

Tackling the issue of bust-out fraud

I imagine you work in a retail bank where you have responsibility for new business. You have decisioning systems, fraud controls, credit bureau links and you feel confident you can protect yourself against customers who could expose your organisation to every type of risk.

One day, a potential customer walks into your branch requesting to open a current account. You follow all the processes, making the necessary checks and the account is opened. Over the following months the customer lodges their monthly salary, credits and debits are made and the account always has a positive balance, although they do take up your offer of an overdraft facility. They set up a savings account and maintain a healthy balance.

With such a good customer, you want to balance risk with reward and increase value, so you cross-sell them a credit card. They run this account well, revolving a balance and never missing a payment so after six months the credit limit is increased. You offer a personal loan, which is taken up, leaving your organisation exposed to up to £10,000 of potential lending. However, they are a low risk customer... or are they?

Suddenly, overnight, the current account is emptied and the overdraft used to the limit. The credit card is over limit. You try to contact the customer with no success. Payments are subsequently missed on the loan and credit card and no credits are made to the current account. The account holder disappears without trace and you realise you have been the victim of a calculating fraudster.

Whatever you call this type of fraud, bust-out, advances fraud, runaway spenders or sleeper fraud, this type of first party, open account fraud is becoming a significant issue to the financial services industry. Unlike application fraud, it involves a long-term plan, deliberately manipulating banking behavioural systems to maximise the value of the fraud, posing as a good customer before seizing the full credit facility and disappearing.

Losses on these accounts, while not small, are not as significant as bust-out schemes carried out by criminal gangs, often involving identity theft and links to organised crime and terrorist financing.

In the US, card issuers estimate losses from bust-out fraud to be over \$1.5 billion annually (Credit Risk International, September 2004). In the UK, it is felt that bust-out fraud is a much more significant

problem, with some sources attributing 25% of credit losses directly to this type of fraud (Experian Credit Card Bust Out Workshop, January 2006). Some UK banks have even publicly acknowledged that the growth in this type of fraud has contributed to their recent increases in bad debt provisions.

How to commit bust-out fraud

Firstly, you need to get a bank account. You can simply use your own accounts but these are easily traced, so the fraudster sometimes chooses from a number of other options; identity theft, collusion or an account takeover.

Identity theft as a fraud method in its own right is one of the fastest growing trends in the UK (CIFAS Annual Report 2006). Fraudsters will steal an identity from an individual or group of individuals and use this to gain access to credit. It often takes more than 12 months for the victim to discover the fraud, leaving plenty of time for the fraudster to develop the accounts and bust out, leaving the victim with the task of proving their innocence. Alternatively, the fraudsters can build a new identity, based on an individual, living or dead, using this information to access a range of documentation, including a passport, utility bills and other proofs of identity.

“Whatever you call this type of fraud, bust-out, advances fraud, runaway spenders or sleeper fraud, this type of first party, open account fraud is becoming a significant issue to the financial services industry **”**

Identity theft can also be perpetrated with the collusion of the individual, where their identity is 'bought' by the fraudster. Often, those about to leave the country or who are particularly financially distressed will sell their personal and account details, knowing that when the financial institution contacts them about the fraud they can prove they were not involved. With no proof of collusion, the financial institution has no choice but to expunge their record of fraud.

Dormant accounts are also a target for takeover and subsequent bust-out. Often carried out by someone known to the victim, the fraudster can access the account and then run it in the victim's name before committing the fraud.

So, you have a bank account. Now you need to understand how the credit



Anthony Sumner

decisioning process works in order to maximise the value of the fraud. Financial organisations use automated scoring and decisioning systems to understand and measure the behaviour of individuals. 'Good' behaviours such as paying on time, keeping a credit balance on a current account, transacting in full on a credit card and not going overlimit, positively influence the decision to increase a limit, offer another product and determine lending levels.

So a bust-out fraudster will run a 'clean' account for anything up to 36 months in order to maximise the available credit. Typically a fraudster will:

- Open or take over a current account and credit it with a 'salary' payment or other available credits. These will be rapidly withdrawn before being re-deposited into the account, with this constant churn on the credits providing a false impression of the overall turnover. A savings account is also opened often with significant deposits;
- Be a model customer. Make regular payments into the current account, avoiding going overlimit and continue to make deposits into the savings account;
- Wait for the bank to increase limits, offer additional products and take them all up. These increases and offers will often be facilitated through an automated process for low risk customers and there is no reason for the bank to suspect otherwise. The fraudster will also stockpile cards and chequebooks to provide the maximum available credit.

When the fraudster has reached their desired level of bust, they will suddenly

increase their spending, maximising available credit limits, and take out additional credit products. Spending is often on goods that can easily be sold, such as white goods and other high value disposable items. Cheques are written and cashed, and cards used until they are stopped.

The key to this type of fraud is the speed at which it happens. The draining of the potential credit happens in a matter of days, faster than most banking systems can react to the situation.

What can be done to stop bust-out fraud?

Bust-out fraud is particularly difficult to predict, because the fraudster plays on the established trust between financial institutions and customers and it often involves a single hit. Many financial institutions use models to predict fraud, including bust-out fraud. As discussed, the success of these models to predict bust-out fraud can be limited because of the speed of fraudulent behaviour.

However, this isn't the end of the story. New research by Experian Decision Analytics has uncovered particular behaviours and event triggers that can be used to identify potential fraudsters before the bust-out occurs. These are based on account behaviours, which deviate from the 'normal' behaviour of an account holder.

Much of this analysis has been carried out in the US and UK, where, for example, bureau data has been trended across time to identify predictive characteristics and trigger points to assess the likelihood of bust-out fraud. This bureau data, when combined with a client's own data, can offer a very powerful solution to combating bust-out fraud.

Some of the key predictors identified include:

- A suspicious sequence of applications prior to this product application;
- Multiple surnames at an address – symptomatic of an organised fraud ring;
- Suspicious trends in spending/debt patterns, with utilisation levels increasing significantly over a short period of time;
- Method of payment changing from Direct Debit;
- Time since last credit limit increase – for example, an account has gone overlimit within two months of being granted a credit limit increase;
- Nationality (inferred) – bust-out appears to be perpetrated by non-

nationals of the country where the fraud is perpetrated.

There are many strong predictors when looking at the current account, such as constant churn of the salary credit or other credits, a lack of utility type transactions or Direct Debits and standing orders, the absence of a council tax payment and specific patterns in the type of merchant transactions, such as a concentration of white good purchases. These could all be indicative of potential bust-out.

In the research focusing on utilising credit bureau trend data and 'event' trigger data, it has been identified that trending bureau data from account origination through time can uncover unusual patterns for bust-outs versus non-bust-outs (e.g., changes in consumer indebtedness). Special event triggers which indicate when a new account has been opened or when a limit threshold has been exceeded can be beneficial if this information is captured and scored quickly enough.

“Bust-out fraud is particularly difficult to predict, because the fraudster plays on the established trust between financial institutions and customers and it often involves a single hit”

The analysis has shown that using bureau-based scoring to try to identify bust-out at the point of application is very difficult. However, continuing to take snapshots of the bureau score thereafter and looking for swings and trends in the score is much more successful. Predictive data trends can also be identified when reviewing other bureau data items, such as the level of consumer indebtedness or credit limit utilisation.

All of this information can be combined to create robust predictive models for bust-out fraud. The effectiveness of the models depends on the timing dimension (high frequency) and a longitudinal perspective (trending). Therefore, it is critical as to how often the accounts are scored as well as how much additional data is included in the scoring process; for example, internal transactional data, bureau data, demographic data and other external fraud data.

The new generation of bust-out fraud detection

It is important to stress that analytical and software solutions to this problem need to be effective in the period of 'clean' behaviour leading up to the bust

out as, after that, it is too late to stop the fraud and subsequent losses.

The research shows that robust predictive models can be developed, using outcomes that are made up of actual bust-outs and then incorporating multiple sources of data.

The models can be implemented into existing customer management systems to create bust-out scores and trigger alerts. Using decision engine technology to score each customer would enable organisations to specify trigger scores/events so that they can manage the number of 'alerts' and subsequent bust-out checks they have to perform.

As already mentioned, the amount of data available is critical to accuracy in modelling.

Data sharing is critical to detection success, as has been seen in many countries for other types of fraud. Fraudsters will repeatedly hit a number of organisations within a short space of time so, by data sharing, other organisations can benefit from checking their accounts against known fraud information.

It is critical that this information is updated and checked on a frequent basis, at least weekly, if not daily, so that when a bust-out event happens to one lender, action can be taken before the fraudster busts out on another account by placing checks and supervision on suspect accounts.

Alternatively, by taking an address level view rather than the traditional consumer level view of current credit activity, addresses with highly 'suspicious' levels of credit usage can be pinpointed. This system can be used not only to highlight existing account fraud but also to prevent fraudulent new accounts being opened. Although difficult to quantify at this stage, Experian's new Suspicious Address Alert system should have a major impact on preventing future bust-out fraud in the UK.

Bust-out fraud is a growing, and challenging problem for financial organisations worldwide. With the complexity and speed of the fraud making traditional fraud detection techniques less effective, there is a need for new solutions. The steps made by Experian Decision Analytics go a long way to creating a workable and effective solution to preventing bust-out fraud and the often significant losses incurred. ♦

Anthony Sumner is a Principal Consultant for Experian Decision Analytics