Fraudulent accounts in collections: improve detection and reduce collector workload

An Experian briefing paper

Experian™

September 2010

1. The inter-relationship of fraud and collections

The fraud and collections functions have a natural affinity, one that is often not recognised in organisations that frequently have these as two distinct and separate operations. With current emphasis moved away from customer acquisition, there is a renewed focus on the efficient and effective management of delinquent customer accounts. Organisations need to ensure they are focused on accounts where revenues can be maximised and outstanding debts are likely to be recovered.

But what if some of these delinquent accounts are fraudulent? Fraudsters, whether committing first or third party, have no intention or no ability to pay, so these accounts will quickly track through to collections. Collections cases can contain a significant proportion of frauds, which would be managed through various stages, incurring costs and time attempting to contact customers who are fraudsters, or who are not responsible for the debt due to identity theft.

Taking these fraudulent cases out of the collections process allows resources to be concentrated on accounts that will deliver a return. This should also be part of a closed feedback loop where the fraud team uses this intelligence to enhance protection to prevent similar accounts being undetected in the future.

The key objective is to identify accounts with a high probability of fraud in the first 30 days after default. However, within some organisations, internal politics may cause conflicting interests between functions. If the collections team can pass cases to fraud it removes them from its bad debt provision; equally, fraud teams are under pressure to not increase their fraud levels and will not, therefore, encourage cases to be assigned to fraud.

Fraud is a shared problem and collectors need to have the ability to correctly determine the action to be taken - to pursue the debt or pass it to the relevant area. The organisation needs to have established, effective processes and available resource for dealing with these accounts, so that appropriate action can be taken when required.

This paper explores how this can be achieved, outlining the practical steps that can be taken to integrate fraud and collections systems and create a joined up approach. The result is reduced collections costs and write-offs, as well as improved fraud protection.

Fraud is a shared problem and collectors need to have the ability to correctly determine the action to be taken.

2. How much of the collections problem is fraud?

In an ideal world, all fraudsters would be identified and stopped at the point of application and therefore fraudulent accounts would not be seen in the collections operation. However in the real world as the sophistication of fraudsters increases, the application and transaction fraud protection systems cannot provide 100% protection against fraudulent activities.

2.1 Types of fraud

Fraudsters will use false or stolen identities to open new accounts and access goods and services. This 'hard' fraud is more serious than first party fraud, where applicants will falsify information on the application form to enhance their likelihood of acceptance and a better offer.

In addition to fraudsters coming through the application fraud process, there is the growing issue of open account fraud, where fraudsters using stolen or false identities takeover accounts and extract the maximum value. Another form of this is 'bust-out' or 'sleeper fraud' where an account will be opened or taken over and run over a period of time to maximise the value of the 'bust-out' that will inevitably come.

2.2 Fraud protection

Nearly every organisation will have application and transaction fraud systems in place; however the sophistication of some fraud will enable it to go undetected through the application process, especially if the fraudster is using a genuine, credit-worthy identity.

Transaction fraud monitoring focuses on patterns of behaviour and sets limits, mechanisms which are designed to spot unusual transactions and will highlight both undetected application fraud and account take over. However fraudsters are quick to exploit the 'rules' of these systems and evade detection.

2.3 The first sign of a problem

As a result, for a significant proportion of accounts, the first sign that there is any problem is when the first or subsequent payments are missed and the account goes into collections.

One simple equation used to determine the size of the fraud problem is to consider:

First payment defaults, **plus**
Accounts that default within first few months, and those ‘gone away’, plus
Accounts with 3 missed payments within first 6 payments due period, equals
The size of the fraud problem

This figure won’t include sleeper and bust-out fraud as these frauds will demonstrate ‘good’ customer behaviour for the first 6-12 months in order to gain access to additional funds or services before the account goes bad.

Estimating the size of the problem

Experian research suggests that the number of accounts that are fraudulent is dependant on the industry and organisation, but estimates the percentage of accounts in collections which are fraud as:

Mobile telecommunications up to 15%
In a typical portfolio with 100,000 new delinquent accounts per month and an average bill of £70 this could be up to £12 million in losses per year

Credit cards up to 4%
In a typical portfolio with 100,000 new delinquent accounts per month and an average bill of £500 this could be up to £2.4 million in losses per year

Personal loans up to 1.5%
In a typical portfolio with 50,000 new delinquent accounts per month and an average loan value of £1000 this could be up to £750,000 in losses per year

Mortgage up to 1%
In a typical portfolio with 10,000 new delinquent accounts per month and an average loan value of £150,000 this could be up to £1.5 million in losses per year

However it is likely that these figures under-report the level of fraud as much of it will be written off as bad debt. Indeed some estimates for the telecom industry put fraud in bad debt as high as 30-35%.

..it is likely that these figures under-report the level of fraud as much of it will be written off as bad debt.

3. Detecting fraud in collections

Every case entering collections will have an assessment and strategy assigned according to the customer's circumstances. One objective of this process will be to determine the reason for delinquency – is there an indication of a change in the customer's situation or a worsening credit risk or, in the case of first payment default, is this administrative error or merely a lazy payer?

In a sophisticated collections operation, the customer screening can be automated and the highest risk cases passed straight through to a referrals team without being seen by a collector. Alternatively, a specialist in the collections team could review the cases and refer as appropriate.

3.1 Reassess fraud risk

As an integrated part of the collections strategy process all accounts should be re-assessed as to their fraud risk. This should screen accounts against all available data sources, both from the company and from national sources, and highlight where the account information matches information which could indicate suspicious activity. This should include any information matching that on previously written-off accounts as this could indicate links which are suspicious.

Information sources should include:

- Internal fraud lists
- Previously written-off accounts
- Application fraud database
- Transaction fraud database
- External fraud databases – including CIFAS and National Hunter
- Mortality files
- Other external fraud indicators such as Experian's Suspicious Activity Score

Scoring models can then assess the likelihood of the account being fraudulent based on the matches between the data.

These checks will have been carried out at the start and during the relationship so the collections check should be an integral part of the fraud process.

However, this should continue to be carried out regularly as the information is continually updated and new data may be found. In some cases the combination of suspicious data (which may not have been strong enough to prompt a decline at origination), combined with default data will be enough to investigate rather than collect.

3.2 Use behavioural information

Accounts may enter collections as a result of account take over or fraudulent accounts that have been run as sleeper accounts. Therefore the behaviour before the delinquency gives a vital insight into the reason for delinquency.

A rapid escalation of account usage and exposure could indicate a change in personal circumstances but is also a strong indicator of open account fraud. A specific fraud methodology is known as 'bust-out' fraud, where fraudsters will run an account, building a good credit history with positive payment patterns in order to build a strong line of credit. Then when the credit available has reached the level required, they suddenly increase their spending and disappear suddenly, leaving behind unpaid balances.

While bust-out fraud can be difficult to predict, Experian analysis shows there are many strong predictors including current account behaviour and transactional patterns, credit bureau trend data and event triggers. This can be used to determine the risk of bust-out on the account.

3.3 Exclude high-risk cases

Those cases with a high likelihood of fraud should be excluded from the collections process and dealt with accordingly.

Following this process, what will be left are cases that may show some indication of being fraudulent and don't have a clear reason for delinquency. These cases have to be dealt with sensitively as these could be genuine customers in difficulty or fraudsters.

A simple measure, which will ensure that a potentially fraudulent account does not exploit services and enter deeper into collections, is to suspend service, if possible. However an organisation can't risk alienating good customers, so a warning that service will be suspended if payment is not received will alert customers who intend to pay that there is a potential problem.

Any action that is applied to potentially fraudulent defaulters should be fast to deploy and low in cost, so a polite reminder SMS and or email within 48 hours could be followed by an automated voice message after 5 days, for example.

If no response is received by way of payment or inbound call, the debtor should be put on an outbound call list. If there is no success after three attempts of outbound calls at different times of the day, the accounts should be referred as suspected fraud to the fraud team.

Screening needs to be carried out regularly and the combination of suspicious data combined with default data will be enough to investigate rather than collect.

4. Managing fraud in collections

A key challenge for organisations who tackle fraud in collections is how to manage these cases. In some portfolios, the number of suspicious cases can be as high as 2% which could, in large organisations equal 2,000 cases, too many to deal with manually.

4.1 Prioritise fraud risk

Using a scoring model, organisations can prioritise the risk of a case being fraudulent and choose to send the lower-risk cases through an automated activity path with appropriate activities. The remaining cases can be prioritised according to their fraud risk and potential loss value and passed to a referral team for action.

4.2 Manage high-risk cases

A referral team is required to process the resulting cases. The best option is to have a specialist fraud/collections referral team. This does not need to be incremental resource as existing resources can be developed into specialists.

Having specialist team reduces time and cost by ensuring the best use of the fraud and collections resources, by enabling them to focus on their core functions.

Incorporating staff with collections and fraud experience, the team would handle referrals passed from collections and determine whether the cases are fraudulent while still being sensitive to the possibility this is a genuine delinquent customer. If the case is not fraudulent the result is passed back to the collections team and would continue through the normal collections process.

Fraudulent cases would then pass through the standard process, potentially leading to more investigation, collation of evidence and loading of data to both internal and national databases.

A major part of an organisation's effectiveness is collaborative working between all the teams, whether they are front office or back office functions. Organisations should ensure that fraud and collections departments work together in order to ensure they each have the necessary systems and processes and the means, and will, to interact. Organisations should ensure that internal targets and team objectives do not hamper the effectiveness of the close working relationships between the two functions.

4.3 Identifying fraud rings

Organised criminals will frequently use common elements to applications and personal information in order to receive the funds (e.g. bank accounts) and communications (e.g. mobile phones).

Using a fraud networks tool will highlight links between seemingly unrelated accounts based on this data and the links can be illustrated graphically as a fraud ring. Often, one known fraud, when used as part of a fraud ring will lead to three or more associated accounts which are likely to be fraudulent, or highlight where impersonation has been used.

Once these accounts have been identified they can all be dealt with through the fraud process as well as investigated further as there may be links with these accounts which will, in turn, lead to further fraud.

4.4 Creating a feedback loop

When fraudulent accounts enter collections, any delay in the collections department passing that information to the fraud team can allow the fraudster to continue accessing funds or services and incurring further losses to the business.

Creating an effective structure to deal promptly with the early identification of fraudulent activity using information contained in the collections system can make a significant difference to reducing subsequent bad debt losses arising from fraudulent accounts.

Analysing known frauds is essential to understand the patterns and trends that are occurring, so there should be a feedback mechanism to ensure that the fraud systems are updated with the characteristics of accounts that are fraudulent.

Patterns and trends can be discerned from analysis of commonalities between fraudulent accounts in collections that can help provide understanding of how different frauds have been perpetrated and to thus improve the controls and make defences more robust. This can also highlight any common elements in the frauds, such as a member of staff which could indicate insider fraud or a staff training issue.

This will ensure that similar accounts do not enter collections the next time, but are picked up at application or during transactions, saving time and money.

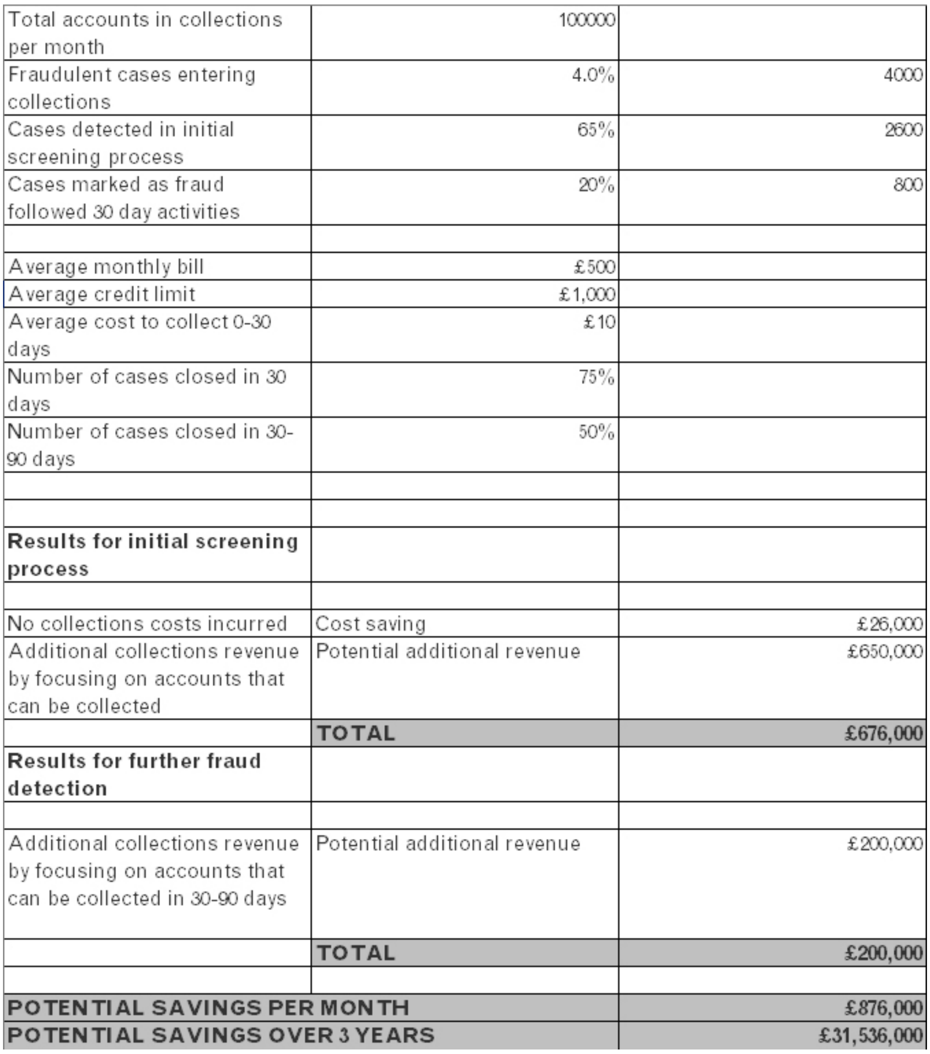
An analysis of Fraud prevention databases shows that only around 20% of the frauds recorded are added post-application. It is estimated this represents less than 25% of the frauds identified post application so broader use of this feedback loop will provide instant pay back.

It is estimated shared fraud data from post-application represents less than 25% of the frauds identified.

5. The opportunity in the collections process

Few organisations fully realise the valuable role that collections and fraud can play together. Organisations who use an holistic approach, where fraudsters are identified as the account becomes delinquent and feeds a continuous feedback loop to improve fraud detection, can reduce losses, make better use of collections resources and improve fraud protection.

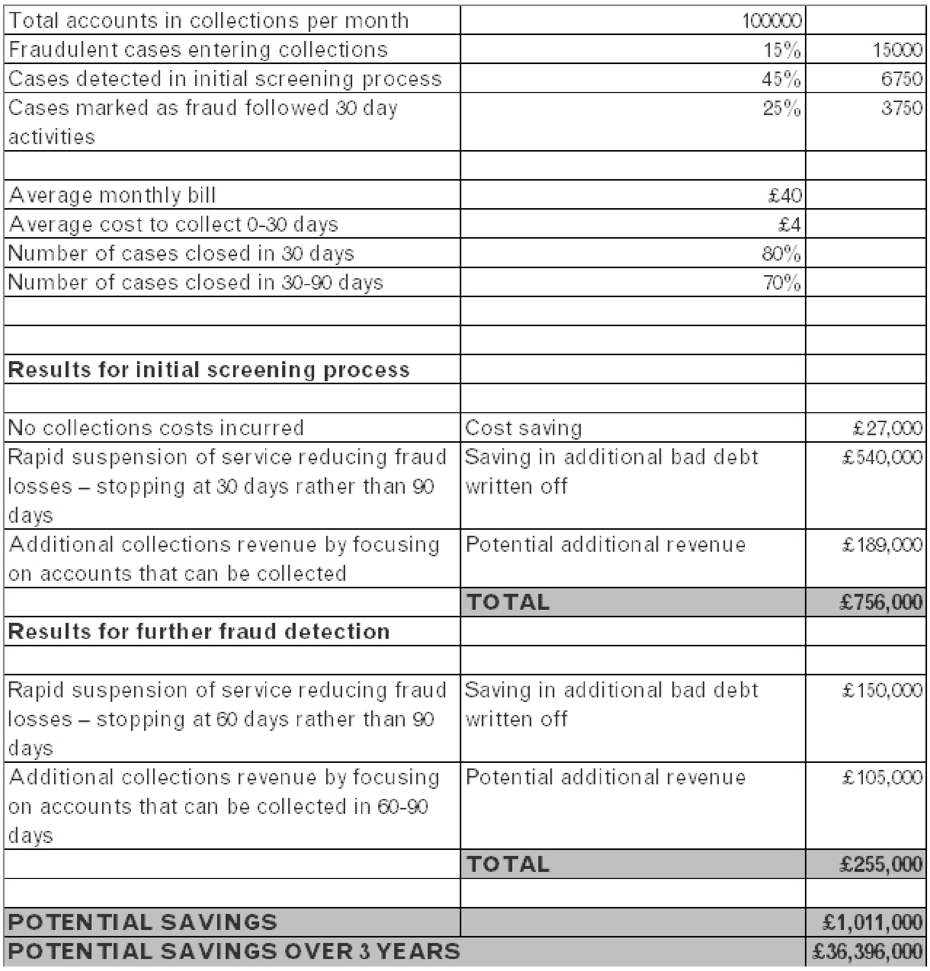
In an example portfolio of 100,000 delinquent accounts for a credit card provider:



Total accounts in collections per month	100000	
Fraudulent cases entering collections	4.0%	4000
Cases detected in initial screening process	65%	2600
Cases marked as fraud followed 30 day activities	20%	800
Average monthly bill	£500	
Average credit limit	£1,000	
Average cost to collect 0-30 days	£10	
Number of cases closed in 30 days	75%	
Number of cases closed in 30-90 days	50%	
Results for initial screening process		
No collections costs incurred	Cost saving	£26,000
Additional collections revenue by focusing on accounts that can be collected	Potential additional revenue	£650,000
	TOTAL	**£676,000**
Results for further fraud detection		
Additional collections revenue by focusing on accounts that can be collected in 30-90 days	Potential additional revenue	£200,000
	TOTAL	**£200,000**
POTENTIAL SAVINGS PER MONTH		**£876,000**
POTENTIAL SAVINGS OVER 3 YEARS		**£31,536,000**

An example portfolio for a credit card could save £800,000 a month.

In an example portfolio of 100,000 delinquent accounts for a telecommunications provider:



Total accounts in collections per month	100000	
Fraudulent cases entering collections	15%	15000
Cases detected in initial screening process	45%	6750
Cases marked as fraud followed 30 day activities	25%	3750
Average monthly bill	£40	
Average cost to collect 0-30 days	£4	
Number of cases closed in 30 days	80%	
Number of cases closed in 30-90 days	70%	
Results for initial screening process		
No collections costs incurred	Cost saving	£27,000
Rapid suspension of service reducing fraud losses – stopping at 30 days rather than 90 days	Saving in additional bad debt written off	£540,000
Additional collections revenue by focusing on accounts that can be collected	Potential additional revenue	£189,000
	TOTAL	**£756,000**
Results for further fraud detection		
Rapid suspension of service reducing fraud losses – stopping at 60 days rather than 90 days	Saving in additional bad debt written off	£150,000
Additional collections revenue by focusing on accounts that can be collected in 60-90 days	Potential additional revenue	£105,000
	TOTAL	**£255,000**
POTENTIAL SAVINGS		**£1,011,000**
POTENTIAL SAVINGS OVER 3 YEARS		**£36,396,000**

An example portfolio for a mobile operator could save £36 million over 3 years.

6. Conclusions

The issue of fraud in collections is growing as both fraud and delinquency increase in the current economic climate. Solutions already exist and build on the solid foundation established in application fraud, using the power of data and data sharing to tackle the shared problem of fraud across every industry.

It takes a holistic approach to the issue, with fraud and collections teams working closely together to develop new processes and methods of working to improve the fraud detection.

However, even just in the collections process this can bring significant rewards, increasing the efficiency of the department as well as providing insight to the fraud team to continually improve fraud protection.

Experian offers expertise in both collections and fraud and, in particular, its Fraud Open Account Monitoring Service can monitor accounts entering collections and screen those against a unique range of data sources to identify and prioritise potentially fraudulent activity.The tool can uncover a range of fraud types, including identity theft and impersonation, as well as identifying links between information indicative of fraud rings.

As part of this comprehensive service, Experian supports organisations in prioritising and managing the investigation and management of these accounts to maximise the benefit to the organisation.

7. About Experian

Experian is the leading global information services company, providing data and analytical tools to clients in more than 65 countries. The company helps businesses to manage credit risk, prevent fraud, target marketing offers and automate decision making. Experian also helps individuals to check their credit report and credit score, and protect against identity theft.

Experian plc is listed on the London Stock Exchange (EXPN) and is a constituent of the FTSE 100 index. Total revenue for the year ended 31 March 2009 was $3.9 billion. Experian employs approximately 15,000 people in 40 countries and has its corporate headquarters in Dublin, Ireland, with operational headquarters in Nottingham, UK; Costa Mesa, California; and São Paulo, Brazil.

For more information, visit http://www.experianplc.com.

www.experianplc.com

Experian™

A world of insight