Combating online application fraud for a global telecommunications provider

Orange
Orange (www.orange.co.uk) is a key brand of the France Telecom Group, providing mobile, broadband, fixed, business and entertainment services across Europe. It is one of the world’s leading telecommunications operators with more than 150 million customers on five continents.

Challenge
In the mobile telecommunications market, indirect sales through dealers add significantly to the acquisition cost of a customer. Direct sales offer a quicker return on investment, especially through a low cost channel like the internet. In 2006, Orange launched an online registration service to grow direct sales in the UK market. However, customer demands for an instant decision and the remote nature of the Internet without the face-to-face contact of other channels puts pressure on the application process, particularly the fraud detection and prevention.

Almost as soon as the online service was launched, it was attacked by fraudsters. Fraudsters are well-organised, and often work in networks to identify the weakest points in an organisation, continually evolving and changing tactics to evade the fraud prevention measures in place. Fraud in this sector was typically applicants manipulating application data to gain acceptance and improve the service offered.

Decision Analytics answer
Orange uses a range of fraud prevention measures from Experian throughout their registration process. These flexible tools were developed and enhanced to tackle the new challenges presented by online sales. Changes can be made to the system rapidly, allowing Orange to react quickly to the dynamic fraud threat.

This is now shifting to identity theft, with applicants impersonating genuine individuals to gain access to the latest handsets, which are then exported for profit. Fraud committed through identity theft and impersonation is much more difficult to detect at the point of application compared to the better understood data manipulation type of subscription fraud. The typical approach is to use a manual review but a resource intensive process was not acceptable or practical in terms of cost and customer service. In the real-time, online process, Orange had the challenge of automating fraud prevention without compromising fraud protection.

Case study: Orange

“With growing customer acquisition costs there is an obvious appetite to grow online sales in the current marketplace of falling margins, but to remain competitive we needed to provide a real time decision” commented Mel Prescott, Senior Credit Analyst, Acquisition Management for Orange.

“The online channel is very different to our other channels - there is no human interaction between vendor and customer and it works 24/7, so our fraud prevention measures had to change to make sure the business was still protected. The system provided by Experian has been extremely powerful – it brings together and automates all the credit risk and fraud elements and is very flexible. Typically changes can be made within 72 hours from concept to implementation, allowing us to react quickly to a dynamic fraud threat. The use of Experian products has helped reduce the online fraud by 88%, saving millions of pounds.”
**Benefits**

- **Reduced fraud losses by 88%** for online applications with rapid and accurate fraud detection
- **Staying ahead of the fraudsters** with the ability to make rapid changes as fraud trends evolve
- **Exploiting the power of data** with links to external sources for enhanced detection and identity authentication
- **Accurate fraud detection** reducing the false positive rate and associated costs
- **Enhanced customer service** offering a real-time decision for genuine customers
- **Reduced underwriting resources** with an automated fraud detection process

Orange uses the Origination system from Experian to automate the registration process, assessing applicants, deciding whether to accept or decline the application and determining terms of acceptance. The fraud checking is managed by the same system, incorporating links to external data sources, fraud scoring and application screening.

The primary fraud detection tool Orange uses is Detect, a bureau-based fraud prevention system. It works by using proven detection rules to compare the applicant details with previous applications and a range of data sources. It looks for discrepancies between the information provided with previous applications, which could be indicative of fraud. It also identifies patterns of behaviour among individuals or groups of individuals that are indicative of fraudulent behaviour.

Experian worked with Orange to develop and enhance the detection rules for the online channel, which proved to be more predictive and produce fewer false-positive matches. The system incorporates the Detect Credit Score which provides a risk assessment of the applicant as well as indicating the likelihood of the application being fraudulent.

This enables the automation of decisions and reduces the resources required within the Underwriting Department. Orange also uses the bureau-based scoring service, Authenticate, which gives a confidence level of the applicant’s identity being valid. The tool has proved invaluable in highlighting high risk applications and protecting the business from identity fraud.

Analysis demonstrated that a large proportion of impersonation fraud was committed using company directors’ identities. In the UK, directors of limited companies are required to publicly register their personal information. Fraudsters can easily access this information, achieve a high credit score and access multiple handsets in one application. To counter this threat the system accesses Experian business databases to verify the information supplied and implement extra checks for any applicants listed as company directors.

This work is continuing, with the rules for fraud detection continually updated as fraud trends evolve. As each new measure is implemented, it has an immediate impact on the fraud rate which is gradually eroded as the fraudsters change strategy. The flexibility of the solution means that new prevention measures can be implemented rapidly to counter new threats.

**The future**

In addition to the internal database of known frauds, Orange is also currently working with other UK mobile networks and the Experian Credit Bureau to establish a Telecom industry fraud sharing database. The power of sharing data comes from the increased level of information available for fraud checking, and the sharing of fraud information means that the fraudster has nowhere to go, protecting the whole industry from this crime.