

Classification of Fraud Types

A White Paper

September 2005

PROPRIETARY NOTICE

© 2005 CubelQ Ltd. All Rights Reserved. No part of this publication may be reproduced or duplicated without the express written consent of CubelQ Ltd.

This report contains confidential information of CubelQ Ltd and her suppliers, which is provided for the sole purpose of permitting the recipient to evaluate the information submitted herein. In consideration of receipt of this document, the recipient agrees to maintain such information in confidence and not to reproduce or otherwise disclose this information to any person outside the group directly responsible for evaluation of its contents, except that there is no obligation to maintain the confidentiality of any information which was known to the recipient prior to receipt of such information from CubelQ, or becomes publicly known through no fault of recipient, or is received without obligation of confidentiality from a third party owing no obligation of confidentiality from CubelQ.

If pricing is included, all prices and conditions in this proposal are valid for the period defined in the cover page or in the corresponding pages unless extended in writing.

This proposal has been prepared in accordance with accepted techniques for system design, and CubelQ's understanding of your requirements based on the information provided to us; all timings, flow charts, system design and related information contained in this proposal reflect CubelQ's best estimates based on this information. However, operating environments (including, among other aspects, speeds, personnel, and costs) may vary from those indicated in the proposal due to variations in volume, environment, personnel, software, programs and other factors and, thus, CubelQ cannot warrant the accuracy of such estimates.

Brand or product names mentioned herein are trademarks or registered trademarks of their respective holders.

Abstract

Combating payment fraud

Classification of types of fraud and criminal offences

Financial institutions worldwide have suffered losses of more than a \$2 billion during 2000, \$2.2 billion during 2001 and \$3.8 billion during 2002, attributed to credit card and debit card fraud.

Fraudulent card activity takes place within a very short time frame: over 50% of the losses are incurred on the first day, while additional 30% of fraudulent acts occur in the following 2-3 days.

In order to mitigate losses caused by debit but mainly credit card fraud, financial institutions recognize the need to improve their fraud detection and prevention systems. For improving fraud detection and prevention systems, identification and classification of fraud types and related criminal offences should be addressed.

Contents

TYPES OF FRAUD AND CRIMINAL OFFENCES	5
THEFT AND USE OF THE CARD	5
"THAI" FRAUD	5
REMOTE RECHARGING OF TELEPHONE CARDS	5
PURCHASE BY CORRESPONDENCE	6
FALSE FRONT ON CARD TERMINAL	6
PIRATING OF POINT-OF-SALE TERMINALS (POS)	6
FALSIFICATION OF STOLEN CARDS	7
COUNTERFEITING	7
BREACHING SECURITY FEATURES OF SMART CARDS	7
DISSEMINATION OF INFORMATION OR DATA LIABLE TO COMPROMISE THE SECURITY OF MEANS OF PAYMENT ..	7
OUR OFFERING	9

Types Of Fraud And Criminal Offences

Theft and use of the card

1st act: Theft

- Simple theft (pick' pocketing, interception of mail, etc.).
- Theft with violence ¹ of a card and sometimes the PIN code.
- Theft by trickery of a card and sometimes the code.

2nd act: Use of the card

- Simple use either in an ATM or for purchases from traders.
 - Cards are in the name of the holder and non-transferable.
 - The charge of fraud by use of a false name may be brought.
- **Third party beneficiary:** A charge may be brought against a third person not participating to the theft for remittance of funds obtained indirectly, if there is complicity on the part of the trader.

¹ Torture and acts of barbarism are increasingly frequent, sometimes preceded by abduction and forcible detention of persons.

"Thai" Fraud

- As a trader, be in possession of a manual credit card imprinter.
- When recording receipt of a customer payment by bankcard, take an imprint of the card (card number, name of holder, validity date, i.e. the embossed areas), and then imprint a different charge slip to effect the actual transaction.
- Keep a copy of the cardholder's signature.
- The first charge slip imprinted does not include the trader's particulars.
- The first charge slip is passed to another trader, in league with the first, who adds his own particulars and makes a fictitious transaction.

Remote Recharging Of Telephone Cards

- Recovery of a charge slip bearing the required 16 figures (certain ATMs, shops and businesses).
- Use of this number to top up a prepaid card from a mobile phone company.

Purchase By Correspondence

Correspondence: Telephone, FAX or the Internet

- Recovery of a payment card number:
 - Either from a charge slip or
 - By using number crunching software to generate a number
 - Real or fictitious validity date (use or creation of a date)
- Use of this number:
 - For a transaction by correspondence (telephone, fax) or
 - On the Internet.
- Use of a false name and address for delivery of goods.

False Front On Card Terminal

*** SMART FRAUD ***

- Producing software or electronic devices for capturing and recording bank card data
- Installation of false fronts and systems for capturing magnetic strips and secret codes.
- Capturing and recording data.
- Possession of media on which data have been recorded.
- Possession of devices used to capture data.
- Encoding numbers on blank cards.
- Purchase and possession of blanks for re-encoding.
- Possession of encoded cards.
- Possession of encoding software.
- Using encoded cards in automatic teller machines in E.U.

Pirating Of Point-Of-Sale Terminals (POS)

*** SMART FRAUD ***

- Design and production of software for intercepting magnetic data and confidential codes.
- Installation of microprocessors and memory in POS.
- Fitting duplicate POS magnetic strip readers and PIN pads.
- Installation of POS in traders' premises (with or without complicity).
- Capture of data during transactions; recording and transmission of such data.
- Possession of pirated data:
 - On listing paper, or
 - In computer memory.
- Encoding blank cards.
- Using cards in ATMs.

Falsification of Stolen Cards

*** SMART FRAUD ***

- Acquisition of cards: See section "Theft and use of the card"
- Possession of devices for flattening, embossing and encoding
- Possession of stolen cards
- Falsification, use and acceptance of falsified cards (acceptance must be intentional to be a chargeable offence).

Counterfeiting

Capture of magnetic data

- Modus operandi described above as regards both traders and distributors ¹.

Skimming

- Construction of devices for reading and recording magnetic data.
- Possession of such devices prior to the commission of the offence.
- Capture of magnetic data

Card counterfeiting

- Manufacture of blank cards, reproduction of security features.
- Encoding and embossing counterfeit cards.
- Use and voluntary acceptance of re-encoded counterfeit cards.
- Possession of material that has been used for counterfeiting and forging.
- Possession of counterfeit cards

<p>¹ Skimming applies essentially to data on the magnetic strip that can be used for purchases from all traders in foreign countries and by foreign cardholders in France.</p>

Breaching Security Features of Smart Cards

- Analysis of the electronic signals between the chip and the payment terminal.
- Cloning of chips and use of clones.

Dissemination of Information or Data Liable to Compromise the Security of Means of Payment

- Supplying or being in possession of means of generating numbers (number crunching software, etc.).
- Dissemination and supply of confidential information on the security features of means of payment.
- Supply and dissemination of methods of fraud.

- Sale, purchase or transmission of such material or data.
- Production and development of such material or generation of false data and supply thereof without any subsequent offence/fraud.

Our Offering

CubelQ is an IT company specialized in Business Process Re-engineering focused in the Banking and Electronic Transaction Processing Market. Our leading-edge software solutions can transform business processes in a more efficient, more productive and cost saving way.

Main **CubelQ** activity is in providing IT solutions to vertical markets one of which is the Banking and Financial market. **CubelQ**, in co-operation with leading banking systems vendors, is in the position to provide end-to-end systems and professional services to her customers. The company maintains strong links with various banking systems companies. These relationships enable us when deemed necessary to work jointly with our foreign partners or to use their specialists and expertise on particular projects in order to offer our clients coverage of the highest professional standard.