

# Internet guidelines for merchant acquirers

Banks put in place stringent checks to prevent rogue internet merchants from obtaining card accepting facilities to sell illegal or unacceptable content online

APACS co-ordinates efforts across the UK banking industry to prevent the illegal use of payment tools, including credit cards and debit cards. Online transactions present specific challenges and the following guidelines have been developed for merchant acquirers (the banks that provide card payment facilities to retailers) outlining the stringent checks acquiring banks will make on a business before they enable them to accept card payments online and the ongoing checks undertaken to ensure they are not involved in unacceptable activities.

The banking industry particularly focuses on rogue merchants involved in unacceptable activities that seek to gain card accepting facilities to sell child abuse images or other illegal content online. Such merchants frequently seek to disguise the nature of their activities by pretending to engage in legitimate business.

A merchant acquirer will not allow or will stop any business involved in unacceptable activities from accepting cards.

The industry also works closely with law enforcement agencies and government to ensure:

- **Full legal compliance**
- **Terminate & report illegal activities**
- **Ongoing checks**
- **Co-operation with third parties**

Due to the efforts of the UK banking industry the problem of rogue merchants obtaining card accepting facilities from UK-based card acquirers has effectively been eliminated. Where the problem continues to exist it is primarily with non-UK based acquirers.

The UK credit card industry provides funding for the Internet Watch Foundation (IWF) to support its activities in fighting illegal sites on the Internet. The industry has worked closely with the Home Office to develop working relationships with the IWF and the Children's Charities' Coalition for Internet Safety. In addition, the industry is an active participant on the Home Office's Child Protection Task Force, and was

instrumental in ensuring the law was recently amended to allow credit and debit card issuers to withdraw cards from online paedophiles.

Previously the Data Protection Act 1998 prevented card issuers from processing sensitive personal data about convictions for purchasing child abuse images where a debit or credit card has been used.

New changes will give card issuers the information needed to fully enforce terms and conditions of cards with respect to such offences.

Continued...

## Guidelines for Acquirers Version 2.0 (June 2004)

### 1. Introduction

Acquiring banks provide facilities to Internet merchants that enable them to accept card payments for content or merchandise.

Acquiring banks deplore the abuse of these facilities on ethical, legal and sound business grounds and make every effort to ensure that merchants are not offering content or merchandise that may damage the reputation of the card payments industry.

APACS has developed the following set of guidelines setting out best practice for acquirers to observe in their relationship with Internet merchants. The guidelines are not legally binding. Failure to follow them does not give rise to any right of action.

### 2. Guidelines for acquirers with Internet merchants

- The UK banking industry unequivocally complies with the law and continues to ensure full co-operation with law enforcement agencies and appropriate regulatory bodies.
- Acquiring banks undertake a number of checks prior to recruiting merchants, and where they believe that a merchant is involved in unacceptable activities then they will not sign up that merchant.
- Acquiring banks routinely monitor the transaction activity of their Internet merchants and where they discover that a merchant is involved in unacceptable activities they will remove the card payment facility and terminate that relationship.

- Acquiring banks will not knowingly do business with Internet sites that sell content or merchandise inciting, advocating or perpetuating activities such as:

- child pornography
- racism
- terrorism
- violence against persons, including scenes of sexual violence.

### 3. Effective date

These best practice guidelines are effective from 30 June 2004.