



WORKING PARTY PAPERS

**Guidance on Protecting Your Organisation's Business
When Using the Internet**

**John MacGowan
Advisory Forum for Retail Credit Card Transactions
(AFRECT)**

Guidance on how to protect your organisation's business when using the Internet

◆ Payment Cards

Most, medium sum, E-Commerce payments, whether business to business (b2b) or business to consumer (b2c) have evolved from the use of a credit or debit card as the payment instrument.

Within the UK **credit cards** are issued under the Consumer Credit Act 1975, which affords certain safeguards to the cardholder. For instance if the cardholder uses the credit card to pay for a holiday which subsequently turns out to be a disaster – but the tour company refuses to acknowledge the claim - under Section 75 of the CCA, the cardholder can seek redress from the card issuer. The amount involved must be between £100 and £30,000.

Conversely, a **debit card** is effectively an “electronic cheque” and subject to the normal contractual arrangements between banker and customer.

◆ Card Not Present (CNP) Transactions

In the most simplistic terms, a CNP transaction is one where neither the credit card nor the cardholder is physically present, as typified in mail order / telephone order and internet transactions. In consequence, the retailer doesn't see the card itself, nor the actual card number nor the signature [strip] for comparison.

Retailers require the prior agreement of their Merchant Acquirer to accept CNP transactions and a special clause(s) in the Merchant Service Contract (MSC), which the retailer must sign, allows for any CNP transaction which is fraudulent or subject to query [by the cardholder] to be **charged –back** to that retailer.

As CNP fraud - in the UK alone - exceeded £300 million last year, the risks are obvious and Merchant Acquirer's charge retailers a higher commission rate on CNP transactions. Indeed, if a retailer has no trading history or an adverse history and is refused CNP processing facilities by a mainstream acquirer, the rates levied by a Payment Services Provider (PSP), being even higher, may be more than the profit margin on the goods themselves.

Care and a diligent mind are essential when negotiating with some, so called, Independent Sales Organisations (ISO) by those 'desperate' to secure CNP processing facilities as undisclosed fee structures, implausible rules and strict definitions on what constitutes a non-qualifying [CNP] transaction (by which processing is refused) can result in binding, yet unworkable, agreements that could destroy a business.

◆ Transaction “Authorisations”

Putting it bluntly, obtaining an 'authorisation' for a CNP transaction is worth “diddly squat” (precisely nothing). The CNP clause in the MSC provides the right to charge-back regardless and an 'authorisation' simply checks that the card number is numerically correct, the card is in issue and the card account balance is sufficient to meet the amount of the transaction.

Notwithstanding the realities, 'authorisations' are only required when the transaction sum exceeds an imposed floor limit. However, imposition of a zero floor limit will involve the retailer in additional costs !

◆ **Security / Transaction Screening**

Having briefly outlined the risks, what can best be done to alleviate them ? It is a harsh, but salient, fact that 9 out of 10 (e-)criminals get away unpunished; in 40% of cases they will steal several times from the same site (a schizoid idea of loyalty !)

From the retailer's perspective, consider Security and Transaction Screening.

a) Security

There are various software / security vendors whose products can make a website "secure". But where is this security effective, in most cases at the **front end** (the web page) but transaction data (card, address) does not remain on the screen. It is ultimately stored on a **back end** server usually unprotected and in clear text. There have been enough embarrassing cases of late. Ensure that what you want is what you actually get.

b) Transaction Screening

Transactions being screened for frequency of card usage, consecutive purchases of similar merchandise, whether the card number has been reported lost/stolen, adverse charge-back history, irregular cardholder activity is effective - **but it must be completed PRIOR to the transaction being processed.**

The majority of [neural] transaction analysis software packages are examining data post the event. Install one that works whilst the horse is in the stable - not after its bolted, and has to be caught if that's still possible.

◆ **Common Scams**

a) "Pirating"

Copying content and setting up multiple sites more or less identical to the original, with each site trying to get first place with the search engines. Some of the false sites will incorporate a few of their own [the pirates] banners onto the 'copied' content to attract sales.

b) "Bandwidth" linking

Pirates link themselves to files on your server, so that when someone looks at the 'pirate' page it is your server that hands out the files. Slows response times and increases ISP/webhost charges.

c) "Bait and search"

Redirects traffic to another site.

A legitimate web page that contains common words (i.e. hotels, financial, everyday product names) is COPIED completely including graphics and text. These pages are then hosted on a computer / server run by the perpetrator.

When a search engine runs across the [new] pirated page, it does not know that page is hijacked and automatically inputs the URL ('www ' address) into its database with the keywords. Subsequently, when someone browsing enters a keyword search, **into the search engine**, the duplicate site will appear amongst the results along with the legitimate web page.

Five items of concern, on the Internet, and how to counter them ?

1. Application Service Providers (ASP)

A recent exercise matching our data security requirements against competitive ASP offerings was illuminating.

We found :

- Sloppy network management - with simple passwords replacing more stringent dual authorisation procedures.
- Slipshod lip service to intrusion detection systems, which permitted weak applications to accept miscellaneous input data.
- Credit card data is (invariably) commonly stored on the websites in transaction log files in **PLAIN TEXT**, thereby readable by anyone who has gained access.

Consequently, advice on best practice is :

- protect sensitive information by installing firewalls,
- keep payment card details confidential,
- protect card processing systems and the servers which hold this data.

2. TRANSACTION PROTECTION

Achievable to (virtually) any level required by the use of cryptography allied to public key technology. The key is the 'key length' - no pun intended.

Interested parties in exploiting e-commerce which includes major global companies/retailers (Visa and Mastercard), Government / industry bodies, the EC, software and telecommunication suppliers have contributed to the establishment of proprietary software based on policies, accepted practices, (quasi) standards, legislation and informal agreements, which have centred on the protocols now referred to as :

PUBLIC KEY INFRASTRUCTURE (PKI)

PKI Components

- **PRIVATE and PUBLIC KEYS**
- **DIGITAL SIGNATURES**
- **DIGITAL CERTIFICATES**
- **CERTIFICATION AUTHORITIES**

Encryption techniques

Although Single Socket Layer (SSL) is widely used (requires less technology, quicker, cheaper), and has been accepted as providing a modicum of protection for e-commerce transactions, its effectiveness is a cause for concern as a short length key is easily broken and transactions compromised. Furthermore **SSL DOES NOT** protect the data once its on the back end server at the other end **AND IT IS FROM HERE** that most credit card numbers have been hacked.

End to end encryption is necessary for security and effective b2b trading has to include a transaction audit trail which SSL cannot provide.

Jointly developed by the banks/ card schemes is the technology termed "SECURE ELECTRONIC TRANSACTIONS" (SET), which is intended to be adopted as the standard for **ALL** credit card payments over the Internet.

Complimentary to PKI, SET prevents retailers from seeing the customer's credit card number as it is passed in encrypted form to the Merchant Acquirer. SET also provides software to collect, exchange and verify digital certificates.

Currently SET is not exactly 'user friendly' to operate or administer. Although development, variations are progressing, widespread adoption and use could Undermine the Banks' current right to CHARGE-BACK transactions.

Introduce C-SET

3. FRAUD

At this point, let us examine the fraud issues generally associated with the INTERNET.

**Point 1 : The Internet is responsible for 1% of VISA (branded)
Credit Card sales in the EU.
AND
47% of the Charge-backs.**

Point 2 : Global internet fraud is reliably estimated to be running at OVER £10 billion a year.

Point 3 : Common FRAUD types

- a) 'lifting credit card numbers' (by accessing databases).**
- b) fake shopping pages (routing transactions back to fraudster).**

In mainland Europe any e-retailer can ask a customer (cardholder) to input a card number and PIN. That opens the door to fraudulent opportunities; for example, a bogus internet merchant can use this information to withdraw cash from the cardholder's account (credit or bank account) through the ATM network.

Moreover

IT security specialists have now confirmed that "secure" web server software from Microsoft, Netscape and Apache can be compromised as "private key" details can be located in the memory systems of servers and THUS permit access to data such as credit card numbers.

Solution : move keys OFF servers completely, hold on a separate system.

4. FRAUD PREVENTION and DETECTION SYSTEMS

Most are based around NEURAL networks and post transaction analysis.

The usual repercussion is a telephone call to the cardholder asking if they purchased such an item(s) on a specific date, location and costing £x.

Then, the cardholder is informed that his/her card number has been compromised, CANCELLED and that a replacement card will be issued within a few days !

There had to be a better MORE RESPONSIVE way ?

So I put my thinking cap on, joined forces with some like-minded technical people, spoke nicely to my contacts (to determine what data they held) and became the architect and principal developer of an automated, real time, networked (pan-European) system for detecting and preventing fraudulent or undesirable payment card (credit, debit, smart) transactions PRIOR to the transaction being processed for use in POS, CNP and Internet environments.

We have called the product/ service FRAUDCHECKER.

5. Internet Security - useful hints :

- a) Plan for the worst, attacks are a reality.
- b) Regularly review your security policy.
- c) Ensure that any dependencies (e.g. ISP, web hosters) are part of your security assessment criteria and determine their level of protection.
- d) Do not permit any person to override any security system.
- e) Ensure that there is no single point of failure for any critical system.
- f) Test network design for resilience to security threats and neutralise any risks so discovered.
- g) Implement security at the network level.
- h) Consider need for security within the LAN also, secure data whilst in transit.
- i) Put a firewall in place.
- j) Establish a data encryption policy.
- k) Install intrusion detection systems.
- l) Encryption - keep keys held inside security applications, if possible split keys into multiple components.

- **E-Mails**

If companies do NOT monitor content going in and out through their e-mail servers, it is quite easy for employees to misuse the facility and / or to steal proprietary information.

6. Website Development

Consider :

- Ownership of Software (IPR)
- Domain names
- Limitation of Liability
- Shut down rights
- SLA

Protecting content - Linking sites
Caching sites
Copyright your work
Ownership.

Provide /disclose :

- ✓ **delivery date options**
- ✓ **price ranges**
- ✓ **all shipping / postage / delivery costs.**

7. Scams

"Pirates"

Copy your content and set up multiple sites, more or less identical to yours, each trying to get First place in the search engines. Some will incorporate a few of their own banners onto "your" content to attract sales.

Kiv : Copyright laws give some protection.

Bandwidth

Pirates link to files on your server. When someone looks at the 'pirate' page, your server hands out the files. Slows response times and increases ISP/ webhost charges.

Bait and Search

Redirection of traffic to another site.

A legitimate web page that contains common words (i.e. 'maps', hotels, Financial) is COPIED completely including graphics and text. Those pages are then hosted on a computer/ server run by the pirate.

When a search engine runs across the [new] pirated page, it doesn't know that page is hijacked and automatically inputs the URL into its database along with the keywords.

When someone enters a keyword search INTO THE ENGINE the duplicate site will appear amongst the results along with the LEGITIMATE web page.

FILE Lifting

Copying of files and then hosting them on pirate's own site.
Also META TAG copying.

(META TAGS are HTML tags that help provide descriptions on pages that lack text, and provide a useful way to control your summary in search engines).

8. Also BEWARE of :

a) Unscrupulous Independent Sales Organisations (ISO)

Who prey on those e-retailers DESPARATE to arrange for credit card acceptance on their sites. CNP and no history attracts higher commission rates from credible acquirers.

The enticements used are :

- Fraudulent sales pitches
- High pressure tactics
- Ultra low commission rates, arbitrarily raised after contract.
- Undisclosed fee structures

These ISOs invariably have implausible rules and strict definitions on what will constitutes a non-qualifying transaction (refusal by them to process).

b) Hacker Tools

Password Crackers (War Diallers).

Once the attacker has detected an open modem and cracked some passwords, they will then install back office routines to let them back in later. Prime example is software named "Back Orifice (BO)".

ROOT EXPLOITS - allows an attacker with a user-level account on a UNIX system to gain super user access.

DENIAL of SERVICE (DOS) - causes a system to crash or slow down to the point of not being usable.

REMOTE EXPLORER

An NT virus that installs itself as a service on an NT system. When an Administrator logs on, the virus automatically propagates through an NT network by using the "Admin's" privileges.

c) E-Mails

"Bombs" - 1000s of messages sent to mailbox, expending bandwidth and filling box with junk. Intense e-mail 'bombs' can result in DoS to host servers, routers and other systems that rely on TCP/IP.

"Link Listing" - subscribes an individual to dozens of mailing lists without their knowledge.

John MacGowan

Advisory Forum for Retail Credit Card Transactions (AFRECT)

Tel : 0114 258 1719

Fax : 0114 230 6419

e-mail ; afrect@dial.pipex.com