“Credit card fraud and detection techniques: a review”

AUTHORS	Linda Delamaire Hussein Abdou John Pointon

ARTICLE INFO	Linda Delamaire, Hussein Abdou and John Pointon (2009). Credit card fraud and detection techniques: a review. *Banks and Bank Systems*, *4*(2)
JOURNAL	"Banks and Bank Systems"
FOUNDER	LLC “Consulting Publishing Company “Business Perspectives”

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
0	0	0

Linda Delamaire (UK), Hussein Abdou (UK), John Pointon (UK)

Credit card fraud and detection techniques: a review

Abstract

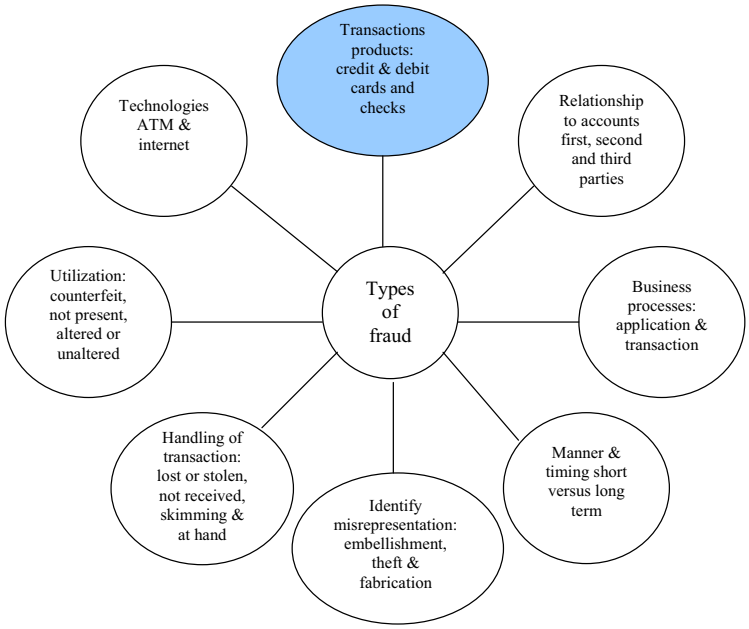
Fraud is one of the major ethical issues in the credit card industry. The main aims are, firstly, to identify the different types of credit card fraud, and, secondly, to review alternative techniques that have been used in fraud detection. The sub-aim is to present, compare and analyze recently published findings in credit card fraud detection. This article defines common terms in credit card fraud and highlights key statistics and figures in this field. Depending on the type of fraud faced by banks or credit card companies, various measures can be adopted and implemented. The proposals made in this paper are likely to have beneficial attributes in terms of cost savings and time efficiency. The significance of the application of the techniques reviewed here is in the minimization of credit card fraud. Yet there are still ethical issues when genuine credit card customers are misclassified as fraudulent.

Keywords: credit card fraud, detection techniques, credit bureaux, data mining techniques.
JEL Classification: C49, G21, G24, K42.

Introduction

For some time, there has been a strong interest in the ethics of banking (Molyneaux, 2007; George, 1992), as well as the moral complexity of fraudulent behavior (Clarke, 1994). Fraud means obtaining services/goods and/or money by unethical means, and is a growing problem all over the world nowadays. Fraud deals with cases involving criminal purposes that, mostly, are difficult to identify. Credit cards are one of the most famous targets of fraud but not the only one; fraud can occur with any type of credit products, such as personal loans, home loans, and retail. Furthermore, the face of fraud has changed dramatically during the last few decades as technologies have changed and developed. A critical task to help businesses, and financial institutions including banks is to take steps to prevent fraud and to deal with it efficiently and effectively, when it does happen (Anderson, 2007).

Anderson (2007) has identified and explained the different types of fraud, which are as many and varied as the financial institution's products and technologies, as shown in Figure 1.



Source: own figure, following Anderson's classification (2007).

Fig. 1. Types of fraud

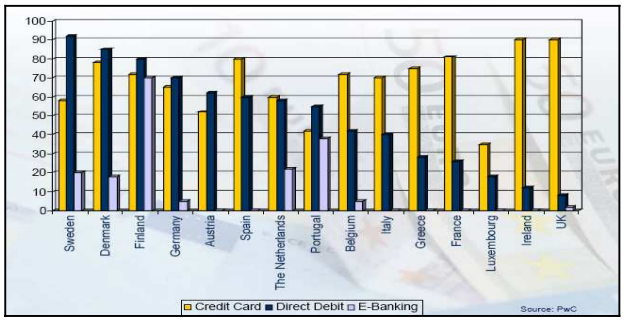
The main aims are, firstly, to identify the different types of credit card fraud, and, secondly, to review alternative techniques that have been used in fraud detection. The focus here is in Europe, and so ethical issues arising from other cultures are not taken into account; but for a discussion of these the reader is referred to Chepaitis (1997) and Gichure (2000). Indeed, transaction products, including credit cards, are the most vulnerable to fraud. On the other hand, other products such as personal loans and retail are also at risk, and have serious ethical

Acknowledgement: The authors wish to thank Peter Sinclair for helpful comments. And very special thanks for Pago e-Transaction Services GmbH, for providing us with all the Figures used in the current paper.

implications for banks and credit card companies. Credit card fraud may happen in various ways, which depend on the type of fraud concerned; it encapsulates bankruptcy fraud, theft fraud / counterfeit fraud, application fraud and behavioral fraud. Each of these sub-fraud categories has its own definition and specificity. Techniques to fight against those are reviewed, and examples from European markets are presented.

Euromonitor International (2006) stated that, impressively, 120 million cards (i.e., debit cards, credit cards, and charge cards) were brought into use in 2004 in Germany, and that the total transaction value generated by cards reached some €375 billion in 2004, up nearly 4% from 2003, including cash withdrawals. Because of the increasing usage of cards for payments, the amount spent on sales and internet purchases with any kind of cards has jumped by 5% reaching €170 billion. However, cash withdrawals faced a lower growth. Those new patterns in customer payment behavior are probably correlated assuming that customers substitute cash payments for card-payments (Euromonitor International, 2006).

Focusing on the credit card business, in the German market, for example, the word "Kreditkarte" refers to both charge cards and credit cards. There is no clear distinction between the two, whereas in English the different products have their own terms. To distinguish between the two products, debit card and credit card, credit card banks have offered the possibility to their customers to revolve their credit through credit cards. This service or credit is also a way to attract them. However, even if customers have the possibility to revolve credit, not all of them use this service. Nevertheless, in 2004, credit cards enjoyed a faster growth than charge cards (Euromonitor International, 2006).

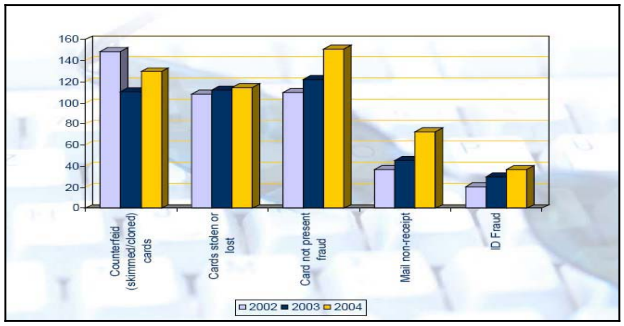


Source: PwC. This is cited in DRF EU Speech on April 19th 2005 in Amsterdam (Pago e-Transaction Services GmbH, 2005).

Fig. 2. Transaction products in Europe

In 2005, as shown in Figure 2[1], the market of transaction products in Europe is split into two groups. The credit card group leads the market. This group includes some of the following countries: Spain, Belgium, Italy, and Greece. In two countries, credit cards have no competitors in terms of transaction product. Those two countries are the United Kingdom and Ireland. On the other hand, another group of country uses mostly debit cards; it is especially the case for Sweden. However, for this group, the standard deviation between the two types of transaction product is less visible than for the other group. As to Germany, for example, the German market appears to be underserved by credit cards. Indeed, payment by cards has been increasing in the German market over the past few years. The market for credit and charge cards is forecast to grow by 23.3% from 2004 to 2009, to reach a value of €56,477 million (Euromonitor International, 2006).

With this extensive use of credit card, fraud appears as a major issue in the credit card business. In the European Union, the first signs could have been seen in the United Kingdom in the 90s. In fact, total losses through credit card fraud in the United Kingdom have been growing rapidly (1997, £122 million; 1998, £135 million; 1999, £188 million; 2000, £293 million [Association for Payment Clearing Services London (APACS), no date]. Yet, in 2006, APACS reported £423 million losses, a decrease of nearly £80 million over the previous two years. The main reason for this improvement is the success of chip & PIN that has led to a decrease of face-to-face fraud. However, if mail-non-receipt fraud and lost and stolen card fraud are decreasing, counterfeit card fraud and card-not-present (CNP) fraud are increasing although they are increasing at reducing rates (APACS, no date).



Source: DRF EU Speech, Amsterdam, April 19th 2005 (Pago e-Transaction Services GmbH, 2005)

Fig. 3. Fraud distribution in Europe

The explosion of credit card fraud is not only due to the constant increase of card usage but also to the ease of perpetuating credit card fraud. The complexity of credit card fraud is that it may be committed in various ways, including theft fraud, application fraud, counterfeit fraud, bankruptcy fraud. In 2005, stolen and counterfeit frauds

dominated the European fraud market, as shown in Figure 3. By not paying enough attention to fraud prevention or detection, the risk for the bank is that "credit card fraud remains usually undetected until long after the criminal has completed the crime" (Caminer, 1985; Bolton & Hand, 2001). Therefore, it will generate irrecoverable costs for the bank.

This paper suggests measures to reduce the expected loss and is organized as follows: section 1 defines the basic terms used in fraud with explanations in the context of the credit card business; section 2 reviews the main types of credit card fraud; section 3 discusses detection techniques; and, finally, the last section concludes the paper.

1. Terms

Credit is a method of selling goods or services without the buyer having cash in hand. A credit card is only an automatic way of offering credit to a consumer. Today, every credit card carries an identifying number that speeds shopping transactions. According to Encyclopedia Britannica (no date), "the use of credit cards originated in the United States during the 1920s, when individual firms, such as oil companies and hotel chains, began issuing them to customers." However, references to credit cards have been made as far back as 1890 in Europe. Early credit cards involved sales directly between the merchant offering the credit and credit card, and that merchant's customer. Around 1938, companies started to accept each other's cards. Nowadays, credit cards allow you to make purchases with countless third parties (Bellis, no date).

In Europe, the most well-known credit card companies are arguably Barclaycard, Citibank, and American Express, offering different types of products depending on their portfolio. Depending on the product offered, the services associated with the card may be different. Interest rate, card fees, exchange rate fee, late payment fee, credit limit, terms and conditions, are elements that can vary from one bank to another and from one product to another.

In the credit card business, fraud occurs when a lender is fooled by a borrower offering him/her purchases, believing that the borrower credit card account will provide payment for this purchase. Ideally, no payment will be made. If the payment is made, the credit card issuer will reclaim the amount paid. Today, with the expansion of e-commerce, it is on the internet that half of all credit card fraud is conducted. Fraudsters have usually connections with the affected business. In the credit card business, it can be an internal party but most likely an external party. As an external party, fraud is committed being a prospective/existing customer or a prospective/existing supplier. Three different profiles can be identified for external fraudsters: the average offender, criminal offender, and organized crime offender (Phua et al., 2005).

Average offenders display random and/or occasional dishonest behavior when there is opportunity, sudden temptation, or when suffering from financial hardship. In contrast, the more risky external fraudsters are individual criminal offenders and organized/group crime offenders (professional/career fraudsters) because they repeatedly disguise their true identities and/or evolve their modus operandi over time to approximate legal forms and to counter detection systems (Phua et al., 2006; Phua et al., 2004).

For many companies sometimes dealing with millions of external parties, it is cost-prohibitive to manually check the majority of the external parties' identity and activities. Indeed, to investigate each suspicious transaction, they incur a direct overhead cost for each of them. If the amount of a transaction is smaller than the cost of the overhead, investigating is not worthwhile even if it seems suspicious (Chan et al., 1999; Oscherwitz, 2005). In order to avoid these overheads and depending on the type of fraud committed, diverse solutions can be implemented.

2. Types of fraud

2.1. Bankruptcy fraud. This section focuses on bankruptcy fraud and advises the use of credit report from credit bureaux as a source of information regarding the applicants' public records as well as a possible implementation of a bankruptcy model. Bankruptcy fraud is one of the most difficult types of fraud to predict. However, some methods or techniques may help in its prevention. Bankruptcy fraud means using a credit card while being insolvent. In other words, purchasers use credit cards knowing that they are not able to pay for their purchases. The bank will send them an order to pay. However, the customers will be recognized as being in a state of personal bankruptcy and not able to recover their debts. The bank will have to cover the losses itself. Usually, this type of fraud loss is not included in the calculation of the fraud loss provision as it is considered a charge-off loss. The only way to prevent this bankruptcy fraud is by doing a pre-check with credit bureaux in order to be informed about the banking history of the customers.

In Germany, for example, some of the most used credit bureaux are SCHUFA and CEG. SCHUFA,

as the leading credit bureau in Germany, offers solutions to its clients over the whole risk management process; 62 million records are stored in their database. Credit bureaux usually report on diverse sectors, such as private banks, savings bank, cooperative banks, special credit institutes etc., and credit card companies.

Usually, the process is as follows: the bank passes an enquiry to the credit bureau. The enquiry includes identification information required by the credit bureau. In a counter party transaction, the credit bureau sends a credit report for this single individual including personal particulars, details of non-compliance with contractual obligations, information from public directories and additional positive information such as repayment of loans according to contract at or before maturity. Some credit bureaux are also able to trace the address of a specific individual, who has moved to an 'unknown' address.

Information in the credit bureau data is gathered from many different sources. Banks, consumer finance companies, credit unions, and collection agencies are some of the entities that periodically report to the credit bureaux. Data are also obtained from state and federal courts on judgments, liens, and bankruptcy filings; the credit bureaux use third parties to gather information. Typically, individual financial companies and others report to the credit bureau every month. The timing of updates from the courts can vary; depending on the size of the court, bankruptcies are usually updated daily. A credit file is created when an individual applies for, or uses, credit or a public record is reported to the credit bureau. Once a credit file is established for an individual, updates are posted on the consumer's credit-seeking behavior, payment and purchase behavior, and any changes to the public records.

The public records section of a credit report contains severe derogatory information on subjects, such as bankruptcy, judgment, garnishment, foreclosure, lien, and collection accounts. Bankruptcy information, obtained from the federal courts, covers all 'chapters' of the bankruptcy code and details whether the court discharged or dismissed the bankruptcy petition, and the amount of the bankruptcy. Judgment, foreclosure, and lien records from both state and federal courts list the amounts in dispute and whether a judgment or lien was satisfied or released. Collection items are posted in the public record section if they are collected by a third-party collections agency. The amount collected by the original credit-granting firm may also be reported in the trade-line section of the file (Thomas et al., 2002). Items are kept in the public records' section of the credit file for varying lengths of time, depending on the event and the credit bureau.

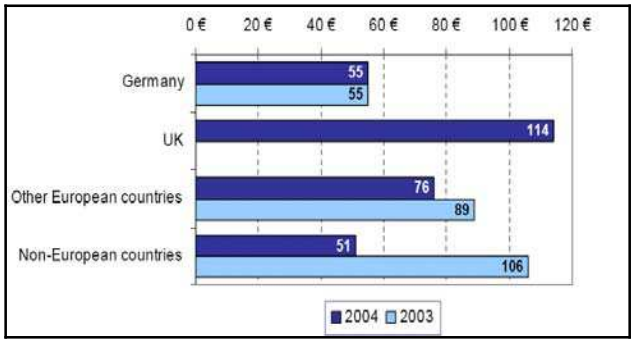
Once the bank has received the credit report from the credit bureau, the bank is free to decide its policy in terms of rejection criteria. On the one hand, the bank can decide to adopt a conservative behavior and to reduce the access to its product to a certain type of customer. On the other hand, the bank can allow itself to be exposed by accepting such a high risk in terms of credit and fraud. This decision depends on the type of business and thus, portfolio, the bank is willing to manage. The source of criteria that have a significant impact in identifying insolvency cases will be collection and court information.

Other methods to detect bankruptcy fraud are few. However, Foster & Stine (2004) presented a model to predict personal bankruptcy among users of credit card. The paper described a model based on standard regression techniques. The method is based on a step wise regression with some modifications. Firstly, the model included interactions and indicator functions to capture respectively non-linearities and missing values. Secondly, it was based on modern decision theoretic variable selection criteria. Thirdly, the method used to predict the standard error was rather conservative to deal with heteroscedastic data (Foster & Stine, 2004). Combining a model to predict bankruptcy with credit reports can be suggested as a solution against bankruptcy fraud.

2.2. Theft fraud/counterfeit fraud. This section focuses on theft fraud and counterfeit fraud, which are related to each other. Theft fraud means using a card that is not yours. The perpetrator will steal the card of someone else and use it as many times as possible before the card is blocked. The sooner the owner will react and contact the bank, the faster the bank will take measures to stop the thief. Similarly, counterfeit fraud occurs when the credit card is used remotely; only the credit card details are needed. At one point, one will copy your card number and codes and use it via certain web-sites, where no signature or physical cards are required. Recently, Pago, one of the leading international acquiring & payment service providers, reveals in its Pago Report (2005) that credit card fraud is a growing threat to businesses selling goods or services through the internet. On-line merchants are at risk because they have to offer their clients payment by credit card. In cases where fraudsters use stolen or manipulated credit card data the merchant loses money because of so-called "charge-backs"[2]. Note that charge-backs are generated if credit card holders object to items on their monthly credit card

statements because they were not responsible for the purchase transactions.

According to the Pago Report (2005), although the average charge-back ratio in European e-commerce seems to be quite low, at only 0.83 percent, significant concerns are revealed in detailed analysis. The share of charge-backs, for instance, resulting from manipulated credit card data has risen from just over 4 per cent in 2003 to more than 7 per cent in 2004. This is presumably due to the overall increase in organized credit card fraud. Yet, according to the Pago Report (2005), the relationship between charge-back ratio and shopping cart value has deteriorated too; whereas the charge-back ratio for transactions of less than 10 Euros is only 0.28 per cent, and 3.71 per cent of transactions over 500 Euros end up as a chargeback. Interestingly, the charge-back ratio for consumers from Germany, at 0.31 per cent, is much lower than that for all other European consumers.



Source: Pago e-Transaction Services (Pago Report, 2005). This is cited in the European e-Business Market Watch. ICT Security, e-Invoicing and e-Payment Activities in European Enterprises, Special Report, September, 2005.

Fig. 4. Average transaction values in European shops by consumer origin

Consumer behavior in making e-payments has changed from 2003 to 2004 as shown in Figure 4. On the one hand, the average transaction values for German consumers has not changed, at €55, while the average value generated from the rest of Europe by purchases from consumers was lower in 2004 than in 2003, at €79 and €89, respectively. On the other hand, non-Europeans have the highest average value, at €106 in 2003, while it was the lowest value in 2004, at €51; they were overtaken by UK shoppers, who generated an average value of €114, the highest in 2004. Therefore, the average transaction value has changed significantly from 2003 to 2004.

A conclusion that could result from those statistics could be that the German credit card market is less affected by credit card fraud than the rest of Europe. However, one could consider that it is a matter of time before the first signs appear. Detecting this type of fraud is a must in the credit card business. Even though the task is not easy, this type of fraud can be detected, thanks to reports such as 'over limit' reports. 'Over limit' reports provide a daily list of customers that have exceeded their credit limit. A certain degree of tolerance may be accepted. For the credit card listed, the customers are contacted and if they do not react, the card is blocked. Other reports are vintage reports which identify delinquent customers, i.e. transaction reports which identify suspicious transactions.

A fraudulent transaction is difficult to detect and to define. Nevertheless, ATM transactions of large amounts are suspicious and demand contact with the customer. Purchases of goods for a larger amount than normal will also be notified to the customer as well as abnormal overseas spending patterns. Fraudulent transactions are usually impossible to prevent as they occur in a really short period of time. However, once a card is identified, the card is blocked.

2.3. Application fraud. Application fraud is when someone applies for a credit card with false information. To detect application fraud, the solution is to implement a fraud system that allows identifying suspicious applications. To detect application fraud, two different situations have to be distinguished: when applications come from a same individual with the same details, the so-called duplicates, and when applications come from different individuals with similar details, the so-called identity fraudsters.

In most banks, to be eligible for a credit card, applicants need to complete an application form. This application form is mandatory except for social fields. The information required includes identification information, location information, contact information, confidential information and additional information. Recurrent information available would be for identification purposes, such as the full name and the date of birth. The applicant would inform the bank about his/her location details: the address, the postal code, the city and the country. The bank would also ask for contact details, such as e-mail address, land-line and mobile phone numbers. Confidential information will be the password. In addition, the gender will be given. All those characteristics may be used while searching for duplicates.

To identify the so-called *duplicates*, cross-matching techniques are in common use. Rather than using statistical techniques, another method easy to implement is cross-matching. For instance, simple queries that give fast results are to cross-identify information with location details. Examples would

be "last name and date of birth and postal code and address" or "last name and address and e-mail and gender". By those queries, individuals with more than one card are identified. Those are quite simplistic queries but will remove most duplicates from the system. Note that duplicates may usually be genuine. Customers can reapply filling in a new address or spelling differently in one of the fields. By contrast, identity crime, as it is named, is perpetrated by real criminals filling wrong application data consciously.

Phua et al. (2006) explain that application fraud, a manifestation of *identity crime*, occurs when application form(s) contain plausible, and synthetic (identity fraud), or real but stolen identity information (identity theft). According to ID Analytics (2004), and based on 300 million opened fraudulent account applications, 88% of those fraudulent accounts were opened by using identity fraud techniques. According to the same study, identity fraud counts for three quarters of the total loss generated by identity crime.

Cross-matching works on the premise that once someone has been successful in perpetrating a fraud, they will attempt to repeat their success with another lender; cross-matching can then detect identity crime. Therefore, some lenders have begun to send details of applications into a central data bank, where some matching algorithms operate to identify common features. Many matching rules will be applied and it is acknowledged that many false-positive cases will be identified (Thomas et al., 2004). Cross-matching techniques have been recommended by Phua et al. (2006), who develop a technique for generating numeric suspicious scores on credit applications based on implicit links to each other. The purpose is to derive an accurate suspicion score for all incoming current or new applications in real time (Phua et al., 2006).

Solutions: to improve the pair-wise matching technique, the authors combined pair-wise matching and suspicious behavior. For instance, considering the number of applications is one way to define a suspicious behavior. Another criterion is the number of active cards corresponding to the combination of fields. The issue is to define relevant fields. The design of pair-wise matching for dynamic applications has to be effective and efficient (Phua et al., 2006). In the credit card business, one key element is the address. It is where the card will be sent. The only way for fraudsters to get several cards is to pick them at one address or several addresses. If the cards are sent to different addresses under different names, application fraud detection is rather difficult. Those fraudsters will be identified later on once they use the cards and behave according to their profile (over their limit, off-line transactions, abnormal transaction, delinquency status, etc.). However, those giving the same address under different names can be identified.

A proposal which has been tested is to pair-wise the number of applications, the address, the postal code and the number of active cards. In order to pair-wise correctly, a first step is to "clean" the applications. For instance, consider a German address; the system has to be developed in a way that "Hauptstr.29" will be pair-wised with "Hauptstrasse29" or that "Heidestrasse85" will be pair-wised with "Heidestr.85". The second step is similar for the postal code; "77756" has to pair-wised with "D-77756". This pre-work on the data is fundamental to prevent fraud applications. Fraudsters will always try to find new ways to beat the system, which is why those control checks have to be up-dated as often as possible.

A suggestion is to have three levels of risk for the different fraudulent behavior: level 1: "high risk" – this group contains all individuals with the same address and postal code and at least one active card listed 10 or more times; level 2: "medium risk" – this group contains all individuals with the same address and postal code and at least one active card listed at least 5 times but less than 10 times; and level 3: "low risk" – this group contains all individuals with the same address and postal code and at least one active card listed at least twice but less than 5 times.

Applications: the technique was applied to a full application data set supplied by a German bank in 2006. For banking secrecy reasons, only a summary of the results obtained is presented below. After applying this technique, the level 1 list contains a few cases but with a high probability of being fraudsters. All individuals mentioned in this list had their cards closed to avoid any risk due to their high risk profile. The situation is more complex for the other list. The level 2 list is still restricted enough to be checked on a case by case basis. Credit and collection officers considered that half of the cases in this list could be considered as suspicious fraudulent behavior. For the last list and the largest, the work is fairly heavy. Less than one third of those customers are suspicious. In order to maximize the time efficiency and the overhead costs, an option is to include a new element in the query; this element can be the five first digits of the phone numbers, the email address, and the password, for example, those new queries can be applied to the level 2 list and level 3 list.

This system is not aimed to provide a 100% solution, but it is a first step to control application fraud. Professional fraudsters will, of course, not be identified by such techniques but amateurs will. Another solution that has been investigated is a web service for credit card detection based on collaboration amongst different banks (Chiu & Tsai, 2004; Fan, 2004). Those banks share their information about fraudsters. This idea is interesting but difficult to implement as it requires the cooperation of different banks, for banks may not be willing to share their information due to competition in the market, and for legal reasons, such as data protection law.

Fraudsters, responsible for identity crime that will remain in the system after this first check, are prone to commit behavioral fraud and, therefore, will be identified further on thanks to a fraud scorecard.

2.4. Behavioral fraud. Behavioral fraud occurs when details of legitimate cards have been obtained fraudulently and sales are made on a 'cardholder present' basis. These sales include telephone sales and e-commerce transactions, where only the card details are required (Bolton & Hand, 2002). Behavioral fraud can be detected by implementing a fraud scorecard predicting which customers are likely to default. Traditional credit scorecards are used to detect customers who are likely to default, and the reasons for this may include fraud (Bolton & Hand, 2002). Regarding the process, using scoring for fraud prevention is similar to any other use, including profit, default, and collection. The score reflects experience of past cases, and the result is a binary outcome: a genuine customer or a fraudster.

The key difference is that professional fraudsters will make their application look very genuine. Therefore, some scoring developments for fraud prevention have not proved worthwhile because they are unable to differentiate between genuine applications and fraudulent applications. On the other hand, if one uses scoring as a fraud check in addition to using a different scoring model as a credit risk check, any improvement will add value. However, the value of this additional check relies on it not presenting too many false-positive cases (Thomas et al., 2004). To detect fraudulent applications is possible once they have gone through the system and have been bank customers for a certain time. To build a scorecard, it is important to define what the profile of a fraudulent customer is, and especially the cardholder level profiles encapsulating normal transaction patterns, such as frequency of use, typical value range, types of goods purchased, transaction types, retailer profiles, cash usage, balance and payment histories, overseas spending patterns and daily, weekly, monthly and seasonal patterns (Thomas et al., 2004; Siddiqi, 2006).

With application fraud, fraudsters will only be detected while accounts are sent out or repayment dates begin to pass. Time delays are the main issues with suspicious scorecards. Generally, a bank would need a 12-month period to collect enough relevant data to build this model and to have such a model fully implemented (Thomas et al., 2002).

3. Detection techniques

3.1. Decision tree. The idea of a similarity tree using decision tree logic has been developed. A similarity tree is defined recursively: nodes are labelled with attribute names, edges are labelled with values of attributes that satisfy some condition and 'leaves' that contain an intensity factor which is defined as the ratio of the number of transactions that satisfy these condition(s) over the total number of legitimate transaction in the behavior (Kokkinaki, 1997). The advantage of the method that is suggested is that it is easy to implement, to understand and to display. However, a disadvantage of this system is the requirements to check each transaction one by one. Nevertheless, similarity trees have given proven results [Fan et al. (2001) also worked on decision trees and especially on an inductive decision tree in order to establish an intrusion detection system, for another type of fraud].

3.2. Genetic algorithms and other algorithms. Algorithms are often recommended as predictive methods as a means of detecting fraud. One algorithm that has been suggested by Bentley et al. (2000) is based on genetic programming in order to establish logic rules capable of classifying credit card transactions into suspicious and non-suspicious classes. Basically, this method follows the scoring process. In the experiment described in their study, the database was made of 4,000 transactions with 62 fields. As for the similarity tree, training and testing samples were employed. Different types of rules were tested with the different fields. The best rule is the one with the highest predictability. Their method has proven results for real home insurance data and could be one efficient method against credit card fraud.

Chan et al. (1999) also developed an algorithm to predict suspect behavior. The originality of their research is that the model is evaluated and rated by a cost model, whereas other studies use evaluation based on their prediction rate/the true positive rate and the error rate/the false negative rate. Wheeler &

Aitken (2000) developed the idea of combining algorithms to maximize the power of prediction. In their article, they present different algorithms: diagnostic algorithms, diagnostic resolution strategies, probabilistic curve algorithms, best match algorithms, negative selection algorithms, and density selection algorithms. They conclude from their investigation that neighborhood-based and probabilistic algorithms have been shown to be appropriate techniques for classification, and may be further enhanced using additional diagnostic algorithms for decision-making in borderlines cases, and for calculating confidence and relative risk measures.

3.3. Clustering techniques. Bolton & Hand (2002) suggest two clustering techniques for behavioral fraud. The peer group analysis is a system that allows identifying accounts that are behaving differently from others at one moment in time whereas they were behaving the same previously. Those accounts are then flagged as suspicious. Fraud analysts have then to investigate those cases. The hypothesis of the peer group analysis is that if accounts behave the same for a certain period of time and then one account is behaving significantly differently, this account has to be notified. Break-point analysis uses a different approach. The hypothesis is that if a change of card usage is notified on an individual basis, the account has to be investigated. In other words, based on the transactions of a single card, the break-point analysis can identify suspicious behavior. Signals of suspicious behavior are a sudden transaction for a high amount, and a high frequency of usage.

Table 1. A summary of studies investigating different statistical techniques in credit card fraud

Study	Country	Method	Details
Aleskerov et al. (1997)	Germany	Neural networks	Card-watch
Bently et al. (2000)	UK	Genetic programming	Logic rules and scoring process
Bolton & Hand (2002)	UK	Clustering techniques	Peer group analysis and break point analysis
Brause et al. (1999a)	Germany	Data mining techniques & neural networks	Data mining application combined probabilistic and neuro-adaptive approach
Chan et al. (1999)	USA	Algorithms	Suspect behavioral prediction
Dorronsoro et al. (1997)	Spain	Neural networks	Neural classifier
Ezawa & Norton (1996)	USA	Bayesian networks	Telecommunication industry
Fan et al. (2001)	USA	Decision tree	Inductive decision tree
Ghosh & Reilly (1994)	USA	Neural networks	FDS (fraud detection system)
Kim & Kim (2002)	Korea	Neural classifier	Improving detection efficiency and focusing on bias of training sample as in skewed distribution. To reduce “mis-detections”.
Kokkinaki (1997)	Cyprus	Decision tree	Similarity tree based on decision tree logic
Leonard (1995)	Canada	Expert system	Rule-based Expert system for fraud detection (fraud modelling)
Maes et al. (2002)	USA	Bayesian networks & neural networks	Credit card industry, back-propagation of error signals
Quah & Sriganesh (2007)	Singapore	Neural networks	Self-Organizing Map (SOM) through real-time fraud detection system
Wheeler & Aitken (2000)	UK	Combining algorithms	Diagnostic algorithms; diagnostic resolution strategies; probabilistic curve algorithm; best match algorithm; negative selection algorithms; density selection algorithms and approaches
Zaslavsky & Strizkak (2006)	Ukraine	Neural networks	SOM, algorithm for detection of fraudulent operations in payment system

3.4. Neural networks. Neural networks are also often recommended for fraud detection. Dorronsoro et al. (1997) developed a technically accessible on-line fraud detection system, based on a neural classifier. However, the main constraint is that data need to be clustered by type of account. Similar concepts are: Card watch (Aleskerov et al., 1997); Back-propagation of error signals (Maes et al., 2002); FDS (Ghosh & Reilly, 1994); SOM (Quah & Sriganesh, 2008; Zaslavsky & Strizkak, 2006); improving detection efficiency "mis-detections" (Kim & Kim, 2002). Data mining tools, such as 'Clementine' allow the use of neural network technologies, which have been used in credit card fraud (Brause et al., 1999a; Brause et al., 1999b).

Bayesian networks are also one technique to detect fraud, and have been applied to detect fraud in the telecommunications industry (Ezawa & Norton, 1996) and also in the credit card industry (Maes et al., 2002). Results from this technique are optimistic. However, the time constraint is one main disadvantage of such a technique, especially compared with neural networks (Maes et al., 2002). Furthermore, expert systems have also been used in credit card fraud using a rule-based expert system (Leonard, 1995).

However, no matter the statistical techniques chosen, the fraud detection system will need to fulfil some conditions. As the number of fraudulent transactions is much less than the total number of transactions, the system will have to handle skewed distributions of the data. Otherwise, the data need to be split into training samples, where the distribution is less skewed (Chan et al., 1997). The system has to be accurate with actual performing classifiers and to be capable of handling noise in the data; a suggested solution is to clean the data (Fawcett & Provost, 1997). The system should also be able to handle overlaps; fraudulent transactions may be similar to normal transactions. As fraudsters reinvent new techniques constantly, the system needs to be adaptive and evaluated regularly. A cost profit analysis is also a must in fraud detection to avoid spending time on uneconomic cases.

For new issuing banks, a proposal would be to rely on credit bureaux score in order to control fraud and avoid expected losses. Even though those scorecards are primarily used to predict defaulting customers, one could use them to detect fraud, since fraud and default are strongly correlated. Generic scoring systems are typically based on a sample from the past experiences of several lenders. Generic systems are sold to creditors who believe they will find them useful. The systems are often available on a transaction as well as a purchase basis (Thomas et al., 2004).

The most dominant generic models are those available through the major credit bureaux, and influence most credit decisions made by major creditors. A credit bureaux score may be included in the credit report of the individual or as a stand-alone product. Each bureau has its own models, and the competition is intense. Generic models were developed by scoring vendors working with credit bureau development staff. Though only information from a single credit bureau is used in model development, sample sizes typically range from the hundreds of thousands to over a million files. In general, the predictive powers of the generic bureau models are outstanding, and comparable with those of customized models.

Generally, a credit bureau scorecard is developed into a model for forecasting the payment behavior of an applicant using the characteristic data available for that applicant. Typically, credit bureau scores are based on external data which have been calibrated in such a way that, with regard to age and gender, for example, they reflect the population. The scorecard is also established with variables, such as risk indicator, social status, family status, type of house and post code.

For this purpose, Fair Isaac, for example, produces software for detecting credit card fraud. Their solution is based on neural network techniques processing transactional, cardholder, and merchant data to detect fraudulent activity. Experian also has developed its own solution called Hunter. Pago fraud screening is also one tool used for fraud prevention. However, those solutions are often costly, yet unaffordable for small banks.

It can be argued that one ethical problem that arises from the use of detection techniques, to predict fraudulent and genuine customers, is that a technique may predict some customers as genuine, when actually they are fraudulent, and other customers as fraudulent, when actually they are genuine. In terms of justice, these errors should be minimized. However, from the bank's own perspective the cost of predicting as genuine a customer who is actually fraudulent is much higher than the cost to the bank of predicting as fraudulent a customer who is actually genuine. In the latter case the bank loses the opportunity cost of the associated profit margin that would have been earned. However, in the former case the bank loses the capital value of the loan as well as the interest. To operate in the best interests of the bank's shareholders its objective should be to minimize the misclassification costs rather than to minimize the propensity to incorrectly classify customers as fraudulent or genuine. Yet, it would be unethical to

reject genuine customers that happened to have the same array of characteristics as those of fraudulent customers.

Conclusion

Clearly, credit card fraud is an act of criminal dishonesty. This article has reviewed recent findings in the credit card field. This paper has identified the different types of fraud, such as bankruptcy fraud, counterfeit fraud, theft fraud, application fraud and behavioral fraud, and discussed measures to detect them. Such measures have included pair-wise matching, decision trees, clustering techniques, neural networks, and genetic algorithms.

From an ethical perspective, it can be argued that banks and credit card companies should attempt to detect all fraudulent cases. Yet, the unprofessional fraudster is unlikely to operate on the scale of the professional fraudster and so the costs to the bank of their detection may be uneconomic. The bank would then be faced with an ethical dilemma. Should they try to detect such fraudulent cases or should they act in shareholder interests and avoid uneconomic costs?

As the next step in this research program, the focus will be upon the implementation of a 'suspicious' scorecard on a real data-set and its evaluation. The main tasks will be to build scoring models to predict fraudulent behavior, taking into account the fields of behavior that relate to the different types of credit card fraud identified in this paper, and to evaluate the associated ethical implications. The plan is to take one of the European countries, probably Germany, and then to extend the research to other EU countries.

References

1. Aleskerov, E., Freisleben, B. & B Rao. 1997. 'CARDWATCH: A Neural Network-Based Database Mining System for Credit Card Fraud Detection', Proc. of the IEEE/IAFE on *Computational Intelligence for Financial Engineering*, 220-226.
2. Anderson, R. 2007. *The Credit Scoring Toolkit: theory and practice for retail credit risk management and decision automation*. New York: Oxford University Press.
3. APACS, Association for Payment Cleaning Services, no date. Card Fraud Facts and Figures Available at: http://www.apacs.org.uk/resources_publications/card_fraud_facts_and_figures.html (Accessed: December 2007).
4. Bellis, M. no date. Who Invented Credit Cards-the History of Credit Cards? Available at: http://inventors.about.com/od/cstartinventions/a/credit_cards.htm (Accessed: October 2008).
5. Bentley, P., Kim, J., Jung. G. & J Choi. 2000. Fuzzy Darwinian Detection of Credit Card Fraud, Proc. of 14th Annual Fall Symposium of the Korean Information Processing Society.
6. Bolton, R. & Hand, D. 2002. 'Statistical Fraud Detection: A Review'. *Statistical Science*, 17; 235-249.
7. Bolton, R. & Hand, D. 2001. Unsupervised Profiling Methods for Fraud Detection, Credit Scoring and Credit Control VII.
8. Brause R., Langsdorf T. & M Hepp. 1999a. Credit card fraud detection by adaptive neural data mining, Internal Report 7/99 (J. W. Goethe-University, Computer Science Department, Frankfurt, Germany).
9. Brause, R., Langsdorf, T. & M Hepp. 1999b. Neural Data Mining for Credit Card Fraud Detection, Proc. of 11th IEEE International Conference on Tools with Artificial Intelligence.
10. Caminer, B. 1985. 'Credit card Fraud: The Neglected Crime'. *The Journal of Criminal Law and Criminology*, 76; 746-763.
11. Chan, P., Fan, W. Prodromidis, A. & S Stolfo. 1999. 'Distributed Data Mining in Credit Card Fraud Detection'. *IEEE Intelligent Systems*, 14; 67-74.
12. Chan, P., Stolfo, S., Fan, D., Lee, W. & A Prodromidis. 1997. Credit card fraud detection using meta learning: Issues and initial results, Working notes of AAAI Workshop on AI Approaches to Fraud Detection and Risk Management.
13. Chepaitis, E. 1997. 'Information Ethics Across Information Cultures'. *Business Ethics: A European Review*, 6: 4, 195-199.
14. Chiu, C. & Tsai, C. 2004. A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection. Proc. of 2004 IEEE International Conference on e-Technology, e-Commerce and e- Service.
15. Clarke, M. 1994. 'Fraud and the Politics of Morality'. *Business Ethics: A European Review*, 3: 2, 117-122.
16. Dorronsoro, J. Ginel, F. Sanchez, C. & C Cruz. 1997. 'Neural Fraud Detection in Credit Card Operations'. *IEEE Transactions on Neural Networks*, 8; 827-834.
17. Encyclopedia Britannica, no date. Credit Card. Available at: http://www.britannica.com/eb/article-9026818/credit-card (Accessed: October 2008).
18. Euromonitor International, 2006. Financial cards in Germany Available at: http://www.euromonitor.com/Financial_Cards_in_Germany (Accessed: November 2006).
19. European e-Business Market Watch. 2005. ICT Security, e-Invoicing and e-Payment Activities in European Enterprises, Special Report, September.
20. Ezawa, K. & Norton, S. 1996. 'Constructing Bayesian Networks to Predict Uncollectible Telecommunications Accounts'. *IEEE Expert*, October; 45-51.
21. Fan, W. 2004. Systematic Data Selection to Mine Concept-Drifting Data Streams, Proc. of SIGKDD04; 128-137.

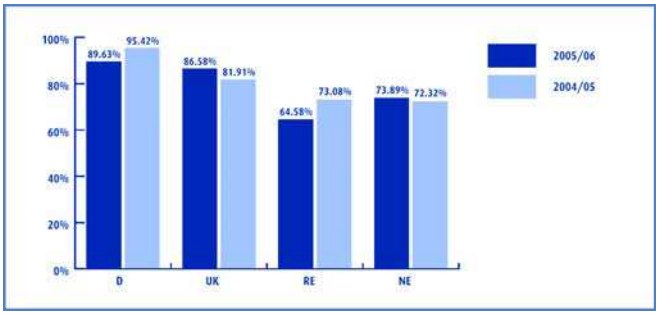
22. Fan, W., Miller, M., Stolfo, S., Lee, W. & P Chan. 2001. Using Artificial Anomalies to Detect Unknown and Known Network Intrusions, Proc. of ICDM01; 123-248.
23. Fawcett, T. & Provost, F. 1997. 'Adaptive Fraud Detection'. *Data Mining and Knowledge Discovery*, 1; 3.
24. Foster, D. & Stine, R., 2004. 'Variable Selection in Data Mining: Building a Predictive Model for Bankruptcy'. *Journal of American Statistical Association*, 99; 303-313.
25. George, E. 1992. 'Ethics in Banking'. *Business Ethics: A European Review*, 1:3, 162-171.
26. Ghosh, S. & Reilly, D. 1994. 'redit Card Fraud Detection with a Neural-Network, Proc. of 27th Hawaii International Conference on Systems Science, 3; 621-630.
27. Gichure, C. 2000. 'Fraud and the African Renaissance'. *Business Ethics: A European Review*, 9:4, 236-247.
28. ID Analytics. 2004. Identity 2004: The Identity Risk Management Conference.
29. Kim, M. & Kim, T. 2002. A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection, Proc. Of IDEAL 2002, 378-383.
30. Kokkinaki, A. 1997. On Atypical Database Transactions: Identification of Probable Frauds using Machine Learning for User Profiling, Proc. of IEEE Knowledge and Data Engineering Exchange Workshop; 107-113.
31. Leonard K. 1995. 'The development of a rule based expert system model for fraud alert in consumer credit'. *European Journal of Operational Research,* 80; 350-356.
32. Maes, S., Tuyls, K., Vanschoenwinkel, B. & B Manderick. 2002. Credit Card Fraud Detection using Bayesian and Neural Networks, Proc. of the 1st International NAISO Congress on Neuro Fuzzy Technologies.
33. Molyneaux, D. 2007. 'Two case study scenarios in banking: a commentary on *The Hutton Prize for Professional Ethics*, 2004 and 2005'. *Business Ethics: A European Review*, 16:4, 372-386.
34. Oscherwitz, T. 2005. Synthetic Identity Fraud: Unseen Identity Challenge, Bank Security News, 3; 7.
35. Pago-Report. 2005. The development of E-commerce sectors, ©Pago eTransaction Services GmbH.
36. Pago-Report. 2007. Trends in Consumer Purchasing and Payment Behaviour in selected E-commerce Industries, ©Pago eTransaction Services GmbH.
37. Phua, C., Alahakoon, D., & V Lee. 2004. 'Minority Report in Fraud Detection: Classification of Skewed Data'. *ACM SIGKDD Explorations: Special Issue on Imbalanced Data Sets*, 6; 50-59.
38. Phua, C., Gayler, R., Lee, V., & K Smith. 2006. On the Approximate Communal Fraud Scoring of Credit Applications, *Proceedings of Credit Scoring and Credit Control IX*.
39. Phua, C., Lee, V., Smith, K. and Gayler, R., 2005. A Comprehensive Survey of Data Mining-based Fraud Detection Research., Artificial Intelligence Review.
40. Quah T. S, & Sriganesh M. 2008. 'Real-time credit card fraud using computational intelligence'. *Expert Systems with Application*, 35:4, 1721-1732.
41. Siddiqi, N. 2006. *Credit Risk Scorecards: Developing And Implementing Intelligent Credit Scoring*, John Wiley & Sons, USA.
42. Thomas, L.C., Edelman, D.B., & J.N Crook. 2002. *Credit Scoring and its Applications*, SIAM Monographs on Mathematical Modeling and Computation, Philadelphia.
43. Thomas, L.C., Edelman, D.B., & J.N Crook. 2004. *Readings in Credit Scoring: Foundations, Developments, and Aims*, Oxford University Press, USA.
44. Wheeler, R. & Aitken, S. 2000. 'Multiple Algorithms for Fraud Detection'. *Knowledge-Based Systems*, 13; 93-99.
45. Zaslavsky V. & Strizhak A. 2006. 'Credit card fraud detection using self-organizing maps'. *Information and Security*, 18; 48-63.

Notes

1. All the figures in this paper are used with permission of Pago e-Transaction Services GmbH, October 2007.
2. For more details see Appendix A: 'Success rates and charge-back ratios' (Pago Report, 2007).

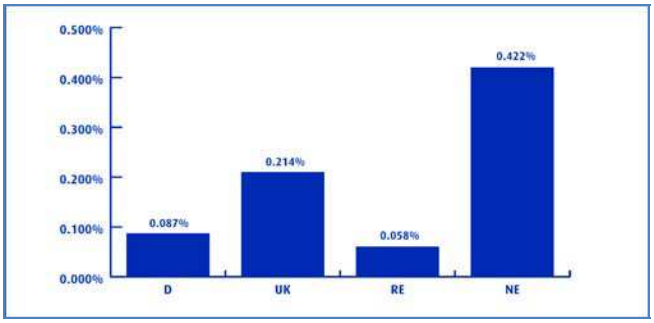
Appendix A. Success rates and chargeback ratios

It can be shown from Figure A.1 that success rates have deteriorated significantly in Germany (D), and the same for consumers in the rest of Europe (RE), except for rates for UK consumers and consumers outside Europe (NE) which are higher than previously. The success rate for credit card holders from the rest of Europe is less than 65%*.



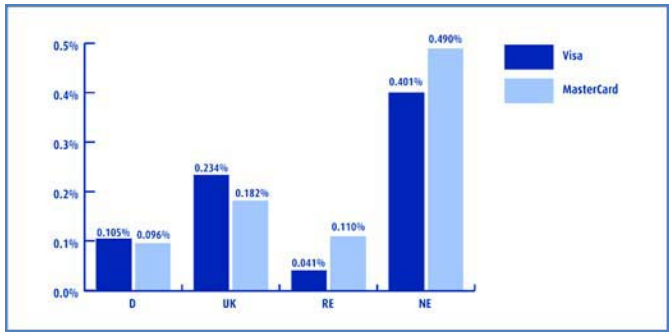
Source: Pago e-Transaction Services GmbH, Pago Report, 2007.

Fig. A.1. Success rates for credit card transactions by consumer country, in all shops



Source: Pago e-Transaction Services GmbH, Pago Report, 2007.

Fig. A.2. Charge-back ratios for credit card transactions by consumer country, in all shops



Source: Pago e-Transaction Services GmbH, Pago Report, 2007.

Fig. A.3. Charge-back ratios for credit card transactions by credit card brand and consumer country, in all shops

As shown in Figure A.2, the overall average charge back ratio is around 0.33%. This ratio for transactions with German consumers is tremendously low, at 0.087%. Similarly, this ratio is low for consumers in the rest of Europe, at 0.058%. For consumers outside Europe and for UK consumers, the ratios are 0.422% and 0.214%, respectively. For consumers from outside Europe the chargeback ratio fell but is still the highest between all groups. It should be emphasized that this situation differs from 2004; in 2004 no consumer group achieved a chargeback ratio less than 0.10%. As a conclusion, non-payment risks no longer present a significant problem for e-commerce.

The non-payment risk and credit card brand vary depending on different groups as shown in Figure A.3. For users from Germany and the rest of Europe, it is quite clear that both Visa and MasterCard ratios are quite low compared with the same ratios for users outside Europe and even for UK users.

* This is the worst value ever calculated in Pago Reports.