



CHARITY PAYMENTS

By James Redhead – Director of Finance @ CTT

PROCESSING CREDIT CARDS AND DIRECT DEBITS - 'New rules and regulations'

The last five years has seen many new forms of fundraising emerging, all requiring new systems and financial controls for processing credit and debit card and direct debit income payments.

The internet has seen the launch of on-line direct debits, known as paperless direct debits, particularly for donations and memberships and a demand for the ability to accept recurring transactions on credit or debit cards.

Face to face fundraising has required new systems for collecting direct debit and card information.

Telephone fundraising and television has seen further growth and the requirements for more sophisticated technology to collect the information required securely and quickly.

Even traditional direct mail campaigns have continued to grow in volume and complexity creating new processing challenges.

The card payment industry has responded to these new payment channels with new regulations and standards, set in the context of increasing security measures to counteract the problem of card fraud. In the past 2 years, we have seen the introduction of 'Chip and Pin' for cardholders present transactions and more recently 'Verified by Visa' and '3D Securecode' for internet transactions.

These new regulations and changes to the rules on what card information may be requested from supporters making payments, has raised queries and caused some confusion in the sector. The changes offer new opportunities for charities as well as some potential threats. This section aims to provide the information you need to understand the implications of these new rules and regulations.

PCI-DSS

PCI-DSS is the abbreviation for the Payment Card Industry- Data Security Standard.

The Payment Card Industry Data Security Standards (PCI-DSS) provide explicit guidelines for collecting; batching; storing and processing credit and debit card payments. The standards are set by Visa and Mastercard and require your acquiring bank to ensure their merchants (e.g. charities) are meeting these standards.

The guidelines apply to every charity, regardless of size, that processes, stores, or transmits credit card data. A charity that fails to comply with this standard and suffers a data breach may be fined by the bank that processes the organization's transactions or have their merchant status removed.

All four leading acquiring banks are now contacting their charity clients to find out whether they are complying with these standards. Do you know whether you comply?



PCI-DSS Compliance

Those organizations required to comply with PCI-DSS are categorized into four levels according to their annual number of credit card transactions.

Level 1 merchants (those processing more than six million transactions a year), Level 2 includes merchants that process one million to six million transactions per year. Level 3 is 20,000 to one million transactions, and Level 4 is fewer than 20,000 transactions a year.

Level 4 organizations don't have to hire a third-party auditor. Instead, they can perform a self-assessment using a questionnaire developed by the PCI Security Standards Council. Level 4 organizations must also undergo an annual security assessment scan from a PCI DSS-qualified organization.

Level 4 Requirements

Most charities process fewer than 20,000 transactions per year and will fall into Level 4. The standard consists of 12 requirements that cover a broad range of security issues, from network protection to access controls to creating an information security policy.

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update antivirus software.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

PCI-DSS is important. If you want to make sure you comply with these new standards, there is a simple solution. The solution is to make sure that you do not keep or collect credit card or debit card information at all.

In practice this means taking the following action:

- Scan all paper documents containing card information, which you have kept for audit purposes and confetti shred the paper records.
- Ensure any third party processors you employ for any fundraising activities such as telephone fundraising; direct marketing campaigns are processing any card information on systems which are PCI-DSS compliant.
- Ensure your on-line donations are processed using a secure payment gateway provider who is PCI-DSS compliant.

If you are in any doubt, please speak to your acquiring bank.



Personal Security

The card payment industry has introduced a number of major security measures to combat the growing problem of card fraud. These measures are a mixed blessing for charities.

Chip and PIN

The introduction of Chip and Pin has been a significant success. The chip on the front of the card is difficult to duplicate and is used to verify that the card is a valid card. The PIN number known only to the cardholder is verified by the Chip on the card.

This technology has been implemented by a range of payment processing companies providing chip and pin terminals for retail outlets. These terminals not only accept credit and debit card payments but can be used for mobile top ups and utility bill payments. Importantly for charities the cost of providing these terminals is coming down and 2008 will see the introduction of free chip and pin terminals, opening up the potential for charities to offer card payment facilities in their retail premises.

AVS/CVV2

AVS is the address verification service, which validates the numeric part of the card holders' address. The limitation of AVS is that it is UK only and is not used by all the card issuers. CVV2 refers to card verification or card security codes. It is more commonly known as the 3 digit number of the back of your card.

There has been a lot of confusion about where and when charities should be requesting the CVV2 number. This is the current position.

If you wish to accept internet transaction e.g. via your charity website, then CVV2 is mandatory. If you wish to accept mail order or telephone order (MOTO) transactions, it is not mandatory to collect the CVV2 number but it is desirable for telephone. The reason is risk; The banks place a higher risk on MOTO transactions are now applying a higher transaction charge as a result. We do not believe it is safe or secure to request a CVV2 number on a donation form, which the donor is then completing and posting back to you. We would recommend you speak to your acquiring bank to confirm their latest position.

Verified by Visa/3D Secure

Verified by Visa and 3D Securecode are the two new card security measures introduced by Visa and Mastercard for internet transactions.

The new security measures will be implemented across all card issuers and by all acquiring banks over the course of the next year. These measures will have a short term impact for charities as the registration process and resulting use by individuals will provide additional information in order to complete their transaction.

The measures work in the following way:

The individual is invited to register with the card issuer and asked for a phrase and password. The individual is re-directed to the card issuers secure web site, where the phrase is displayed to prove it really is the Issuer's site. The individual is asked to enter their password to verify they are the card holder. The issuer web-site then confirms to the card holder the payment. The benefit of implementing Verified by Visa or 3D Securecode is that the liability is shifted from the card holder and charity.

Card Processing Options



The options available to charities when applying or renewing merchant account applications for processing credit and debit cards has also changed. Your acquiring bank should be in a position to offer you the following four options.

Cardholder Present – if you wish to accept card payments from card holders who are present at the time of the transaction taking place, then you will require cardholder present. This will cover retail outlets such as charity shops using chip and pin terminals.

MOTO – the most common option used by charities for mail order and telephone order transactions.

Internet – if you wish to accept donations or take payments for goods via your website, then you will require the internet trading option.

CAT – this is a new option and applies to continuous authority transactions or CAT for short. If you request the CAT option, this will allow you to accept recurring credit or debit card transactions either MOTO or internet. This new option will provide charities with an attractive alternative to direct debits.

The Card Payment Industry is moving quickly to develop new secure processing methods to combat the growing threat from card fraud. Charities need to be sure they are fully aware of the changes taking place and the new rules and regulations. This trend will continue and is expected over the coming years to be followed by BACS in respect of Direct Debit services and the collection and storage of personal bank account information.