

INFORMATION, IDENTITY & THE INTERNET
- fighting card crime in the information age

European Central Bank

“Electronic Payments without Frontiers”



APACS

Association for Payment Clearing Services

November 10 2004

Contents

Today's session will focus on:

- why the 3i's is facilitating card crime in the UK
- Combating CNP fraud
- The enemy within
- APACS efforts to curb Identity Fraud
- Tackling 'Phishing'
- Questions

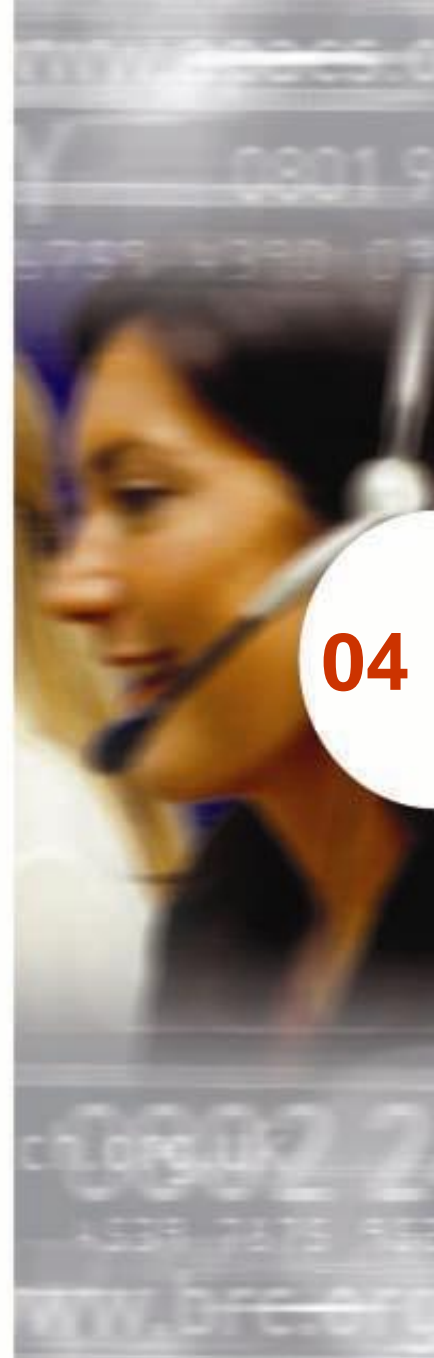


About APACS

- Umbrella Body for UK Banking Industry
- Coordinated approach to non-competitive aspects of fraud prevention
- Known for getting things done I.e. DCPCU, Chip and PIN
- Fraud Migration Projects – CNP and Identity Fraud
- www.apacs.org.uk
- Riten Gohil : riten.gohil@apacs.org.uk : 0207 711 6256

FACT...

- Information is the hottest commodity to the fraudster
- Information, Identity and the Internet is the major conduit to modern day card crime
- This type of fraud is driven by:
 - ◆ Static data authentication techniques
 - ◆ Social engineering
 - ◆ Public sources for consumer data
 - ◆ Weakness in consumer personal security *bin raiding*
 - ◆ The enemy within
- Importantly, Fraudsters...
 - ◆ *know this too!*
 - ◆ *are looking for new methods in Chip/PIN era*
 - ◆ *have an interest in other types of organised crime too*



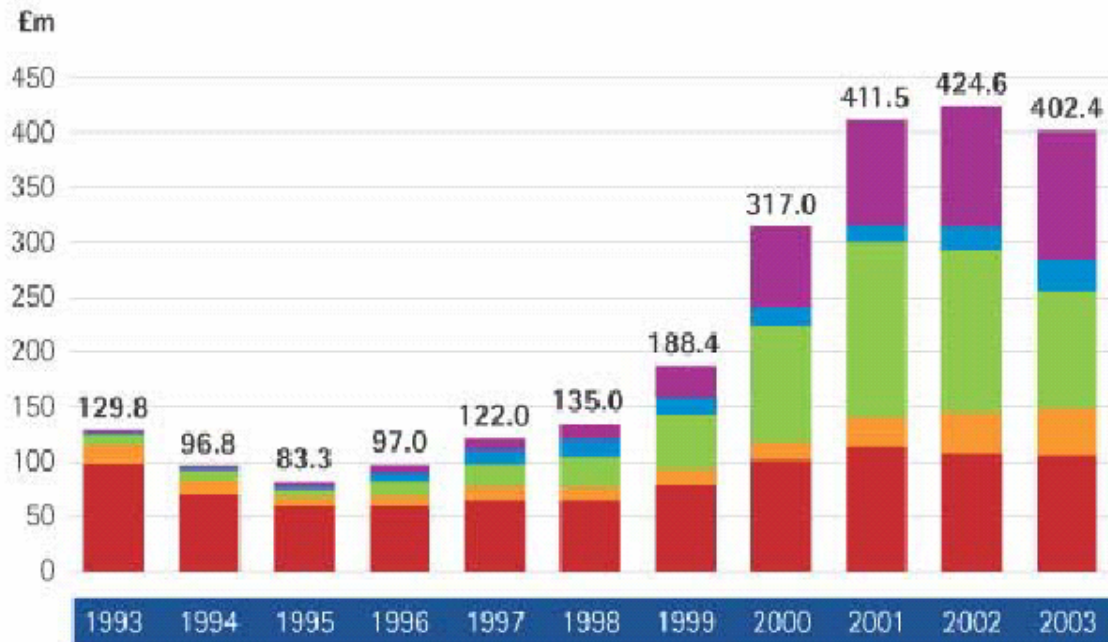
Analysis of 2003 figures

	2003 <i>(change)</i>	2002	2001
Counterfeit cards	106.7 <i>(-28%)</i>	148.5	160.4
Cards stolen or lost	106.1 <i>(-2%)</i>	108.3	114.0
Card not present fraud	116.4 <i>(6%)</i>	110.1	95.7
Mail non-receipt	43.4 <i>(17%)</i>	37.1	26.8
ID Fraud	29.7	20.6	14.6
– fraudulent applications	<i>(45%)</i>		
– account takeover			

UK plastic card fraud losses by fraud type 1993 - 2003

Fraud losses £m

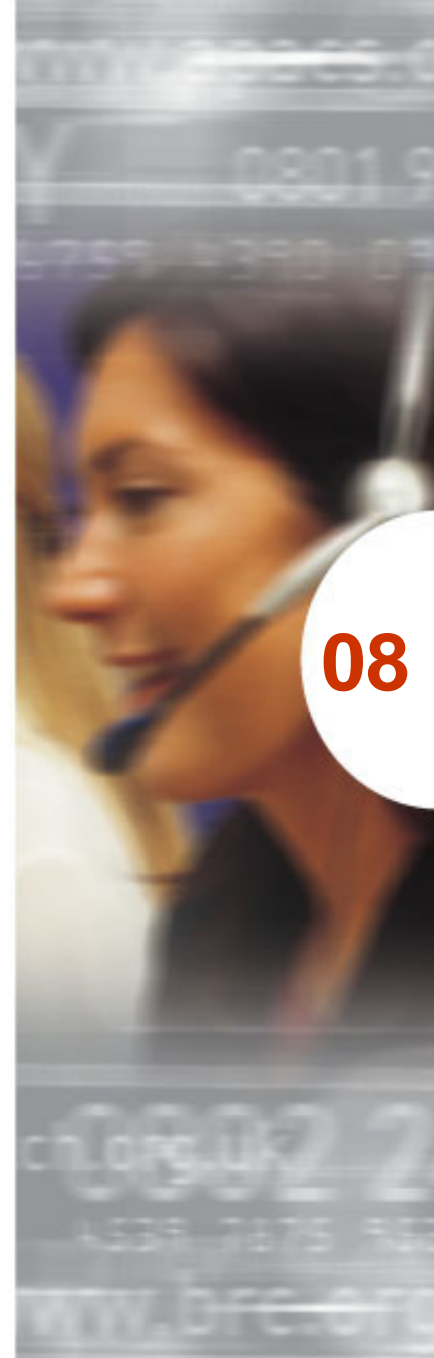
Lost and stolen Mail not-received Counterfeit Identity theft Card-not-present (CNP)



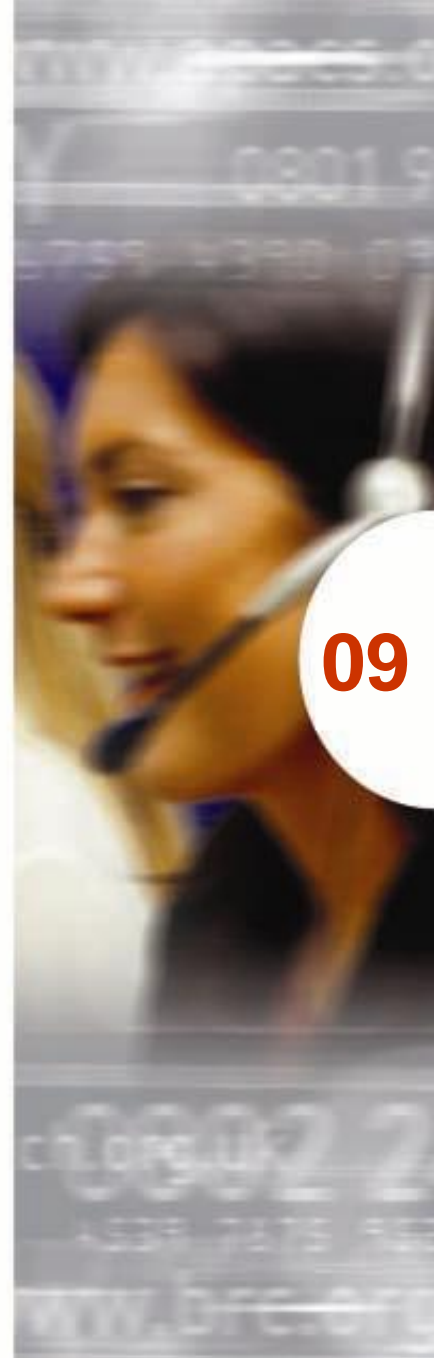
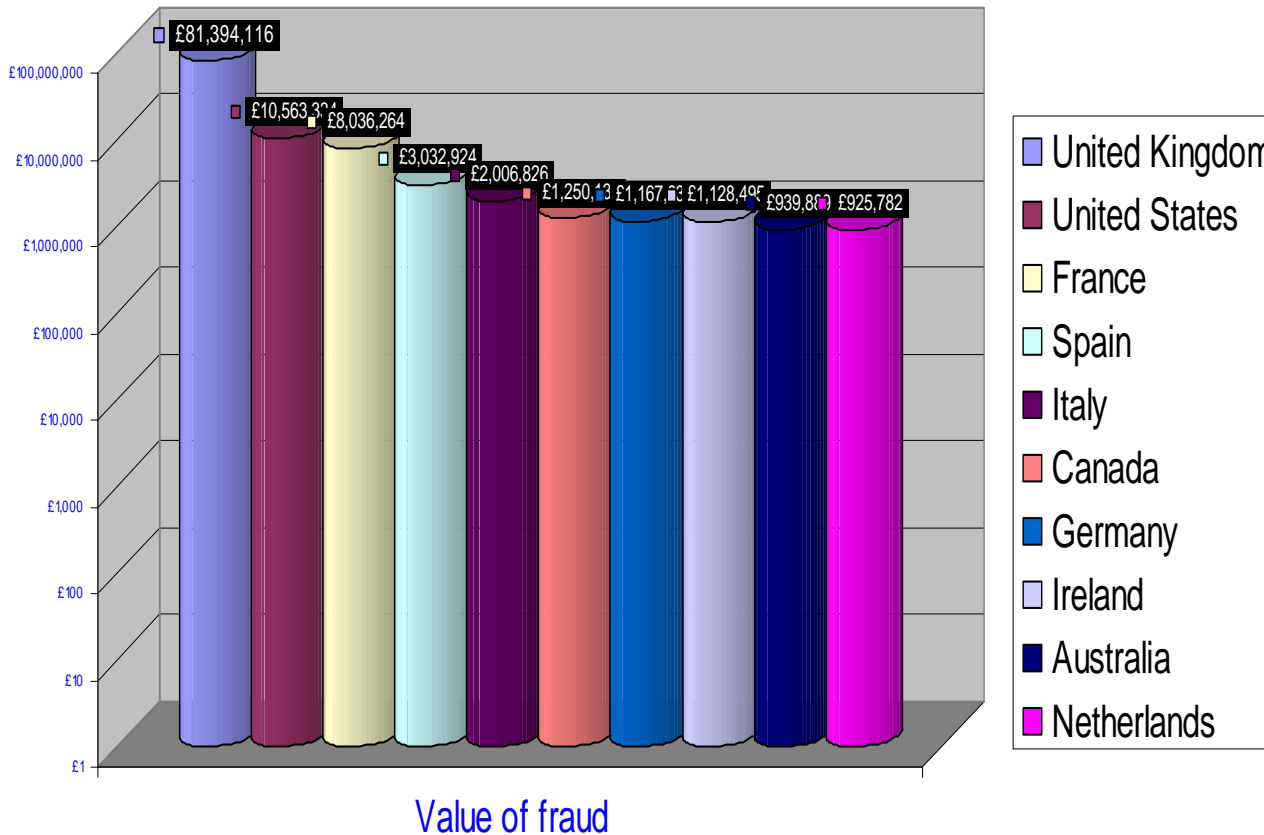
Countering the threat from CNP Fraud



CNP fraud losses 1994 to 2003



Where CNP fraud happened - 2003



APACS CNP Project

- Designed to consider the migration of fraud from Chip and PIN
- APACS undertook a CNP Project in Dec 2002 to tackle the problem
- Development of 4 CNP sector-specific forums
- Educational process first key objective
 - APACS CNP Fraud Training Material
 - Sector-based Best Practices
 - Profiling fraudsters
 - Promoting and realising benefits of existing solutions
- Discussing the development of new solutions

The current risks from CNP fraud

CNP merchants cannot:

- check the security features of a card
- confirm the transaction is made by the genuine cardholder
- neither can the banking industry

Therefore merchants are responsible in the event of fraud

Fraudsters committing CNP fraud:

- are anonymous
- using various techniques to obtain card details
- use other false information to commit the fraud
- have goods and services delivered/provided to addresses that may not belong to the genuine cardholder



The risks from CNP fraud (continued)

Merchants are particularly at risk from transactions outside the UK, because:

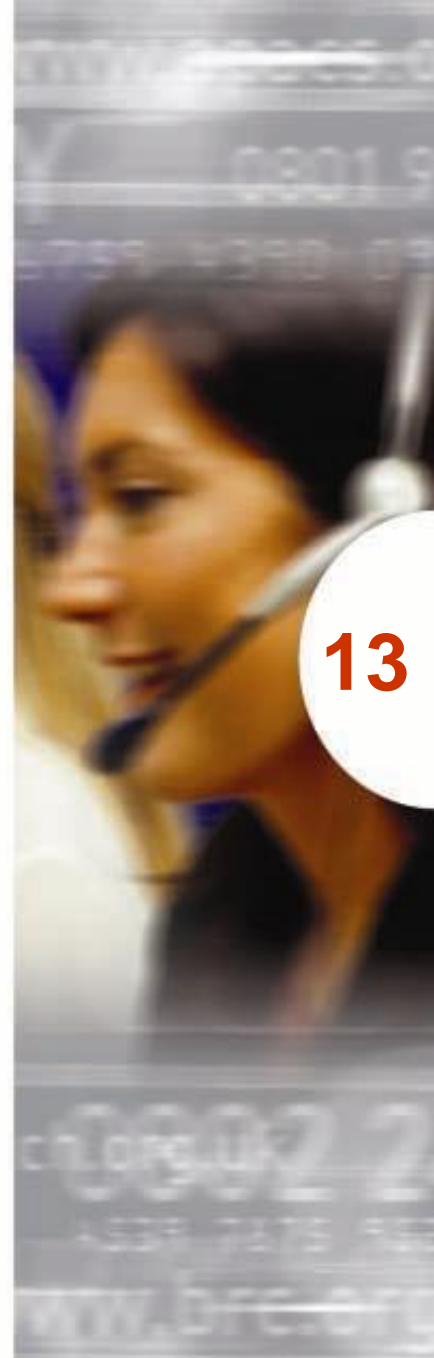
- the opportunity to make contact with the customer is limited
- tools to authenticate a customer are not as effective outside the UK
- fraudsters are using the international networks to facilitate their crime
- police are restricted in undertaking overseas enquiries



Authorisation does not guarantee payment

Authorisation only confirms two things:

- that there are sufficient funds in the account
- that the card number provided has not been reported lost or stolen



Address Verification Service (AVS) and Card Security Code (CSC)

AVS/CSC was introduced in 2001 to assist merchants combat CNP fraud. It provides merchants with additional information to decide whether to proceed.

AVS allows the merchant to check numerics in a cardholder's statement billing address with the issuer.

Card Security Code

MasterCard, Visa or Switch: 531

American Express: 7555

Cardholder's statement address

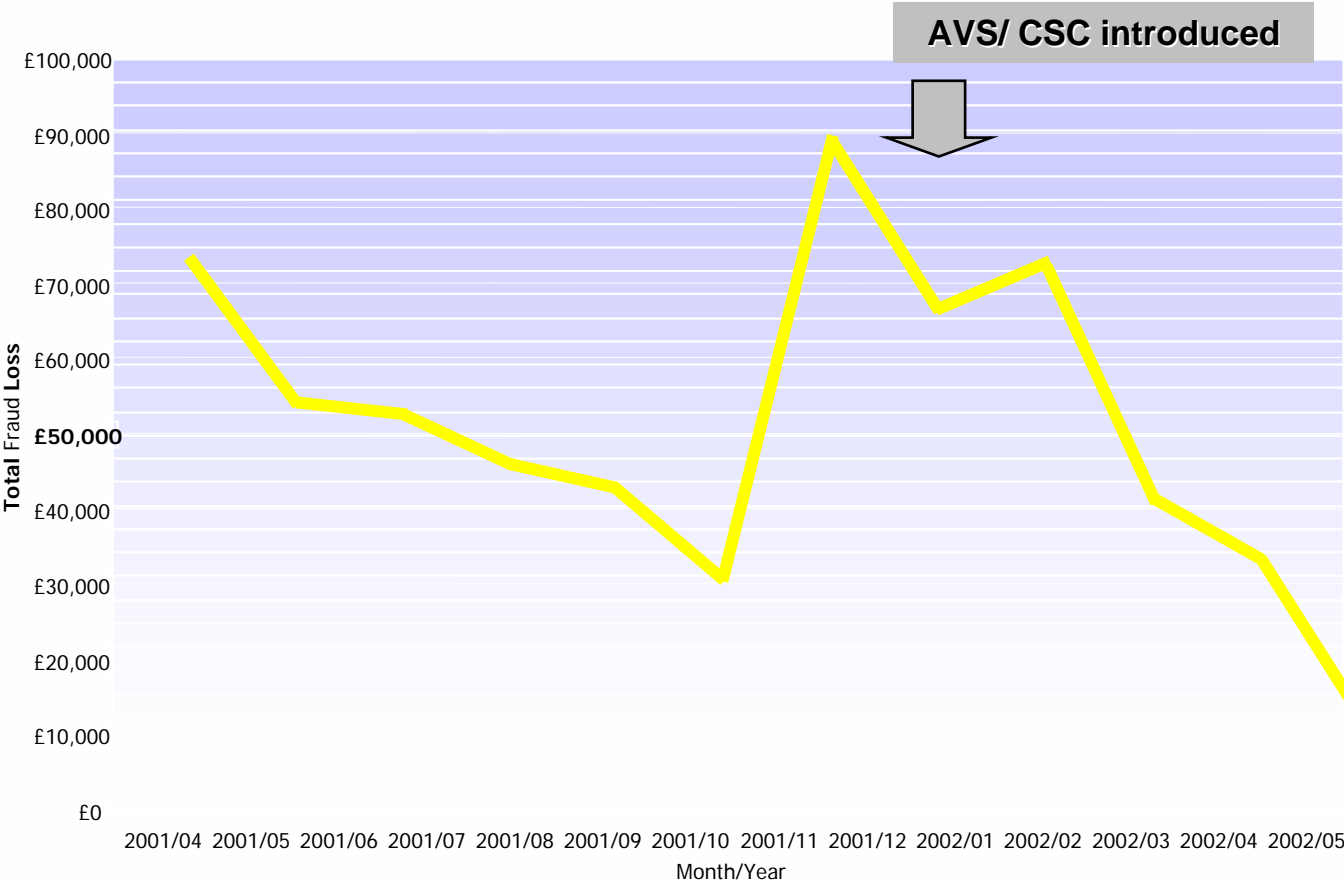
15 The Street
Any Town
Any Country
WR19 3NS

Details to be entered into your terminal

MasterCard, Visa or Switch: 531 193 15
Card Security Code Postcode House number

American Express: 7555 193 15
Card Security Code Postcode House number

AVS/CSC does work!!

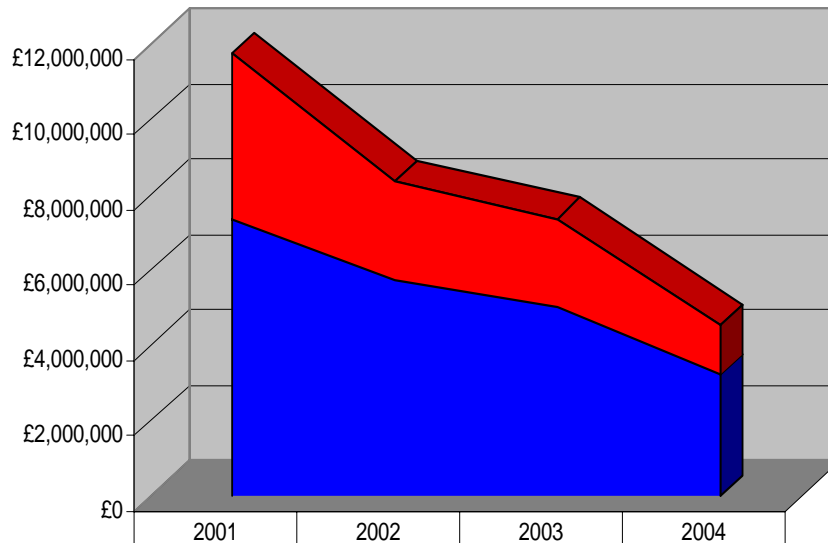


AVS/ CSC introduced

15

*Source : Barclaycard

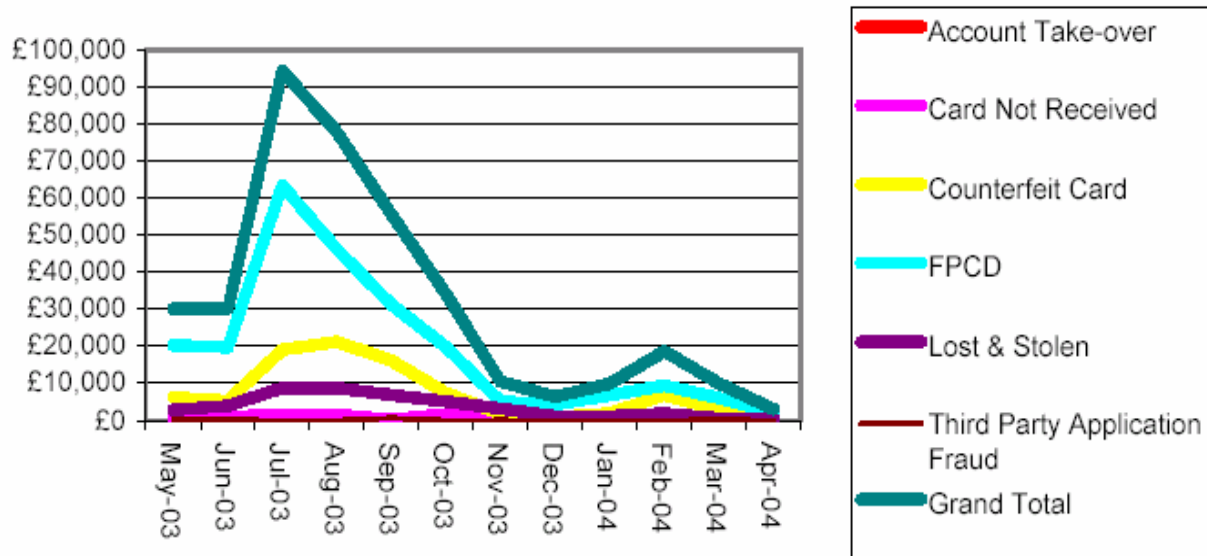
CNP Fraud in the Telco Sector



	2001	2002	2003	2004
■ Telecommunication Service	£4,425,615	£2,589,376	£2,328,312	£1,270,082
■ Telecommunication Equipment	£7,354,859	£5,745,625	£5,043,517	£3,242,912

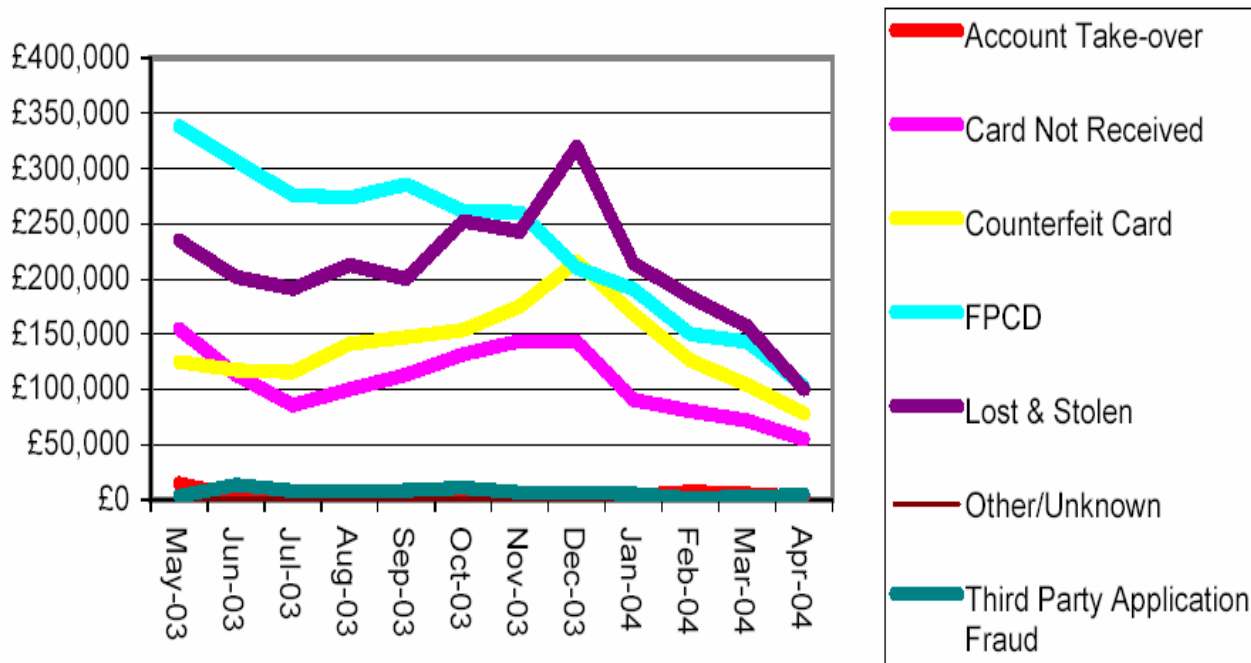
NB:2004 figures to July

Recent successes – leading UK CNP Rail Ticket Operator



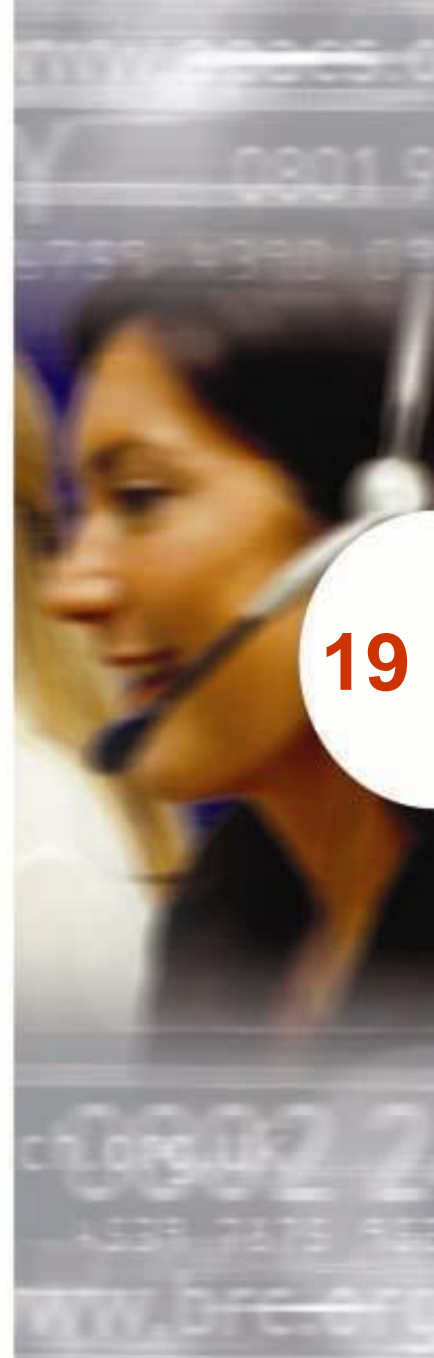
17

Recent successes – leading UK CNP General Retail Merchant



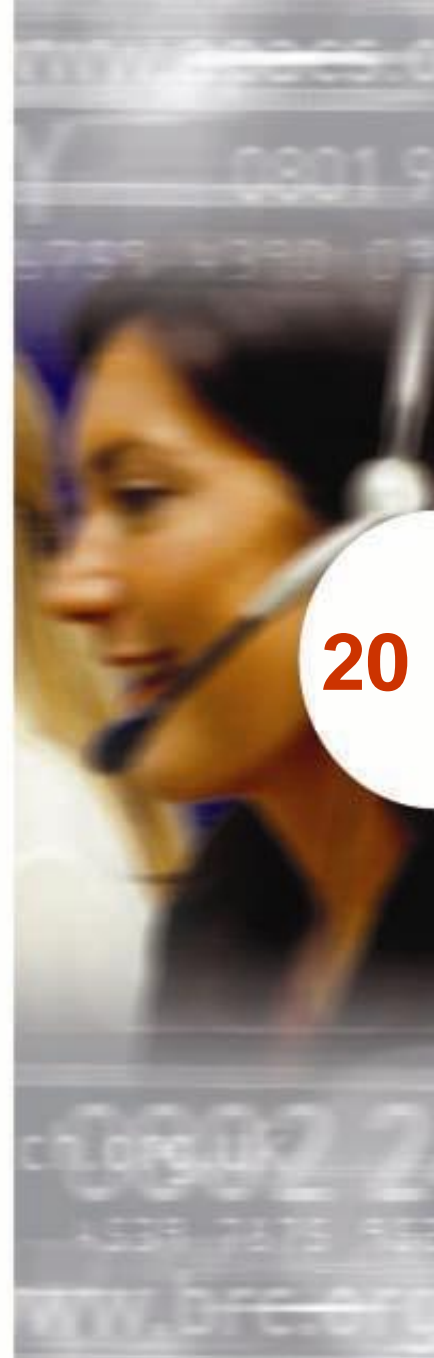
On-line authentication

- Internet payments made secure by creating a 'trust chain' with relevant parties
- **Verified by Visa** and **MasterCard SecureCode** provides stronger customer identification for Internet payments
- Use of the services result in a change to merchant liability:
 - **Visa** – liability shift on global transactions if merchant and acquirer enrolled
 - **MasterCard** – liability shift on EU transactions if merchant and acquirer enrolled
- Liability applies as soon as Merchant deployed and transaction authentication attempted



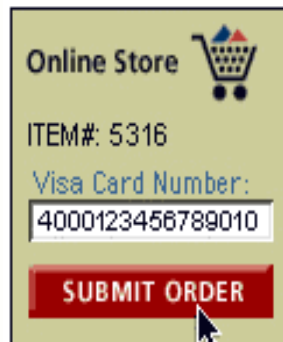
On-line authentication : how it works


- Acquirers need to be able to offer the service to merchants
- Cardholders need to register to join the scheme
- Issuers can invoke registration or can be merchant driven I.e. their first 3D Secure transaction
- Once user registration process commences, a username and password is set up
- Each subsequent transaction with a 3D Secure merchant, cardholder asked to authenticate
- Merchant best practice advice should be considered in respect of registration



Consumer Experience

1.



Online Store 

ITEM#: 5316

Visa Card Number:

SUBMIT ORDER

Shop at participating online stores. Enter your Visa number and submit your order.

2.



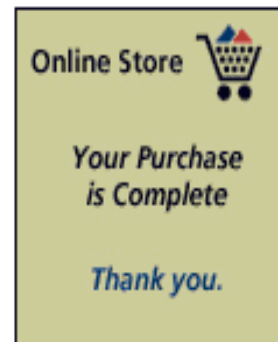
VERIFIED
by VISA


Password

SUBMIT

A window will appear. Submit your password; your identity will be confirmed, and you're done.

3.



Online Store 

Your Purchase is Complete

Thank you.

You're then returned to the online store.

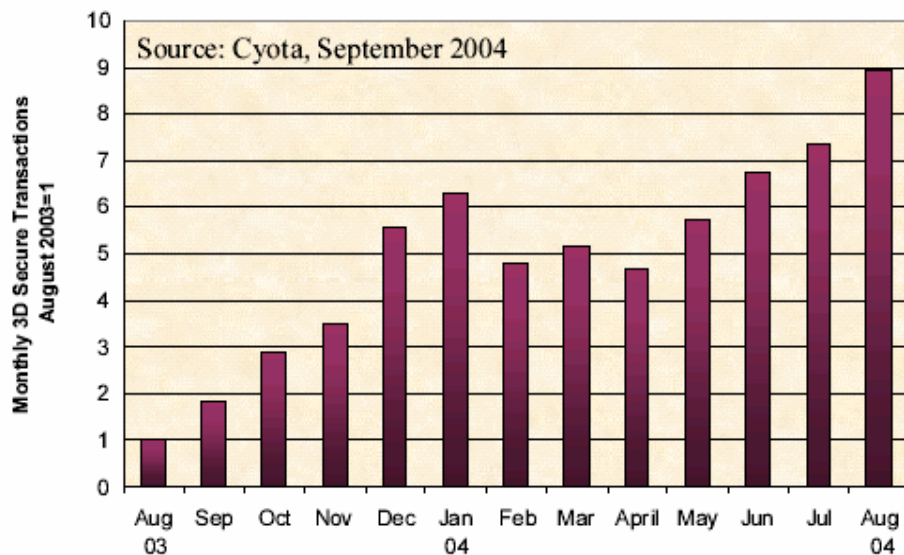
What do we know about 3D Secure?

- Issuers and Merchants are experiencing better results with 'inline' integration as opposed to 'pop-ups'
- Pop-up killers are becoming commonplace
- Design and marketing of the 3D Secure pages by the merchant instil trust to cardholder benefiting all
- Cardholder participation increases as large implementations go live I.e. Worldpay, British Airways, London Underground, Lastminute.com
- Activation During Shopping (ADS) is an ideal way to increase cardholder participation – 56% registration level with UK issuers

Cardholder Registration

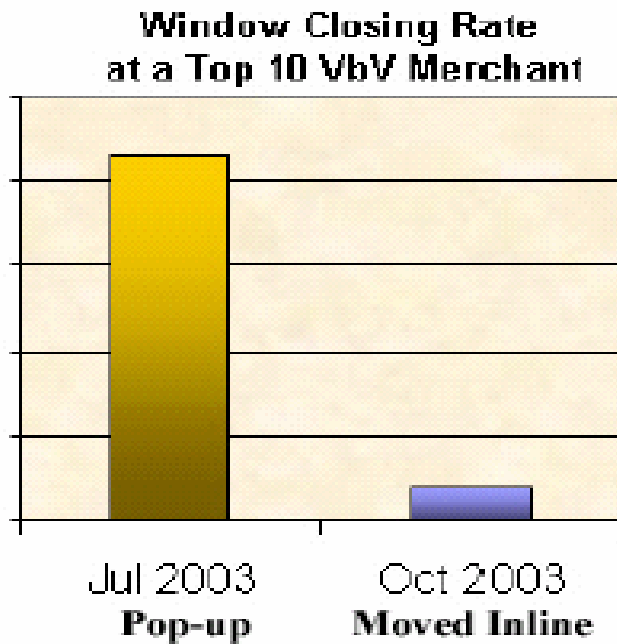
3D Secure Merchant Adoption

As reflected by monthly transactions at Top 5 UK issuer



Merchant adoption level is constantly increasing

Window Closing : Inline v Pop-Up



24



Making Chip and PIN work for GNP

Delivery made



User Places order



User inputs Chip card into handheld reader

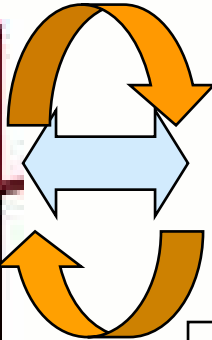
Enters PIN number

PIN Accepted and 'Signature' generated

Purchase completed with 'Signature' input on merchant site



Registration Details, Card No. Expiry, Delivery Details etc + "One Time Signature" request



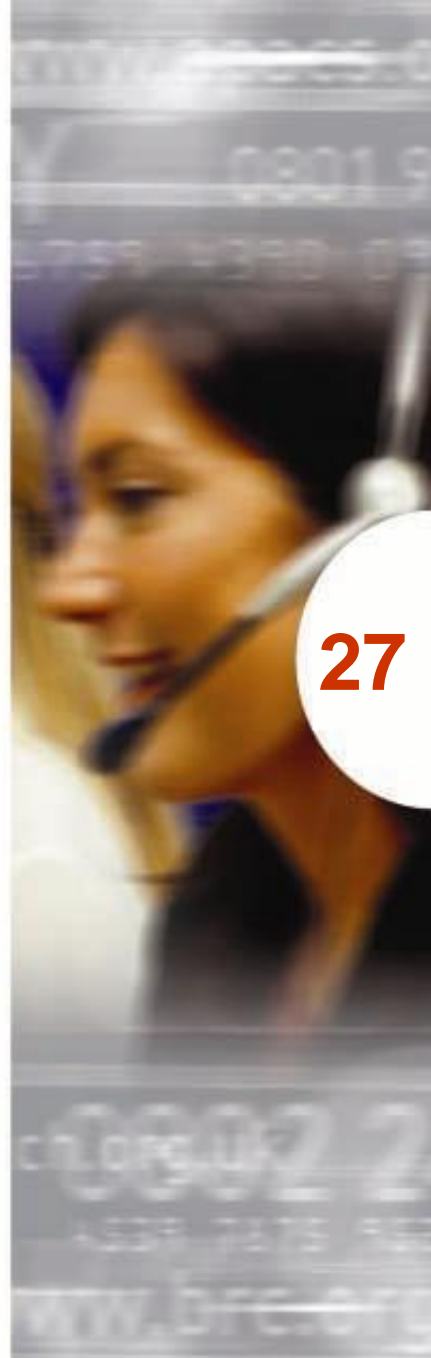
'Signature' confirmed with bank



APACS CNP Project – Next Steps

- Facilitate Token Based Access discussion as long term solution for CNP
- TBA alleviates vulnerability from static data and leverages of Chip/PIN investment
- CNP training programme availability
- Interactive training facility for use within merchant and banking environments
- Enabling AVS/CSC and 3D Secure solutions to penetrate the market
- Working ACPO to provide a minimal set of standards for law enforcement officers in dealing with CNP fraud:
 - Police Minimal Standards document
 - Fraud reporting proforma

Fighting the “Enemy Within”

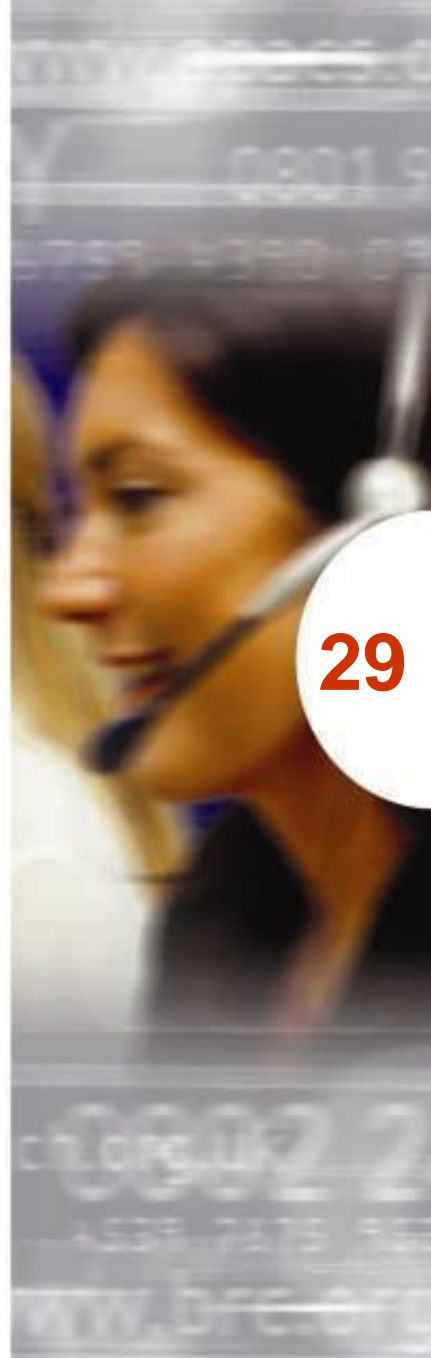


Internal Fraud in the banking sector

The banking industry is susceptible to infiltration from collusive staff. Key vulnerabilities exist with the access and availability of sensitive customer data. Industry strategy to focus on:

- Development of Best Practice Guidelines to assist the industry in dealing with such threats, to include:
 - Whistleblowing policies
 - Monitoring solutions
 - Policy and procedures review
 - Access rights and system controls
 - Procedures for dealing with offenders
 - Training programme to work with the IFeP *more later*

Combating Identity Fraud



29

Identity Theft themes in the UK

Identity Theft is the fastest growing financial crime in the UK. The government believe it cost the public and private sector £1.3bn a year.

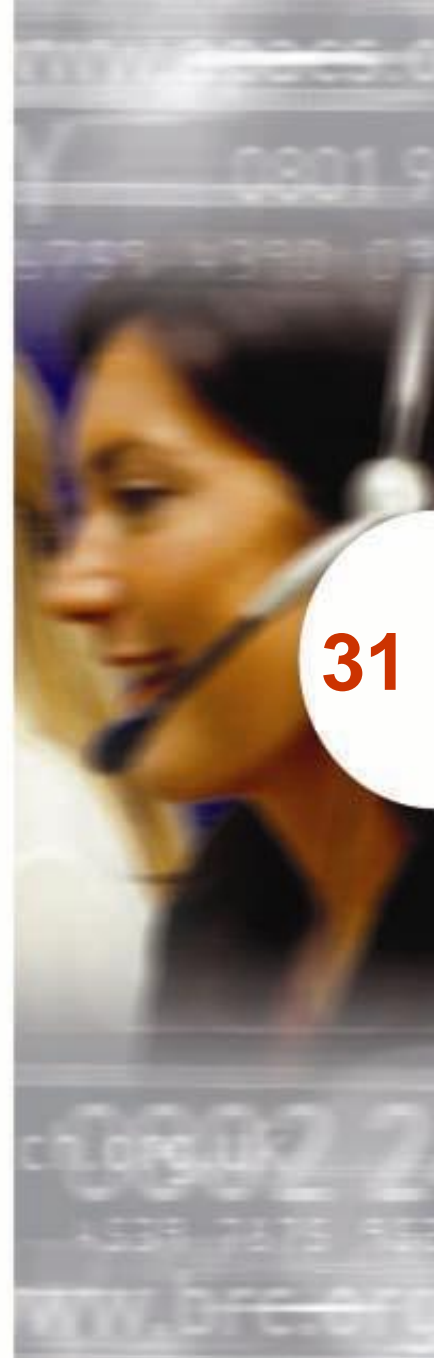
- APACS recorded £30m Identity Theft losses in 2003, 45% increase on the previous year
- Losses equally split between Application Fraud and Account Takeover Fraud
- Awareness has increased in the media, through high profile examples e.g. Home Secretary's identity compromised by BBC journalist Paul Kenyon
- Financial organisations in the UK use a combination of predictive solutions, credit bureaus and scorecards
- Data sharing is done through organisations such as National Hunter and CIFAS, however longer term data sharing between public and private sector is critical



APACS Identity Fraud Initiatives

APACS has continued to be the focal point for Identity Fraud mitigation in the UK. Since March 2002, activity has included:

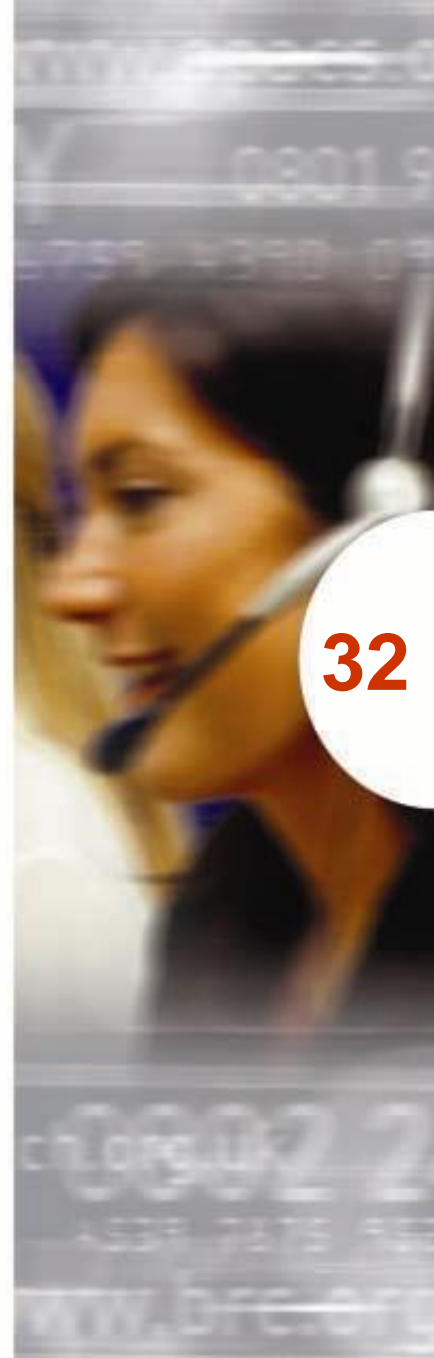
- Coordinating a Multi-Sector Working Party to tackle ID fraud involving the production “Identity Fraud the UK Manual”
- Engaged with BBA and CIFAS in the development of the Identity Fraud eLearning Project (IFeP) which will provide:
 - Organisations an interactive training programme covering all elements from the manual
 - A testing and competency functionality
 - Management to monitor progress and knowledge of employees
 - Resources for checking security features of documents globally through Keesings
 - Passport Verification through UKPS



APACS Identity Fraud Initiatives

Cont...

- Key stakeholder in Home Office Identity Fraud Steering Committee
- Project management of Identity Theft consumer support centre.
- Engaging with government agencies to examine the longer term benefits from:
 - Passport Verification Service
 - Driver Vehicle Verification
 - Identity Cards benefits realisation
- Sharing data through Account Takeover Working Group, already demonstrated links between frauds in other sector such as telcos and travel currency





Identity Theft *How to protect yourself and what to do if you think you are a victim*

Protecting Yourself

What if it happens to you?

Who can help?

What is being done?

Identity theft occurs when your personal information is used by someone else without your knowledge. It may support criminal activity, which could involve fraud, deception, or obtaining benefits and services in your name.

It is estimated that more than 100,000 people are affected by identity theft in the UK per year, costing the British economy over £1.3billion annually.

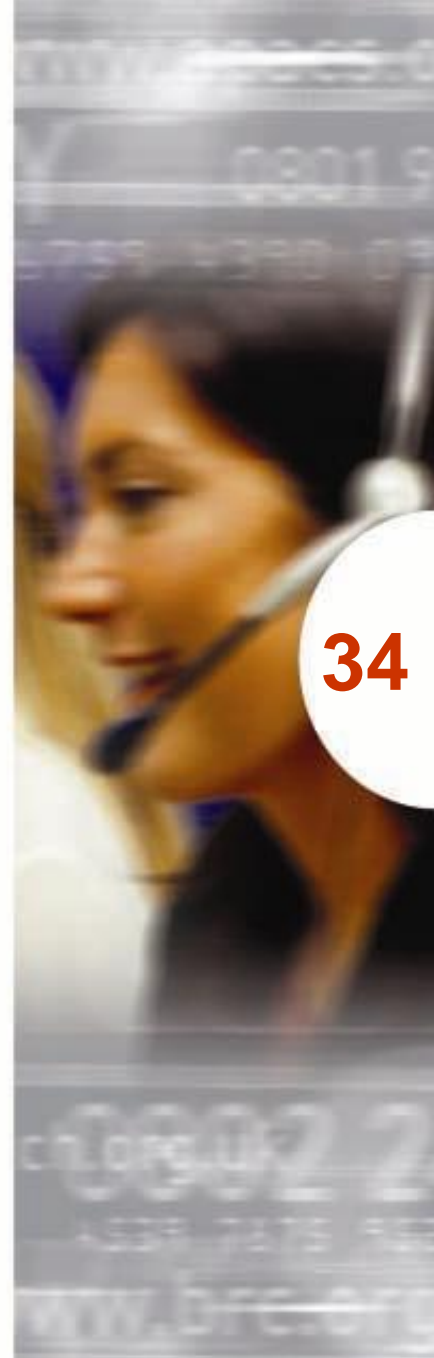
This web site has been produced by the [Home Office Identity Fraud Steering Committee](#) which is a collaboration between UK Financial bodies, Government and the police to combat the threat of identity theft.

This site can help you protect yourself, advise you what to do if it happens to you and suggest ways of getting further help.

So what do we do about Phishing?

APACS developed the eBanking Fraud Liaison Group to :

- Provide appropriate consumer messages and develop awareness
- Co-ordinate and collate information and intelligence and attacks
- Share information with members to understand typologies and trends
- Establish technical details with a view to location origins of 'spoof site'
- Move to shut the website down if appropriate
- Engage in international liaison particularly Australia



Final Note

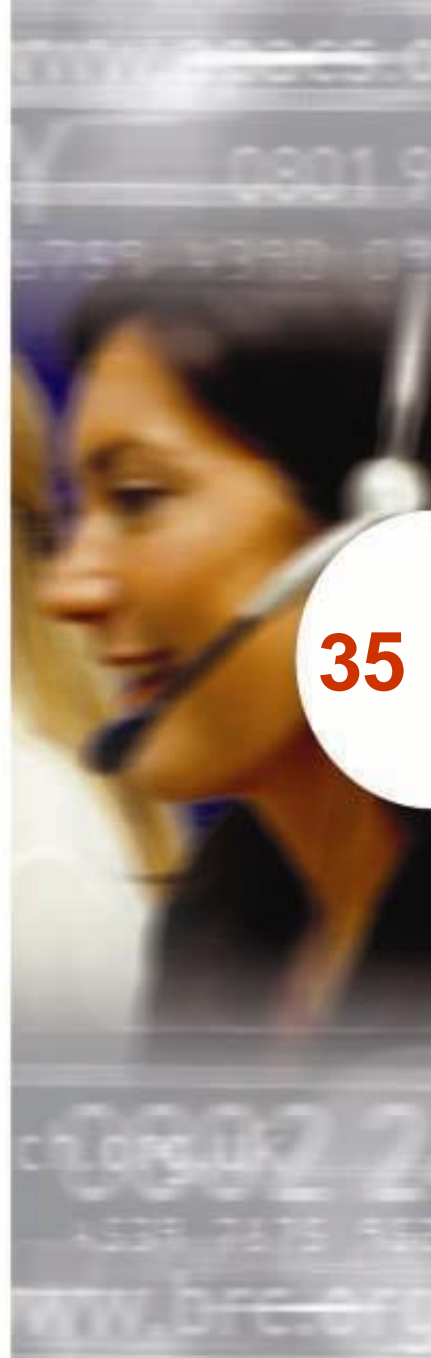
Fighting fraud in the information age, requires a number of strategies.

These should involve:

- Raising awareness and education within the business and of consumers
- Use of internal/external fraud prevention solutions
- Learning from experiences
- Working in partnership

For more information contact:

- Riten Gohil riten.gohil@apacs.org.uk
- 0207 711 6256



Fraud 'a victimless crime'?

Low Graphics version | Change edition

About BBC News | Feedback | Help

BBC NEWS WORLD EDITION

WATCH/LISTEN TO BBC NEWS

News Front Page Last Updated: Wednesday, 5 May, 2004, 14:38 GMT 15:38 UK

E-mail this to a friend Printable version

Police arrest 12 for 'phishing'

Twelve people have been arrested for allegedly laundering money stolen from bank accounts through so-called "phishing" scams.



Six men and six women from Estonia, Latvia, Lithuania, Russia and the Ukraine are suspected of transferring the money on behalf of a Russian gang.

"Phishers" are usually based abroad and need accomplices in the UK

Computers, passports, chequebooks, bank cards and crack cocaine were seized during raids mainly in London.

Have Your Say
In Pictures
Week at a Glance
Country Profiles
In Depth
Programmes

SPORT
WEATHER
ON THE STAY

36

Questions

- Riten Gohil : riten.gohil@apacs.org.uk
- 0207 711 6256

