COMMIDEA

EFT-POS, 7 Eastham Street, LANCASTER. LA1 3AY
Tel: 01524 380881 Fax: 0870 168 1899
www.eft-pos.com
email: sales@eft-pos.com

PLEASE NOTE THIS IS A BETA DOCUMENT
WORK IN PROGRESS !

CARD FRAUD

FACING FACTS & THE FUTURE

1 Introduction

1.1 Scope

This document is intended to highlight the current issues facing card not present (CNP) retailers with regards to credit and debit card fraud in the U.K. today. This document also examines the likely results of inaction by retailers in the wake of card industry developments to tackle card fraud in other market sectors, and seeks to present Commidea's fraud prevention services as the key weapon in the armoury of retailers facing up to the facts of card fraud.

1.2 Our Philosophy on Card Fraud

1.2.1 Understand The Issue

Card fraud is an enemy of all forms of retail business - full stop. But for cardholder not present retailers or "distance selling organisations" its implications are more costly than for most. The liability for card fraud in your environment rests with you, 100%, no argument.

It is theft; theft of your goods, theft of your income and theft of your time. It is both a loss to and a cost to your business and it needs to be fought against. To fight this enemy we must first learn to understand it and to do that we look at its character and the tactics it uses. We must also take a positive and proactive decision to fight it and to not simply react to its aggressions. We must also commit to a long term, possibly lifelong, strategy of monitoring and evaluating its nature and effects and to a strategy of reviewing and adapting the tools we use to prevent it.

Chapter two of this document seeks to understand card fraud in detail by examining statistics and identifying the various types of card fraud prevalent in all forms of retail. Later in this document the explanation of Commidea's Fraud Prevention Service details the leading edge technologies that can work in unison to prevent fraud now and deter it in the future.

1.2.2 Decide to Fight Back

But understanding is useless without a proactive decision to fight back and for most of us that is common sense. But have we done that or have we instead just accepted fraud as a cost of doing business - an unavoidable fact of life? Have we conned ourselves into believing we fight it by striving to increase top line turnover to achieve the real profitability we desire - despite the fraud? If so then all we are really doing is reacting to fraud by accepting its consequences. We might just as well budget for fraud as a standard administrative eaxpense. In this common scenario, the enemy wins. As you increase your turnover, so increases the fraudsters cut. Another 5% for you is another share for them and whilst this cycle continues all we do is provide encouragement to the enemy to carry the on fight.

The reality, however, is that a proactive approach to detect and prevent fraud not only increases profitability on existing turnover, but also increases profitability on future turnover gains. Detecting and preventing card fraud today discourages fraudsters from attacking us in the same way again.

"Before success in any man's life he is sure to meet with much temporary defeat and, perhaps, some failure. When defeat overtakes a man, the easiest and most logical thing to do is to quit. That is exactly what the majority of men do."
Napoleon Hill

"and what most fraudsters will do too!"

So let's face facts. We're dealing with criminals whose very nature is to take the soft option, to not work hard for a living by preying on the most vulnerable, the easy targets. A decision needs to be taken to fight back and make life hard for the fraudster. A decision that will detect, prevent and deter card fraud from your business.

1.2.3 Make A Long Term Commitment

And once the decision to fight has been taken and early success is achieved it is vital to continue fighting and not sit back. Fraud patterns and trends are ever changing, and when one avenue is blocked for fraudsters they seek others. Today's card fraud is organised and extensive. It is usually not the whims of "work alone" criminals but the organised, co-ordinated and pre-planned actions of teams of fraudsters combining their various skills and efforts towards a common goal of stealing from you. For that reason, fraud prevention isn't simply the purchase of systems that may work today and not tomorrow, nor the introduction of simple business rules that can affect good customers as well as bad, and nor is it to close sales channels where fraud percentages appear high. Rather, it is an investment in a co-ordinated and pre-planned set of tools and strategies that are as flexible as the fraudsters and seek to block their efforts at ever changing points of attack. Fraud detection and prevention requires constant attention, regular review and speedy implementation on a long term basis.

1.2.4 Seek Assistance.

Commidea has invested significantly in the infrastructure, technology and skill sets necessary to provide retailers with these key weapons, recognising that for many retailers such independent investment is neither viable nor desirable. Our Fraud Prevention Services are therefore designed to bring you all of the benefits, advantages and gains of a sophisticated, complex, responsive and diverse fraud prevention system. Our services are designed to require as much or as little effort on your part as you desire and at a cost where return on investment is quickly realised. The detail of our Fraud Prevention Service is explained fully later in this document.

1.2.5 Consider The Future

As an industry leader of card payment processing solutions, our extensive knowledge of the entire card market leads us to another belief that is widely shared within the industry. This belief is that card not present fraud is likely to become the most significant card fraud category within three years and will grow more rapidly than any other card fraud segment, possibly doubling in value.

The reason is simple. Every other area of card fraud is being actively tackled by card schemes, issuers and acquirers leaving the CNP market as the weakest link. For example, committing card present fraud will become enormously more costly and complex with the roll out of chip cards with PIN verification replacing signature verification at the point of sale. E-commerce fraud is being tackled with the introduction of on-line payer authentication programmes such as Verified by Visa and

MasterCard's Secure Code (although these schemes require careful evaluation at this stage and are discussed in more detail later in this document). And finally, mail non-receipt fraud (where newly issued cards are intercepted by fraudsters), application fraud and lost/stolen card fraud are being tackled in a number of different ways by the industry.

The result is that card fraudsters will do what they have always done and target the softest option or more specifically concentrate their efforts on committing CNP fraud.

1.2.6 Summary

Commidea therefore believes that it is essential for card not present retailers to tackle card fraud now by taking a decision to be proactive in understanding, detection and prevention. We believe that it is also essential to commit to a long term strategy of evolvement through analysis, review and adaptation of fraud prevention tools and techniques. This in light of an existing upward trend in card not present fraud and in fair assumption that this trend will continue.

2.1 Introduction

In order to begin the fight back against fraud it is very important to understand its nature and to understand the patterns and trends of the past which may lead us to more accurate assumptions in the future. It is also necessary to identify the varieties of fraud so that we can learn to assess them in relation to our own enterprises. This chapter therefore seeks to provide statistical information and analysis on the current and historical position of card fraud in the U.K. As an overview, however, here is a statement from David Cooper, Chairman of APACS Plastic Fraud Prevention Forum :-

"At £424.6 million in 2002, plastic card fraud losses are still increasing - although not as dramatically as in previous years. Our multi-layered fraud prevention initiatives, coupled with the work of a new police card fraud unit, are starting to disrupt the illegal activities of organised criminal gangs.

However, we cannot afford to be complacent in the fight against plastic card criminals and the implementation of a chip card and personal identification number (PIN) system in the UK will lead to a significant reduction in predicted levels of counterfeit and lost and stolen card fraud. Indeed, if Chip and PIN was not introduced it is estimated that total card fraud losses on UK-issued cards would be in the region of £1 billion by the end of the decade.

Banks, retailers, police and the Home Office also continue their partnership approach to tackle card fraud by utilising a number of short to medium-term prevention initiatives. A notable example of this is the two year pilot of a dedicated police unit that has been set up to tackle the organised criminal gangs behind the rise in card fraud in the UK. These initiatives are successfully complementing the longer term benefits that we will gain from the introduction of Chip and PIN." Source: Card Fraud The Facts 2003

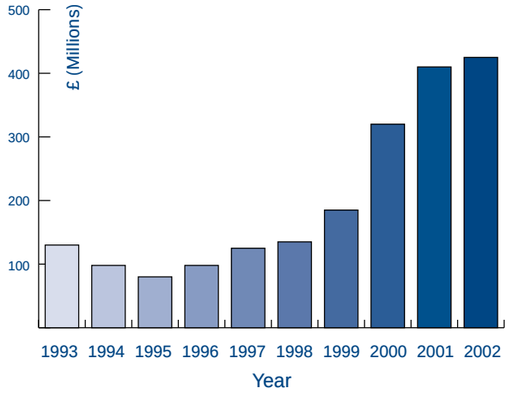
Whilst this statement is good news in general terms, it represents a worry for the card not present retailer in confirming that fraud in general continues to rise and that CNP fraud remains ineffectively addressed by the industry leading to a likely fraud migration from card present to card not present environments.

2.2 General Statistics

Card fraud in the U.K. rose last year to a staggering £424.6 million, a rise of £13.1 million on the 2001 figures. Whilst the rise in fraud from 2001 to 2002 was far less than the previous year's increase of £94.5 million, it continues a trend started back in 1995 of year on year card fraud increases. In the few years prior to 1995 fraud was decreasing steadily. This was the result of the roll out of on-line authorisation and integrated on-line authorisation systems such as Commidea's Soft-EFT and WinTI. As usual however, fraudsters adjusted their own strategies and found ways around each new initiative that the industry introduced to combat fraud, and an upward trend was started

In the same way as on-line authorisation decreased overall fraud steadily for a number of years, the smaller increase in fraud during 2002 is largely a reflection of the number and scale of initiatives undertaken by the industry to stop fraud losses from running out of control. These include the introduction of address and card security checking systems, the creation of a police unit tasked with dismantling organised crime gangs, retailer education programmes and the enhancement of bank security systems aimed at detecting unusual spending habits - to name but a few.

Overall Fraud Losses

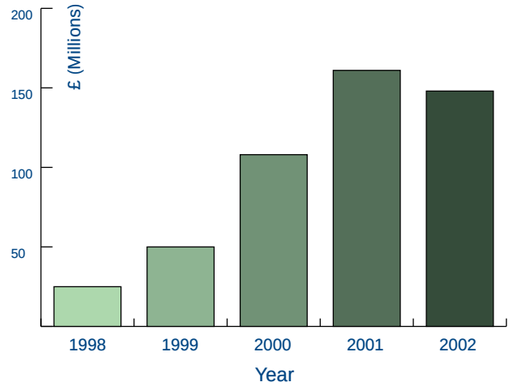


The Chip and PIN programme is likely to have an even greater effect on overall fraud by reversing the current trend of increasing overall fraud levels in the same way as on-line authorisation did in the early 90s. But having witnessed the doggedness of fraudsters to "find new ways", let's expect a migration of fraud to the one area left largely unprotected by the industry - card not present fraud.

2.3 Types of Card Fraud

U.K. card fraud is split into five broad categories. In 2002 the total value of fraudulent transactions committed on U.K. issued cards was £424.6 million, an increase of 3% on 2001. Whilst these figures overall were lower than anticipated, the success was concentrated in only two of the five fraud categories. Card not present transaction fraud was not one of them and grew by 15% last year. It should also be noted that the total value of £424.6 million is not the total cost of fraud, just the value of fraudulent transactions. It does not include the administrative costs involved in handling fraudulent transactions and certainly does not include the costs incurred by retailers in chargeback processing fees or higher merchant service charges resulting from fraud losses incurred by the card industry. The following sections describe the different areas of fraud and their current trends.

Counterfeit Card Fraud Losses



2.3.1 Counterfeit Cards

Counterfeit card fraud cost £148.5 million in 2002, a fall of seven per cent on losses of £160.4 million in 2001. The fraud reduction in this category is due to the successful implementation of banking industry tactical initiatives combined with the creation of a unique police unit set up to tackle the organised criminal gangs behind counterfeit card fraud. Losses of £148.5 million per annum still represent a very significant problem, but this will be countered in the UK by the roll out of Chip and PIN by 2005

A counterfeit card is one that has either been created from scratch by criminals using real or fake card numbers or is a valid card that has been altered.

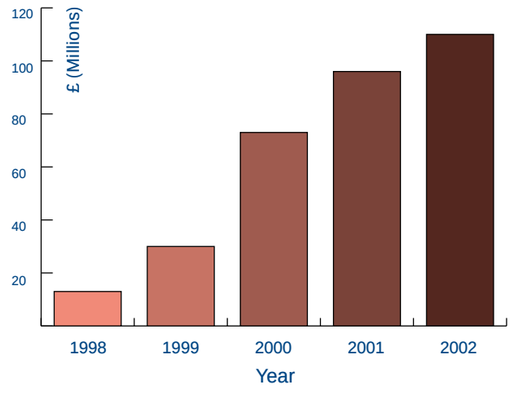
The majority of counterfeit card fraud finds its source from skimming, the process whereby legitimate card details are recorded from a card's magnetic stripe and are subsequently encoded onto a fake card by the criminals. Skimming is normally perpetrated by retail staff who record card details using pocket sized recording units before returning the valid card to the cardholder during a sale. They then sell the recorded information to organised criminal groups, who make the counterfeit cards. Skimming is particularly prevalent in the hospitality and petrol markets. However, the use of skimmed data is not limited to the production of fake cards for use in card present environments. The information is also used to undertake fraudulent card not present transactions with false delivery addresses.

2.3.2 Card Not Present Fraud (fraudulent possession of card details)

This category includes fraud from mail order, telephone order (MOTO), fax order and e-commerce transactions.

Card not present fraud cost £110.1 million in 2002 - an increase of 15 per cent from the 2001 figure of £95.7 million. This type of fraud involves using fraudulently obtained card details to make a purchase. Usually the details are taken from discarded receipts or copied down without the cardholder's knowledge. As with most card fraud, the legitimate cardholder may not be aware of the fraud until a statement is received.

Card Not Present Fraud Losses



An address and card security code checking system has been made available to retailers by the UK card industry to fight this type of fraud and the usefulness of these countermeasures are discussed in detail later in this document. Suffice to say at this stage that the address verification system is experiencing a number of

accuracy problems and the security codes are already available for sale to criminals with associated card numbers over the internet. Commidea believes that these countermeasures, whilst useful tools, should not be used in isolation to combat card not present fraud.

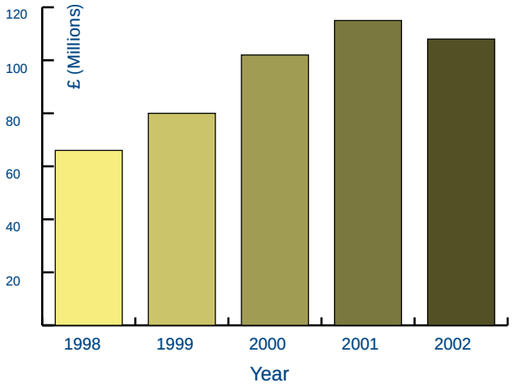
It is also worth noting that e-commerce or “internet” transactions accounted for £28 million of the £110.1 million lost to fraud in card not present areas. This alone represents a significant increase from £15 million the year before and just £3.8 million in 2000 - a jump of 24.2 million in just two years.

2.3.3 Lost and Stolen Card Fraud

Fraud on lost and stolen cards cost £108.3 million in 2002. Most fraud in this category takes place at retail outlets before the cardholder has reported the loss.

A retailer education programme, set up by APACS in 2001, teaches shop staff how to detect stolen cards being presented for payment at the point-of-sale. A further tool used by the banking industry to help detect fraud on cards that are not yet reported missing is the use of intelligent computer systems that track customer accounts for unusual spending patterns. These initiatives, combined with the work of the Industry Hot Card File has led to a five per cent reduction in lost and stolen card fraud from 2001.

Lost & Stolen Card Fraud



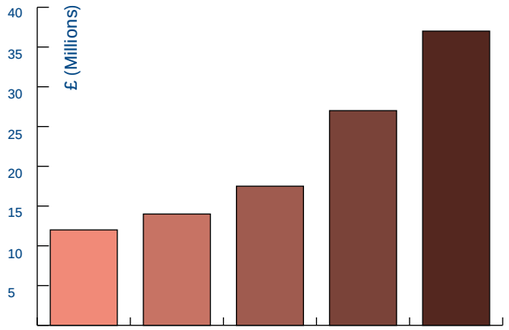
The introduction of Chip and PIN in the UK will see cardholders use a PIN at the point-of-sale instead of a signature, which will make it extremely difficult for criminals to use lost and stolen cards in a face-to-face transaction, although this may lead to a partial fraud migration towards card not present fraud using lost/stolen card details.

2.3.4 Mail Non-Receipt Fraud

This type of card fraud, although increasing significantly by 39% in 2002, still only represents 9% of total card fraud. This is largely attributable to an ongoing partnership between the banking industry and the Royal Mail to ensure security in card distribution.

Mail non-receipt fraud along with and in conjunction with card not present fraud are believed to be the two areas most likely to be targeted by fraudsters as areas of fraud migration when the Chip and PIN roll out matures towards the end of 2004.

Mail Non Receipt Fraud



In response to this potential threat, the Association for Payment and Clearing Services (APACS) has established an action group to implement specific initiatives in this area.

2.3.5 Identity Theft

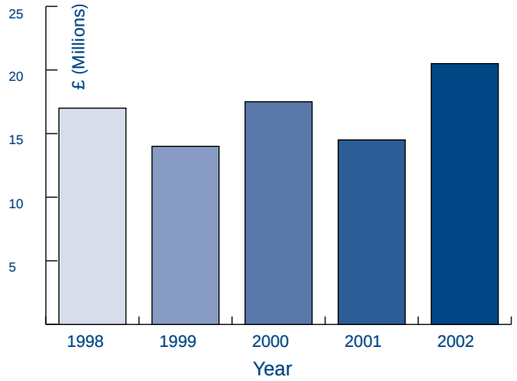
Identity theft fraud, whilst relatively minimal in the U.K. currently at just 4.85% of total fraud, is an area of growing concern not just within the card industry, but across a broad range of industries that involve personal data security. The roll out of chip & Pin is again likely to have an adverse effect on growth in identity theft fraud.

Identity theft fraud is broken into two sub categories; Application fraud (£10.2m) and account acquisition fraud (£10.4m) and are described as follows :-

Application fraud
Application fraud involves criminals using stolen or false documents to open and use a card account under false pretences, usually under someone else’s name. Criminals may use discarded personal documents such as a utility bill or a bank statement to create an apparently legitimate application.

Account acquisition
Criminals try to mimic or acquire a legitimate card account, first by gathering information about the intended victim and then by either using that information to mimic the cardholder during a transaction with goods diverted to a different address, or even to contact the card issuer to ask that mail be redirected to a new address. Once identity has been stolen, most other forms of card fraud are then open to the criminal.

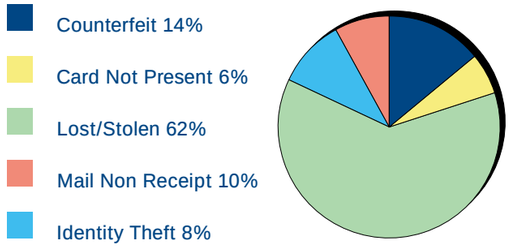
Identity Theft Fraud



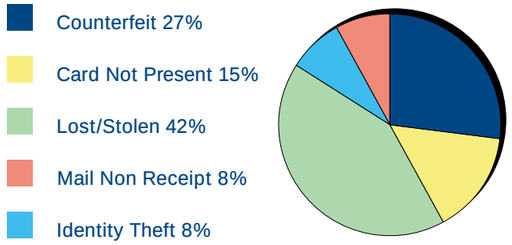
2.4 Fraud Trends

The following pie charts show the changing trends of card fraud losses over the last ten years. Counterfeit and card not present fraud have steadily increased, whereas other fraud categories have decreased as the result of significant industry initiatives. For example, the proportion of fraud committed on lost and stolen cards is steadily decreasing.

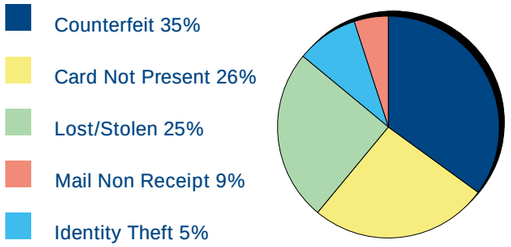
Fraud in 1996



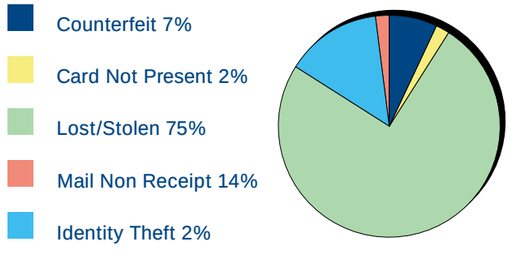
Fraud in 1999



Fraud in 2002



Fraud in 1993



By the end of 2005 it is expected that Chip and PIN will have greatly reduced fraud in the counterfeit and lost/stolen categories - the 1st and 3rd largest categories of card fraud today. The question is, how much increase or migration will there be to other categories - particularly card not present fraud where industry initiatives are scarce or of short term benefit and which represents the 2nd largest and fastest growing category of card fraud today.

3 Business Objectives

3.1 General

It would be natural now to state that the primary objective connected with fraud prevention should be to eliminate fraud from your business altogether. But if that were to be your objective then you do not need a complex fraud prevention service. You only need to reject all “possibly” fraudulent orders and for that you could devise simple in-house rules. In doing so, however, you will reject a higher percentage of valid orders and insult more genuine customers. This in turn will result in the loss of genuine revenue to a value higher than the original losses due to fraud.

No, the primary business objectives of a card fraud prevention system must be to reduce fraud to minimal levels, and to do so in a way that retains most, if not all, of your genuine orders whilst preserving a positive customer ordering experience. This strategy allows for measurement of the fraud prevention service and confirms that genuine orders and customers are not being turned away. A balance must be achieved to reject most of the fraud and to accept most, if not all, of the genuine orders.

3.2 Consumer Experience

Whether in relation to fraud or not, the consumer ordering experience is a key factor in your efforts to create repeat business and in enforcing brand strength. Intrusive or cumbersome fraud prevention tactics often have an adverse effect on this key business objective by frustrating cardholders and creating a negative consumer experience. It is therefore vital to employ an efficient and seamless fraud prevention service to shore up your efforts towards building consumer confidence and excellence in your customer service.

3.3 Cutting Costs

According to a survey sponsored by Cybersource Int’l Ltd by Mindwave research, the most significant costs associated with on-line fraud are liability for chargebacks, loss of staff time and direct loss of revenue. A seamless and efficient fraud prevention system can significantly reduce all of these cost areas by reducing the incidence of fraud (and therefore chargeback), by automating a higher percentage of decisions thereby reducing time spent on manual order review (which for some “most at risk” merchants involves the review of 100% of orders), and by rejecting a higher percentage of attempted fraudulent transactions and reducing direct revenue losses. However, there are many more factors that contribute to the costs associated with card fraud that can be reduced or eliminated through a multi-faceted fraud prevention system.

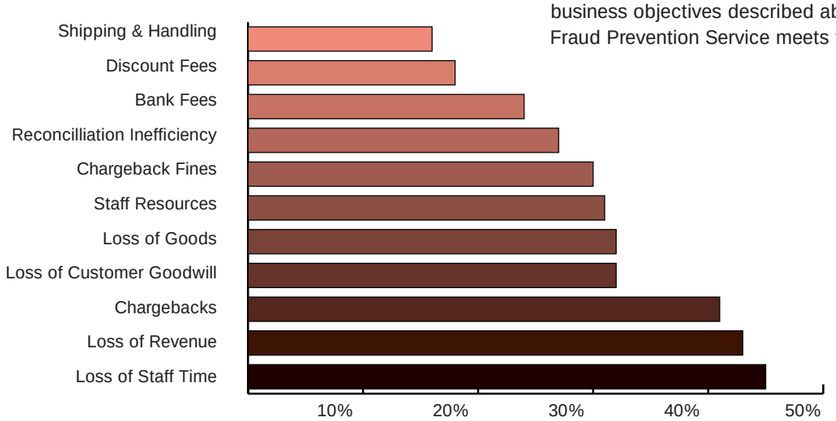
3.4 Eliminating Insults

Fraud prevention must be a combination of as many useful tools as possible to bring accuracy and to prevent customer insults. The use of over zealous or “one size fits all” rules to try and prevent fraud will inevitably lead to the rejection of some valid orders. This can easily create a customer perceived insult which, unless your product categories are unique, often leads to consumers altering their choice of supplier for those goods and the associated loss of potential revenue for your business.

3.5 Return on Investment.

In this day and age, almost all businesses demand a quickly realisable return on investment in technology solutions. Retail experience particularly in the area of CRM and ERP has led to a sharper focus on technology ROI and fraud prevention is no different. A fraud prevention system must provide a measurable reduction in all cost areas associated with card fraud and to achieve that, it must be effective in meeting all of the business objectives described above. The Commidea Fraud Prevention Service meets this objective.

Negative Impacts of OnLine Fraud



4 Existing Prevention Techniques

In addition to the basic card transaction checks that have been available for many years, the industry has recently introduced a few new initiatives aimed at preventing or detecting fraud for CNP merchants.

4.1 Basic Card Checks

Any retailer undertaking CNP transactions should, as a minimum, perform basic card checks through an electronic card processing system (be it manual key entry into a swipe machine or a more sophisticated integrated system). These checks are described as follows :-

* Card Number Check

This is a calculation performed on the card number itself to ascertain the correct value of the last digit of the card number. It is often referred to a “Modulus 10” check or “check digit calculation”. Whilst this check can instantly identify a fabricated card number which will have only a 1 in 10 chance of being correct, the calculation is very public and fraudsters rarely fall foul of this check.

* Issuer Check

The first 6 digits of most card numbers are used to identify the bank that has issued the card. Each issuing bank is provided with one or more BIN (Bank Identification Number) ranges under which their cards are issued. If a fabricated card does not fall within a valid BIN range for any bank then it can be detected as fraudulent. Again, fraudsters rarely fall into this trap when generating card numbers.

* Expiry Date Check

Quite obviously expired cards are deemed to be invalid, but the precise expiry date can now be checked during an online authorisation call. A specific card’s expiry date is not publicly available and so this a useful tool to check against fabricated numbers. However, fraudsters have taken to attempting to use fraudulent cards online with low risk merchants such as charities to try different expiry dates until they find the correct one to use.

* Start Date Check

As with expiry dates, start dates are only valid once they have passed. This does help prevent fraud on “mail non-receipt” cards until after the start date and does give opportunity for cardholders to report non-receipt of a new card and for the issuer to block the card against authorisation before it can be used.

* Issue Number Check

Issue numbers only appear on Switch or Solo cards and are checked as part of an online authorisation call. This can catch out fraudsters although only after a card has been reissued and usually not when using fabricated cards.

* Online Authorisation

The most realistic way of catching a fraudster using existing methods is to perform an online authorisation call. Not only does it involve the checking of expiry date, issue numbers and start dates, it also involves a lookup on the customer’s card account to see if the card has been reported lost or stolen, checks to make sure that the account is valid and allows the issuers to check the transaction against spending habits and patterns. For example, issuers can detect fraud if the same card has apparently been used in two different countries within an unrealistic time delay and confidently assume that one of the transactions is likely to be fraudulent. At the same time an online authorisation call also provides issuers with the ability to check account status and take credit decisions.

For most retailers all of these checks are already provided automatically either in part through an order processing system or in full through a card payment processing solution such as Commidea’s WinTI, BatchPro or ICP service. These checks are now widely adopted and considered to be default in terms of card acceptance. Unfortunately, CNP fraud has risen consistently since 1995 despite these basic checks.

4.2 Recent Initiatives

Over the last couple of years, three new initiatives have been introduced to combat CNP fraud.

4.2.1 Cardholder Address Verification (AVS)

AVS has been introduced to enable card not present retailers to verify the cardholder billing address for customers living the US or UK. It uses only numeric values within the house number and postcode fields and is checked as part of the authorisation process. To date, AVS checking has been marred by several factors including minor differences between the addresses quoted by cardholders and those held by the issuing banks, shared property addresses (such as flats), the absence of house names in many UK addresses (e.g. use of house names with no numerics) and the ease with which fraudsters have been able to obtain cardholder billing information. To date the industry is still only quoting a 70-80% accuracy in address checking although based upon their own experiences, many retailers and other organisations believe that AVS only provides a valid match on a little as 25% of orders. Whilst a useful tool, it cannot be used as the sole or even principal tool in detecting card not present fraud as it could cause the rejection of high volumes of valid orders.

4.2.2 Card Security Code (CSC) Verification

The card security code is the three digit number printed on the signature panel of most cards (American Express uses a four digit code printed on the face of the card just above the card number and is called the 4DBC). The number is not encoded onto the magnetic stripe of the cards and is not captured electronically when a card is swiped or when a card is skimmed, and is not printed on card receipts. CNP retailers can ask cardholders for this number and check its validity as part of the authorisation process. This check is far more accurate and is very useful in confirming that the card is in the possession of the cardholder when placing an order. However, CSC numbers have become available for sale to criminals over the internet with valid card numbers and so once again, this check cannot be used solely or principally to detect CNP fraud.

4.2.3 E-Commerce Payer Authentication

Payer Authentication is an e-commerce version of PIN verification and is supported only by Visa and MasterCard at this stage. Visa's scheme is called Verified by Visa and MasterCard's scheme is called Secure Code. Both schemes require cardholders to register their cards online and to assign a password or PIN number to each of their cards. The PIN number or password can then be verified by the issuer when making an online purchase. This scheme is not only very good at preventing online fraud, it also brings with it a liability shift for the online retailer. Instead of accepting 100% liability for online fraud, the simple ability to support payer authentication means that the liability for chargebacks, where a customer denies making the purchase, remains with the card issuer. Good news indeed!

Unfortunately, the adoption rate amongst UK retailers is thus far minimal. Why is that? Possibly because the technology is not yet standardised nor fully operational. Possibly because the intended 100% liability shift away from retailers towards issuers is attracting the consideration of conditions and provisos (e.g. liability shift denied in certain merchant categories or where incidence of fraud exceeds 1%). Possibly because online retailers don't want to further complicate the buying process online with additional pop up windows and password prompts. But probably because these and other factors make it early days for payer authentication and few retailers want to make what is perceived to be a costly investment without a good chance of return. Significantly also, cardholder registration levels are disappointing at an estimated 0.1% with no plans yet for compulsory registration. Many retailers are therefore questioning the legitimacy of a scheme that has yet to establish itself and prove that it will be in force for the foreseeable future. On the positive side, payer authentication is reported to increase consumer confidence when used, and reports suggest that transaction values also increase as a result of this added confidence.

Commidea believes that payer authentication should be readily available to all online merchants and used as a key tool in fighting online card fraud. For that reason our Fraud Prevention Service includes payer authentication processing without the need for massive up front investment or commitment from our customers. Whilst adoption rates are low from both cardholders and online retailers, it is predicted that as many as 35% of online transactions will utilise payer authentication by the end of 2004. In the long term retailers may even reject orders unless cardholders are enrolled in payer authentication schemes.

4.3 Additional Prevention Tools

All of the basic card checks and more recent advanced checks can be made as part of the authorisation process through card payment processing systems such as Commidea's. However, there are a number of additional manual checks that can be used and that are recommended by APACS. Unfortunately most of these additional checks are either time consuming, costly or both and many rely heavily on manual intervention in order processing. Some of these checks are described below :-

* Velocity of use check - Check to see how many times a card is used over a short time period. High instances may suggest fraud.

* Velocity of change check - this type of check can detect several different fraud patterns and are based upon multiple data elements to detect change. For example, check to see if the same card has been quoted with different delivery addresses or if it has been used with different expiry dates which may indicate fraudsters attempting to find the correct expiry date for a card created by a number generator.

* Landline check - check that the home phone number given exists or check it against the address provided using directory enquiries.

* Typical customer check - check to see if new customers fit in with your typical customer profile.

* Product and quantity check - look out for unusual orders either in terms of value or quantity of product ordered.

* Delivery address check - don't deliver goods to high risk areas. Ask your Acquirer for up to date information on high risk areas and countries.

For a comprehensive approach to fraud prevention, retailers must consider both basic, advanced and additional checks. The Commidea Fraud Prevention service combines not only these checks but many more in an all-encompassing approach that can be tailored to you and to your market.

5 Commidea Fraud Prevention Service

5.1 Introduction

The Commidea Fraud Prevention Service is a multi-faceted service combining a range of state of the art tools to increase screening accuracy and to decrease the incidence of fraud and of valid order rejection. The system comprises seven separate elements, any combination of which can be utilised to different degrees to suit your business. Tailoring the process is achieved through the use of business logic strategies which Commidea will either write for you, write with you or implement for you.

The service is run in house by Commidea with customers submitting screening requests to us electronically (via a number of different connection methods - see Chapter 6 “Connectivity”) which include several mandatory and optional data elements per request. The data elements are described in detail in Chapter 7.

For simplicity, the responses generated from the service are limited to “Accept, Reject or Manual Review”. However, additional result information is returned to you to allow you to assess the reasons behind any rejections or manual review responses. Furthermore, our TMIS management information system provides a sophisticated report generation tool to aid analysis, a manual review module to enable you to accept or reject manual review transactions and a reconciliation tool for those customers using Commidea for settlement processing.

5.2 Components

5.2.1 Rules

The first tool employed by the system is a rules engine and business logic application that will not only determine the entire workflow of your transactions through the various tools described below, but is also used to apply rule criteria to transactions on a true/false basis. For example, if you wanted to reject any orders where the home phone number provided is a mobile number, a simple rule can be applied within your strategy such as follows :-

“If home phone starts 07 then reject, else proceed”

Of course, you may not want to reject an order just because of this one factor, so the business logic application can be used instead to assess the result of this rule and add an additional value to the transaction which can be used in conjunction with other rule results and criteria to make a decision later in the process (i.e. use this rule to increase the risk factor of the transaction, but not to accept or reject the transaction based upon this one rule).

The rules engine is used throughout the screening process and can be used to influence results based on any factor present within the processing request as it proceeds through a strategy.

5.2.2 Authorisation

Some customers will seek card payment authorisation outside of the Fraud Prevention Service, either through an alternate supplier or through Commidea’s BatchPro or WinTI payment software. If so, this check is available to ensure that an authorisation has already been obtained for the request. Alternatively, the service can be used to obtain authorisation (and/or settlement) from any UK Acquiring Bank, prior to screening for fraud but as part of a single process. This module will therefore seek or confirm authorisation and proceed with fraud screening when necessary.

5.2.3 Lists

One of the most basic but often most effective methods of fraud prevention is to maintain positive and/or negative customer lists. The Commidea fraud prevention service provides the ability for you to check your transactions against separate lists containing information relating to your customers only. For example, by adding the details of a cardholder who has committed fraud against you previously to your negative list, you can block future transactions containing the same or similar details. Similarly you can create positive lists of good customers to identify them at an early stage in the process. The lists are held centrally by Commidea on your behalf as part of the service and can be updated at any time.

5.2.4 Velocity

List checking is then backed up within the service by velocity checks. There are two different types of velocity check available within the service; velocity of use and velocity of change. Velocity of use (where a card is used many times over a short period) can detect fraudsters trying to gain maximum value from a stolen card/details or from a counterfeit card. The velocity of use check looks to see how often a name, address, phone number and card number have been used over a short time period. It not only checks against the transactions that you have presented, but also against records spanning several thousand merchants, for similar usage patterns. Velocity of change looks for patterns in small changes to customer details. For example, the same card being used with different expiry dates could indicate that a fraudster is trying to find out the correct expiry date for a card number obtained from a number generator. It can also be used to detect the use of several different card numbers with the same delivery address. In fact, velocity of change checking can detect a wide range of unusual patterns that may increase the likelihood of a transaction being fraudulent.

5.2.5 Payer Authentication

For e-commerce retailers, payer authentication could lead to substantial savings against fraud liability. At present the two major card schemes, Visa and MasterCard are offering a 100% liability shift for merchants, even if the cardholder is not enrolled in the scheme and cannot therefore be verified on-line. The scheme is relatively simple to operate. On making a purchase from your online store, a message is sent from you to Commidea and then on to the issuing bank to check to see if the cardholder is enrolled. If they are, a popup window is displayed to the cardholder asking them to enter their password or PIN. The PIN is verified centrally by the issuer who sends you an encrypted code. You then send the encrypted code to Commidea for verification along with a normal fraud screening request. If the code is successfully verified, you may not wish to undertake any further fraud screening on the transaction, as the liability already rests with the issuer for any fraud. Alternatively you may wish to screen the transaction as normal to avoid the possibility of losing your liability shift if your online fraud exceeds the suggested 1% threshold.

5.2.6 Predictive Score

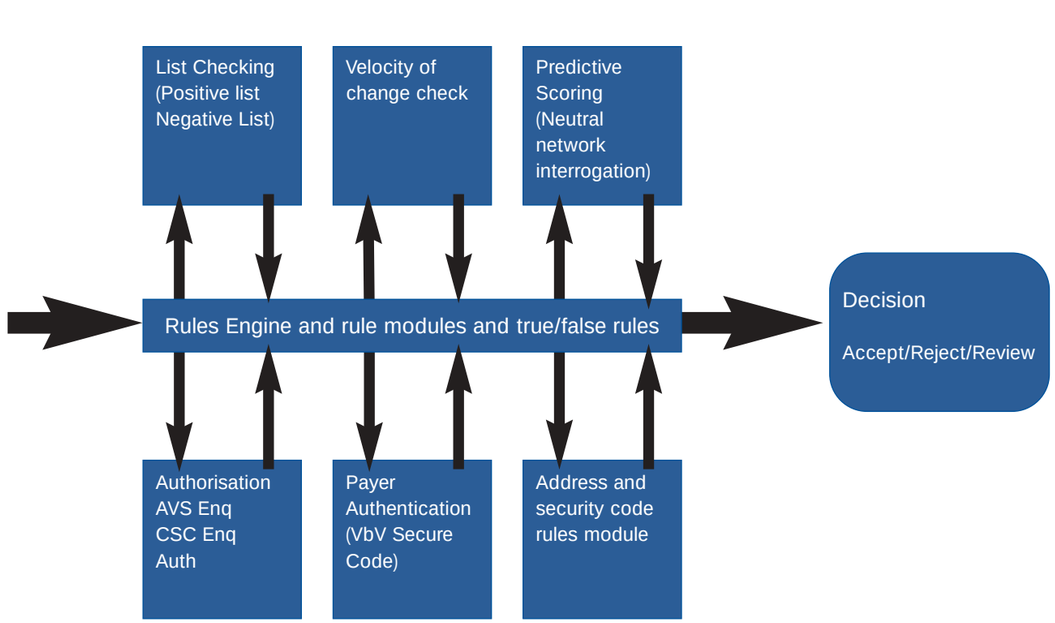
Predictive fraud scoring is a complex process for which Commidea is proud to work in partnership with Cybersource International - a world leader in card fraud prevention. The process employs a hybrid combination of neural networks, databases, geolocation and over 150 different checks using sophisticated risk modelling techniques that combine to score each transaction against the likelihood of fraud. A score between 0 (low risk) to 99 (high risk) is assigned to each transaction along with a range of key factor codes that were most relevant to the score. The system constantly assesses worldwide fraud trends and card usage patterns to uphold its accuracy and to detect fraud trends more rapidly than other systems.

The score and the factor codes are then analysed by the rules engine based upon your specific strategy to aid in the decision making process. Strategies are normally formulated to allow transactions under a specific score to be accepted (e.g. under a score of 35) and those over a certain threshold to be rejected (e.g. 60) Those in the middle may be flagged for manual review. However, the preceding factors in the overall strategy will play a part in assigning score thresholds and decisions. For example, a transaction that has met all previous criteria (e.g. not detected on a negative list, no problem with velocity checks, no issues with business rules and where the order value, quantity or product type all indicate low risk) and is thus far classified as low risk, may pass through a low risk branch of a strategy where orders are accepted at a higher score threshold than high risk transactions.

5.2.7 AVS/CSC

The final tool in the Fraud Prevention Service suite is an AVS and CSC module that puts a final weight to a transaction's overall result. As mentioned earlier in this document, AVS is a useful tool but cannot be used standalone in the fight against fraud. Both elements of an AVS check are assessed through the AVS module (i.e. house number and postcode) and final decisions made based upon the various AVS result codes (not checked, no match, partial match and full match) returned by an Issuer. Similarly, the CSC result is also filtered to add to the final decision making process for any card transaction presented to the system.

Transaction Flow Diagram



5.3 Strategy

The previous section touched briefly on the need to implement a transaction processing strategy to suit your business. A strategy is used to define the business logic behind your screening processes and governs the criteria upon which you accept, reject or review your orders. Commidea has designed four separate start-up packages based upon the type of strategy required to help customers introduce the service at the earliest opportunity.

5.3.1 Default

Commidea has produced two default strategies which customers can adopt without modification to provide the basis for the business logic employed. One strategy has been designed for Mail Order/Telephone Order (MOTO) sales, the other specifically for e-commerce processing. Both strategies utilise the full suite of tools within the Fraud Prevention Service and have been designed to accommodate a generic approach to fraud prevention for their markets. Each strategy allows transactions to be branched through sub strategies dependent upon the level of risk assigned by you to the transaction originally, or as the result of some pre-built rules checking phone numbers, delivery addresses, and geolocation. These sub strategies are classified as low, medium and high risk. Within the sub strategies the predictive scoring and AVS/CSC processes are used, but with different acceptance or rejection thresholds dependent upon the level of risk involved.

The default strategies are useful for customers without any specific requirements or who simply want to gain experience of the system prior to creating a specifically tailored strategy for their business.

5.3.2 Weighted

A weighted strategy start-up allows customers to use one of Commidea's default strategies but with different weighting within the strategy. For example, you may wish to accept orders at a higher threshold than the default strategy, in which case the strategy would be modified with your own specific requirements. Similarly, the default strategy prohibits orders with delivery addresses in certain countries whereas you may want to allow those deliveries. Again, the strategy would be amended to meet your requirements.

5.3.3 Tailored

A tailored strategy provides you with the ability to create your own unique business logic process using the full suite of tools available within the Commidea Fraud Prevention Service. For example, you may want to decide for yourself the order in which different tools are used within the process and set different levels of

importance to different results. With a tailored strategy you can also choose to implement unique rules within the rules engine that are specific to your business. As an obvious example, if you sold plasma TV screens, you may wish to limit the number that customers can purchase from you on the basis that a customer buying four or five might well be a fraudster. In this case a custom rule can be employed to check the quantity of specific product codes within each order and to act appropriately.

Example of a basic stratagy

5.3.4 Enterprise

The enterprise start-up is a fully consultative approach designed to create multiple and multi-layered strategies for complex sales environments. The enterprise start-up provides complete flexibility for you to determine the exact strategies required in each and every facet of your business to detect and prevent card fraud. The enterprise start-up program includes intensive consultation with all relevant parties within your organisation to make sure that valid orders are maximised, fraudulent orders are kept to an absolute minimum and the overhead of manual review is kept to acceptable levels.

Whichever start-up package is appropriate for your business, Commidea will provide consultancy where requested to help you devise your strategy, fully notated copies of your strategies with supporting logic and the ability for you to change your strategies at any time and in any way you deem appropriate to help protect your business from the threat of card payment fraud.

5.4 Review

The review process is an essential tool in the ongoing fight against fraud. It would be foolish indeed to implement a fraud prevention service with a pre-determined strategy based upon information at hand today in the hope that it will continue to be effective forever. Our review process provides you with a third party analysis of your transaction data and result information compared against the subsequent levels of fraud experienced and the levels of accepted/rejected orders. The review process can highlight deficiencies in existing strategy due to changing fraud tactics, determine adjustments required to reduce manual review overhead and pinpoint areas which could be changed to increase valid order acceptance. Without a review process and without a readiness to be constantly pro-active, the fraudster will soon be back, finding new ways to break through your defences. Commidea offers a wide range of review packages to assist you in this process. Alternatively you may decide to review you own data in-house and simply instruct us to amend your strategies on a regular basis.

5.4.1 Reports

Irrespective of the nature of your review program, Commidea provides you with monthly transaction reports detailing your acceptance, rejection and review levels and highlighting any specific factors that are contributing to the results being achieved. These reports alone can lead to changes to strategies or adjustments to the weighting applied to different screening areas within your strategy.

5.4.2 Strategy Updates

Strategy updates are simple to implement with the Commidea Fraud Prevention Service. If you choose to use Commidea to undertake your review processing we will report to you all of our findings and strategy change recommendations. On agreement for any recommended changes, Commidea will prepare an adjusted strategy for your approval and will then implement your new strategy as directed. If you decide to undertake your own review process, you can simply instruct us to amend your strategy as you see fit. Once again, we will prepare an adjusted strategy for your approval and implement it accordingly.

6 Connectivity

6.1 General

Connectivity to the Commidea Fraud Prevention Service is achieved over the internet to specific IP addresses allocated to you on start-up. Naturally, all data sent to and received from the service has to be encrypted for security of card and consumer details. UK banks require a minimum of 128 bit SSL encryption and all Commidea connectivity solutions comply with this, and other, bank regulations for card security. Additionally, for card payment processing, Commidea has joined the Visa AISP certification programme to bring added confidence to merchants and cardholders alike.

There are three methods of connectivity to the service which are described in the following sections.

6.2 Client Software

Commidea can provide a client end software application module to enable you to securely transmit processing requests to us. The software application, ICP Client, can be integrated with your host applications directly. It is a Windows 32 bit application designed for use on PCs running Windows NT, 2000 or XP. Windows 95 and Windows 98 platforms are no longer supported. The ICP Client application can be configured to run in one of three different ways to suit your preferred method of integration or operation.

6.2.1 Text File Interface

When configured to run with a text file interface, customers have the option to present transactions for processing in the form of comma separated text files. These “input” files are placed by your host system in a specified network or local directory which is scanned by the ICP Client application up to 32 times per second. On detection of a new input file, the ICP Client application imports the data into an internal database and then creates a connection to the Commidea central servers and transmits the processing request. Input files can contain one or multiple transaction processing requests and can therefore be used for real time single transaction processing or for batch/bulk processing. On receipt of a response from Commidea’s central servers, the ICP Client stores the results within its internal database and then produces an output file, again as a comma separated text file, and writes it to a specified directory. The host system can then read the output file or “result” file and act accordingly on its contents. The connection established between the ICP Client and Commidea’s central servers uses 128 bit SSL encryption for security.

6.2.2 DLL Interface

The DLL interface configuration can be used to integrate ICP Client directly with your host application. As with the text file interface, all transaction data passed through the DLL interface is recorded in the ICP Client database and all communications to and from the Commidea central servers is encrypted to a minimum of 128 bit using SSL. All customers need to make available is internet connectivity. Full specifications are provided for the various DLL function calls and for integration.

6.2.3 Keyed Input Interface

For customers not wanting to integrate ICP Client to their host application, the ICP Client can be configured to present a screen input interface. The Client is run in the same way as any other Windows application and the screens prompt users to enter transaction information which is then transmitted to Commidea for processing using the same methods as apply to the DLL or Text file methods. Transaction results are displayed back to operators and all information is stored within the ICP Client internal database.

6.3 Gateway Connection

Our Gateway connection service enables customers to transmit processing requests and receive processing results from any browser-based application including e-commerce platforms. The Gateway service presents customers with an SLL port on a specified IP address at Commidea to which requests are transmitted using a simple http Post command. Result information is returned either as a response to the original POST request or as a separate return post to a URL of your choosing.

6.4 VPN Connection