

... biometrics and why it should be teamed with fraud analytics



The British Retail Consortium recently reported £0.5bn profit leaks from retail fraud. Divvy that up amongst the retail community and everybody is paying - right down to the consumer.

But, with 80% of loss occurring at point of sale, the irony is that it's store employees - those trusted with that other hot topic of 'customer service', whom are the main perpetrators in 'serving' themselves to retail profits.

Combating staff fraud with point of sale technology clearly has massive potential for return. That's why, over the years, we've been through POS pass wording, magnetic cards, video monitoring - a whole evolution of technical effort to solve this problem. But the problem is still there and growing, so efforts thus far have failed. Is it that fraudulent techniques evolve faster than their preventative counterparts? Or is it perhaps that, to date, there is no one solution that has proven its worth in ridding the problem? Both, it appears, are true.

At face value, biometrics is fast emerging as the solution we've all been waiting for. Its infallibility at identifying individuals is unquestioned. But lessons have to be learned from the investments and failures that have gone before to ensure this technology really is given the chance it deserves to crack this difficult nut. To do this, we need to step back to the fundamentals of the problem.

Fraud is a crime. No grey areas there! But, whilst identifying 'who done it' is the ultimate aim of any crime investigation, getting to that stage can take a great deal of investigation, sophisticated thinking and planning. And then, the real point about crime is that it is always best to avoid it in the first place.

Analysing trends and filtering out individual fraudulent activity from a mass of retail transaction data is a grim manual task; arguably impossible. Since unquestionably pinning somebody to a crime using fingerprinting technology requires this back room toil, here lays the flaw in biometrics and its ultimate return on investment. We're not talking here about catching individual 'suspects'. The meaningful returns will only come in the form of totally eliminating fraudulent activities - All dodgy returns. All deceitful no sales. This is impossible to analyse manually; unquestionably.

An all encompassing surround and conquer approach is required using a closely meshed combination of identification AND prevention technology. This is where the engine room power of analytics comes into play. Analytics can serve up trend reports in fraudulent activity - across the board. Tolerance rules and parameters can then be set which automatically trigger SMS or email alerts. Only using these background tools can the foolproof proof that only biometrics offers be called into play meaningfully and on a wide scale.

As always in retail, return on investment is the bottom line. Sure biometrics is the hot thing of the moment. Unless however it is complemented with the correct analytical and alerting technologies, fraudsters will continue to prevail and the returns from this hot technology will fail to sizzle.



Linda Meehan
Head of Marketing
Itim - Adding Retail Value