

# Staying on top of online crime

## Five top tips for upgrading your company's fraud detection system

BY BENN DULLARD

As we dust off the hangovers from new year parties, and have perhaps already broken the best intentioned resolutions, it is back to business as usual in 2008. Sitting in various parts of the world (including Australia), fraudsters and criminals will also be returning to BAU. They will have an increased determination to overcome the various fraud detection and prevention initiatives implemented by the banking industry, and to capitalise on the potential of lucrative payoffs. Well known cybercrime groups and new punters alike will all be looking for their slice of the action, and, in tandem, fraud and security teams will be looking to stop them.

One key weapon in this fight is the fraud detection systems that each bank has in place, varying from in-house developed platforms to large scale enterprise vendor platforms. But what constitutes a great OLB (online banking) fraud detection system and how does an organisation make the right choice? Is it just about keeping the crucial false positive ratio low? Should you build it yourself, or outsource, and if outsourcing, who with? The truth is there is no single common answer or detection product which applies to all banks; every institution must consider a number of crucial factors. However, there are some common considerations which apply to any organisation in the process of upgrading or investing in a new fraud detection platform. The top five include:

### 1 Organisational intricacies

As with any new system implementation, the right choice will depend on the organisation size and structure. A fundamental requirement for any fraud detection system is the ability to create and modify rules. Some systems provide a centralised rule creation facility whereas others rely on outsourcing this capability. The size of a bank's fraud team and how well they are trained will have a major influence

on this decision. The bank's risk profile and in particular its tolerance level for fraud losses will also play a role. The IT structure and development teams are also crucial; for instance, where does the organisation store transactional and customer data which will be fed into the fraud rules (central CIS versus multiple customer databases)? Furthermore, how easy is it for certain systems to connect to that data?

### 2 Scalability and cross-fraud considerations

Scalability of a system is crucial. As any organisation grows, its transaction levels will increase, and at some

point the fraud levels may also increase. Forecasting plays a critical role in system selection. Another consideration is the ability to respond in a rapid manner to fraud trends across multiple channels. This raises the question of whether the solution should be an enterprise fraud solution, or multiple point solutions. Again,

the answer depends on the bank. The increase of identity theft (which can be multi-channel) will also influence the thinking.

### 3 Cost and vendor

Any person in the OLB fraud and security space will know how hard it is to build a business case when losses are low. Proving return on investment can be difficult as it requires forecasting losses, which in itself is impossible. Ironically, business cases are easier to fund when losses occur, but these losses could have been prevented in the first place through proper planning of the OLB fraud environment. The cost model will clearly look further than just the system licensing, but also factor in internal IT chargeback for integration and ongoing maintenance. The numbers can add up and change according to vendor and system setup. The importance of a thorough request for proposal process becomes apparent, with a deep dive into a company's technology roadmap and ability to

influence it. Is the system tailor made for OLB fraud, or is the vendor just trying to capitalise on a new market?

### 4 Real time trends and intelligence

Any OLB fraud system must be able to move quickly and change fraud rules to adapt to fraud threats and losses. OLB fraud changes and morphs quickly, something every fraud analyst knows. Once a fraudster finds a weakness, they exploit it rapidly and share information via underground sites. Banks need to adopt a similar approach to rapidly respond and counteract these threats. The fraud detection system is the first step in detecting the fraud, but how quickly will the system be able to be updated? Similarly the system should also be compatible and allow plug-ins to industry intelligence feeds (for example, mule trends, IP intelligence, and payment types) and be able to rapidly update rules based on this industry intelligence.

### 5 Consider the bigger OLB fraud picture

Finally, the question must be explored: Is it worth investing in a multi-million dollar fraud detection system when there are already multiple other security initiatives in place? Likewise, if investing in a best practice detection system, how much effort should go into other activities such as authentication, response and prevention activities? How does the fraud detection system fit into the existing picture? A holistic view is required with fraud, with security and business teams working together to also balance the impact on customers. Security and fraud managers love to debate these issues with the marketing and customer experience staff at larger institutions!

There are huge risks for implementing the wrong system, including an increase in financial losses. Probably the biggest risk though, is being perceived as an easy target by cyber-criminals, and therefore sustaining more attacks.

Benn Dullard is technical director at online security firm Eunexus

[pbenn@eunexus.com.au](mailto:pbenn@eunexus.com.au)

What constitutes a great ... fraud detection system and how does an organisation make the right choice?