, has its customer relationship management (CRM) systems where data can be vulnerable but it also has another source of card data at rest and one other source of card data in transit.

Card data can be at rest within call recordings and in transit using Voice over Internet Protocol (VoIP), both points at which they are vulnerable to attack. It is therefore important to look at how card data can be securely entered into the contact centre CRM and for contact centres to protect themselves to the full extent of PCI DSS in these vulnerable areas.

CONTACT CENTRE FRAUD — THE FACTS

As soon as an agent has access to card data by hearing it spoken by a caller or through their CRM system, the contact centre is at risk from fraud. This risk should not be underestimated. Here are some facts related to agent-based contact centre fraud:

- In 1999, 9,000 cases of identity fraud were reported in the UK. In 2010 it had escalated to 102,600.[4]
- People in the UK are three times more likely to fall victim to plastic card fraud than to have their homes burgled.
- 6.4 per cent of card holders were victims of fraud in 2009 — up 36 per cent on the previous year.
- 285 million records were compromised in 2008, 20 per cent caused by insiders. Eighty-one per cent of victims were not Payment Card Industry (PCI) compliant, on average meeting less than one-third of PCI DSS requirements.[5]
- Card fraud in the UK peaked at £609m in 2008, with an estimated £5bn worth of losses per year globally. Although Cardholder Not Present (CNP) fraud was down 15 per cent in 2010, this accounted for 62.1 per cent of all card fraud as opposed to 60.5 per cent of card fraud in 2009. This continues the upward trend from 50 per cent in 2006.[6]
- 82 per cent of financial institutions believe that mass data compromise is a growing threat with 71 per cent reporting credit and debit card fraud and 32 per cent implementing solutions to tackle internal fraud.[7]
- 84 per cent of financial service firm respondents say that they have seen increased regulatory interest in their anti-fraud activities in the past year. Twenty-one per cent of organisations are detecting and preventing less than 20 per cent of the fraud attempts made against them, but 66 per cent believe they detect between 20–80 per cent of fraud.[8]

According to UK police services:

'Call centre internal compromise is the biggest form of up and coming fraud in the UK.'
DCI Mark Wilkie, South Yorkshire Police

'One in ten of Glasgow's financial call centres has been infiltrated by criminal gangs.'
DCI George Easton, Strathclyde Police

'Contact centre fraud is serious, well organised, highly prevalent and very difficult to track — a frightening level of criminality that we don't even get close to. There is undoubtedly 100 per cent penetration of fraudulent activities involving data and personal theft in contact centres — companies will just not likely know. Fraud is rife.'
DCI George Easton, Strathclyde Police

Other employee/agent fraud concerns:

- In 2009, CIFAS Staff Fraud Members noted a 45 per cent increase in the number of cases of fraud committed by employees, compared with 2008.[9]
- 71 per cent of respondents say they have seen the number of fraud attacks against their organisations increase within the last 12 months.[5]
- 89 per cent of IT managers admitted that remote and mobile workers made it harder for them to ensure that their organisation remained compliant with its policies, with 50 per cent of respondents indicating that mobile workers actively ignore all IT policy and regulatory compliance requests.[10]

PCI DSS'S 'DRACONIAN' DEMANDS FOR CONTACT CENTRES

Both PCI DSS requirement 3, 'Protect stored cardholder data'[11] and requirement 9, 'Restrict physical access to cardholder data'[11] apply within the contact centre. To become PCI DSS compliant, many contact centres have elected to operate clean room environments to protect card data. This means they adhere to the following:

1. Provide lockers for all contact centre workers and allow no personal items within the work area;
2. Card key 'in' and card key 'out';
3. Visitor logging;
4. CCTV monitoring;
5. No paper and pens (whiteboard and marker pens only);
6. No mobile phones;
7. No web access (increasingly difficult in today's multi-channel world);
8. No e-mail access;
9. Agent supervision;
10. Agent background checks;
11. Policies to protect card data within the contact centre environment;
12. Masking of card data on all systems (complicating data entry).

This often leads to a draconian environment where agents feel 'un-trusted' and staff churn rates increase. But without a clean room it is very difficult to protect card data. For example, if paper is allowed onto the contact centre floor, then the paper needs to be numbered sheets, allocated to specific agents, collected at the end of the shift and then shredded, incinerated or pulped.

Most contact centre managers will know that these are operationally unworkable and

unrealistic expectations to impose upon their staff, and would not, still, in any sense provide effective mitigation against the determined fraudster.

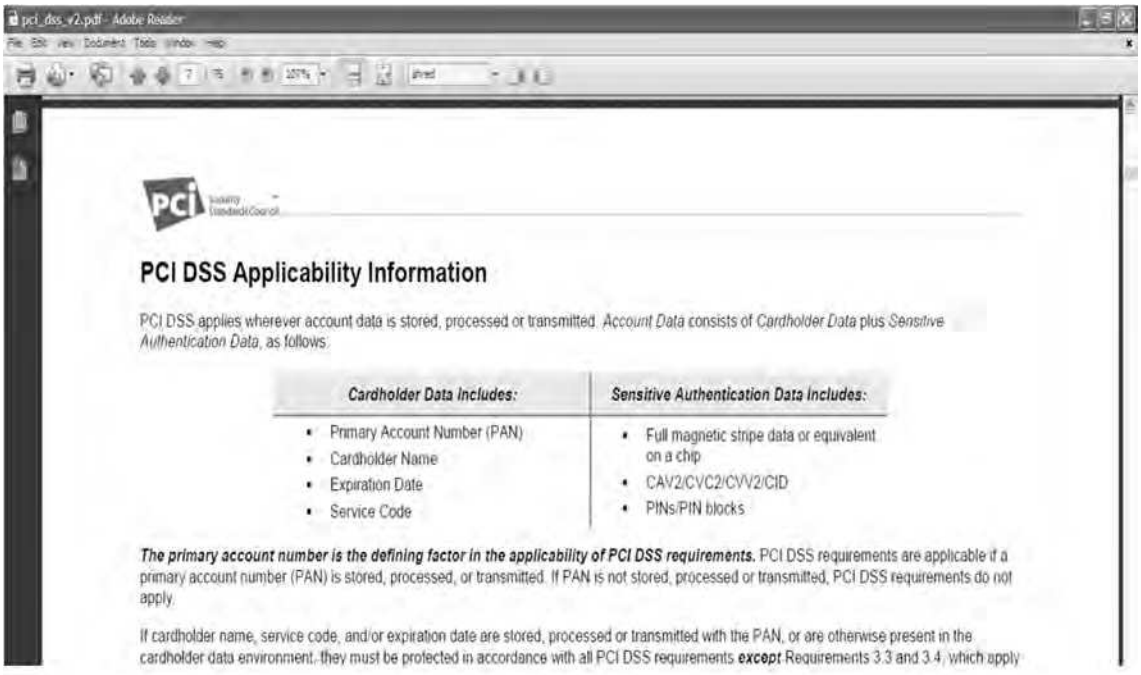
The contact centre has to have a security policy that restricts an agent's ability to remove any card data from the contact centre environment. Clearly, any solution that allows card data to be captured without exposing it to the agent is preferable to the burdens outlined above. The sensible and pragmatic approach has proven to be one where the organisation prevents the temptation of stealing card data arising in the first place by ensuring the data stays out of reach of the staff and systems of the contact centre, thus avoiding the threat of compromise.

FURTHER SCOPE FOR PCI DSS IN CONTACT CENTRES

If agents enter card details into any kind of system via their PC, this immediately brings the desktop and its network into scope for PCI DSS compliance. And if the agent is working on a VoIP handset then both the handset and the VoIP network are in scope for PCI DSS too. If card data is transmitted or stored within the contact centre CRM, then this also falls into scope for PCI DSS.

Alternatively, agents may enter card data into the hosted payment pages of their Payment Service Provider (PSP), but while this can take the CRM out of the picture, the desktop and its network remain in scope. If callers can pay through an automated payment IVR (interactive voice response), then this will also be in scope for PCI.

Finally, if the contact centre records its calls, then one has to consider what card data is being captured. Call recordings are more challenging because, although PCI allows for the capture of an encrypted Primary Account Number (PAN), it does not allow for the storage of Sensitive Authentication Data (SAD), which includes other card data elements such as the card security code (CAV2, CVC2, CVV2 or CID) — see Figure 2.[12] With banks increasingly demanding the capture of the security code for Cardholder Not Present (CNP) transactions, it is now essential to take call recordings out of scope for PCI.


pci_dss_v2.pdf - Adobe Reader

PCI DSS Applicability Information

PCI DSS applies wherever account data is stored, processed or transmitted. *Account Data* consists of *Cardholder Data* plus *Sensitive Authentication Data*, as follows:

Cardholder Data includes:	Sensitive Authentication Data includes:
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full magnetic stripe data or equivalent on a chip • CAV2/CVC2/CVV2/CID • PINs/PIN blocks

The primary account number is the defining factor in the applicability of PCI DSS requirements. PCI DSS requirements are applicable if a primary account number (PAN) is stored, processed, or transmitted. If PAN is not stored, processed or transmitted, PCI DSS requirements do not apply.

If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment, they must be protected in accordance with all PCI DSS requirements ***except*** Requirements 3.3 and 3.4, which apply

Figure 2:: Extract from 'Navigating PCI DSS'

CUTTING RISK BY REDUCING THE SCOPE OF PCI DSS

PCI has 222 information security controls where card data is processed, transmitted or stored. It is not enough to have the capability to apply the controls; organisations have to be able to prove they applied them and took actions based on the results.

These controls require significant investment in the development of new policies, tools and manual procedures to meet them, and also to record them for evidence purposes. Each control and its environment therefore incurs its own built-in cost. And a cost of audit.

As a result, contact centres are finding it more cost-effective to reduce the Card Data Environment (CDE) and eliminate areas which might fall under PCI DSS.

REMOVING CARD DATA FROM CONTACT CENTRES

The simplest way to remove card data from the contact centre is to use an automated payment IVR. Agents can transfer call into the IVR or callers can select it via a menu option. The more sophisticated versions allow the agent to remain on hold during the payment process and keep the agent informed of the progress the caller is making. Although it costs to keep the agent engaged during the payment process, the customer tends to have a better, more 'inclusive' experience.

While some businesses will be willing to allow a machine to process payments, many believe it produces poor customer satisfaction scores and provides lower sales conversion rates — it is too easy for the caller to end the call without completing the payment and then the opportunity is lost. Furthermore, if the caller aborts their attempt to pay through the automated payment IVR then this call still needs to be handled. It is difficult to explain to a client that the only means of making a payment is through the automated IVR or a non-phone channel. While the contact centre is taken out of scope for PCI DSS, the automated payment IVR will itself be in scope and will have to adhere to the 222 information security controls.

There is, however, another way. There are solutions that allow card details to be captured using the caller's telephone key pad, but also allow the voice channel to remain open throughout the transaction. With these solutions, agents verbally invite the caller to enter card details using their telephone keypads. Some of these solutions use white noise to cover the call recording during the transmission of the card details via DTMF (Dual Tone Multi-Frequency) tones. However, the more sophisticated solutions mask the DTMF tones so that agents and the call recording device hear only a flat tone that cannot be decoded to reveal the card details.

Customer satisfaction can be increased as callers intuitively understand that this is a more secure method of sharing card data and, unlike an automated IVR, if the caller has any difficulty the agent can walk them through the process. Once these solutions have gathered the card data, they can communicate this directly with the banks thereby ensuring no card data is shared with the contact centre.

For repeat, recurring and deferred payments, firms can use a token returned from their PSP. The same token can be used for loyalty programmes or other marketing activities. The beauty of the token is that it is out of scope for PCI as it is of value only to the originating business.

While these solutions, unless cloud-based, are in scope themselves, they allow organisations to take out all other aspects of the contact centre from PCI DSS. The more sophisticated solutions can also take the automated payment IVR out of scope too.

THE BENEFITS OF REMOVING CARD DATA FROM CALL CENTRES

As well as the cost reductions already outlined, there are many other benefits to removing

card data from call centres.

Removing any opportunity for agent fraud mitigates any reputational risk. Many organisations have fallen foul of the media for as much as a single breached card. Brand damage has been experienced by Sony,[13] Halifax/Bank of Scotland[14] (Lloyds), Barclaycard,[15] Tesco[16], Norwich Union[17] (Aviva), Netflix,[18] British Airways,[19] HSBC[20] and many more.

This alone is a compelling reason to take card data out of the contact centre. With criminal gangs targeting call centre staff and attempting to put them under duress in order to steal card data, it is also possible to remove such risks to employees. Fraudsters and criminal gangs will quickly learn there is simply no card data to extort.

Through improved customer satisfaction and greater efficiency and effectiveness within the contact centre, these DTMF-based solutions are bringing substantial benefit to the contact centres where they are deployed.

NEW OPPORTUNITIES FOR OFFSHORE VOICE PAYMENT PROVIDERS

Shielding all card data from agents virtually eliminates the possibility of agent fraud. To date, many UK organisations have not outsourced their payments overseas because of the real and perceived exposure to agent fraud within these markets. The BBC and other media outlets have publicised the risks associated with sharing credit card details with overseas contact centres[21] (although these risks also exist within UK contact centres). This presents a great opportunity for offshore outsourcers to mask all card data from agents to offer improved payment services to existing and new clients.

The other opportunity that this provides to internal call centres and outsourcers alike is for home working. According to most QSAs, it is not possible to secure the home environment to comply with PCI DSS where card data is exposed to home workers. Again, by masking all card data from home-based agents and avoiding all card data being processed through the home computer and network these home workers can become PCI DSS compliant.

STOLEN CARDS AND NEW WAYS TO PREVENT FRAUD

It is becoming increasingly difficult to authenticate cardholders for telephone orders. With both chip and pin and 3D Secure, the liability shifts from merchants to the card issuer, but for MOTO (Mail Order Telephone Order), the liability for fraud still lies with the merchant.

Neira Jones, Head of Payment Security, Barclaycard, has said:[22] 'The shift to MOTO fraud has in part been driven by the appearance of scheme-wide initiatives that help reduce fraud. Both face-to-face and ecommerce fraud rates have benefited from these initiatives but there remain a limited amount of solutions that can fight fraud in the MOTO space.'

In countries where chip and pin is fully deployed and 3D Secure is predominantly enforced, MOTO fraud is reaching 60 per cent of all card fraud even though it accounts for only up to 14 per cent of all card transactions. The threat is so great that both MasterCard and Visa have moved directly into the fraud detection space, with MasterCard acquiring DataCash[23] (who had previously acquired Retail Decisions, the provider of ReD Fraud Screen Services) and Visa acquiring CyberSource.[24]

Today, merchants are using simple address authentication and looking to fraud tools to discover patterns that indicate potential fraud. As these often generate false positives, many retailers choose to ship goods even with high fraud scores because of the potential losses of not servicing these false positives and the potential customer relations damage

from declining to do business with genuine clients. Therefore merchants are increasingly looking for new advances to tackle this issue. On the horizon is a new breed of cards with dynamic security codes. In 2012, Visa will launch its CodeSure cards in the UK — see Figure 3.[25] A CodeSure issued card allows the cardholder to authenticate themselves by entering their PIN and then produces a one-off eight-digit Dynamic Security Code that can be authenticated by Verify by Visa.

What is not yet clear is whether it will work for telephone transactions as today 3D Secure is an ecommerce-only facility. On the face of it, it would seem a natural extension to 3D Secure and expose only a one-off security code to an agent. With technologies already available that can mask this data, there could be zero risk. Not only will this protect the merchant from fraud but it will also move the liability of fraud from the merchant to the card-issuing bank.

Other new technologies plan to use voice biometrics to authenticate the cardholder. However, these will be effective only if such solutions are cloud-based and operating across many merchants rather than within a single-merchant environment. It will then be possible to implement velocity fraud checks identifying the same voice across different cards. Genuine cardholder voice biometrics can be established after a period of six to eight weeks when no chargeback (fraud) has been reported. Likewise fraudster's voice biometrics can be registered following any chargeback.

Once these black-and-white lists have been established, it will be possible to fraud score any voice transaction based on a match with the genuine cardholder voice biometric. These solutions will have to take account of the fact that joint account cards do exist and that it is possible to have two genuine cardholder voice biometrics for a single card.

CONCLUSIONS

The financial and reputational risks for organisations being exposed to card and payment fraud are significant and real, and until recently the mitigation strategies have largely been cumbersome, ineffective, operationally impractical and mostly non-compliant with the PCI requirements.

Telephone payments are still the Achilles heel of payment security. They offer fraudsters both a potential source for stealing card data and a place to use stolen cards. The vast investment in chip and pin will be of limited value if the telephony channel remains open to fraud.

By closing this channel to fraud, the industry will be able to relax some of the stringent demands of PCI DSS, in one stroke making the climate harder for fraudsters, and easier for businesses. If there is no channel in which to use stolen cards then the protection of

Figure 3: Visa's CodeSure card

card data becomes less critical. However, it is essential that chip and pin, 3D Secure and secure voice transactions become global realities before card protection can be relaxed. Otherwise cards will be harvested in one market and then be used for fraudulent activity in another.

With chip and pin still about five years from roll-out in North America, there is still some way to go. In the meantime, merchants must not only become fully PCI DSS compliant (achieving it at the lowest cost by reducing their card data environment) but work with the industry's latest offerings to reduce card fraud within their contact centres.

REFERENCES

1. Available at: https://www.trustwave.com/GSR
2. Available at: http://www.njra.org/upload/HPS%20Final%20Press%20Release%202009%2001%2019_743505916_1262009102253.pdf
3. Available at: http://www.philadelphiafed.org/payment-cards-center/publications/discussion-papers/2010/D-2010-January-Heartland-Payment-Systems.pdf
4. Available at: http://www.cifas.org.uk/is_identity_fraud_serious
5. Available at: http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf
6. Available at: http://www.ukpayments.org.uk/media_centre/press_releases/-/page/1324/
7. Available at: http://www.norkom.com/press/whitepapers/729-financial-crime-management-a-renewed-focus.html
8. Available at: http://www.norkom.com/press/whitepapers/536-fighting-crime-defending-the-bottom-line-.html
9. Available at: http://www.cifas.org.uk/secure/contentPORT/uploads/documents/CIFAS%20Reports/The_Internal_Betrayal_CIFAS_Special_Report_Aug_2010.pdf
10. Available at: http://www.netintelligence.com/pdf/On_Demand.pdf
11. See PCI DSS v2.0 available at: https://www.pcisecuritystandards.org/security_standards/documents.php
12. Available at: https://www.pcisecuritystandards.org/documents/protecting_telephone-based_payment_card_data.pdf
13. Available at: http://www.itpro.co.uk/633070/sony-playstation-data-breach-puts-77-million-credit-card-users-at-risk
14. Available at: http://www.liverpoolecho.co.uk/liverpool-news/local-news/2010/02/26/call-centre-worker-stole-money-from-bank-customers-in-250-000-fraud-100252-25916834/
15. Available at: http://www.thenorthernecho.co.uk/news/4166573.Call_centre_worker_stole_customer_s_details/
16. Available at: http://www.dailymail.co.uk/news/article-496119/Tesco-online-store-infiltrated-insider-card-fraudster.html
17. Available at: http://news.bbc.co.uk/1/hi/business/7147704.stm
18. Available at: http://www.idt911.com/KnowledgeCenter/NewsAlerts/NewsAlertDetail.aspx?a=%7B55127584-82F0-4378-8275-D41DB7D2993B%7D
19. Available at: http://www.callcentreclinic.com/myfiles/files/March%2009/OneWeek%20in%20UK%20Call%20Centres%20March%206th.pdf
20. Available at: http://business.timesonline.co.uk/tol/business/law/article680446.ece
21. Available at: http://news.bbc.co.uk/1/hi/uk/7953401.stm
22. Available at: http://www.slideshare.net/Barclaycard/contact-centre-fraud

23. Available at: http://www.mastercard.com/us/company/en/newsroom/datacash_group_plc.html
24. Available at: http://corporate.visa.com/media-center/press-releases/press1010.jsp
25. Available at: http://www.infosecurity-magazine.com/view/13177/rsa-europe-visa-codesure-to-roll-out-in-turkey-soon-uk-in-2012/