The changing fraud landscape and increases in loss to fraud requires automated detection systems. Selecting the right solution is challenging. Scarce IT resources, access to industry experience and fraud knowledge is essential to getting the return on this very costly investment. All businesses are different, configuring the generic fraud system to tackle the unique risks you face is essential to achieve the payback on your investment.

Current environment and drivers
Financial services organisations face an ever increasing range of challenges within the financial crime arena, both internal and external. There is increasing focus on utilising risk management systems and making greater use of intelligence in the response. A number of financial institutions are starting to address fraud monitoring systems at an enterprise level, incorporating anti-money laundering and payment screening for financial sanctions. Monitoring and screening activity can be performed within a single environment that applies rules but also learns and can be calibrated with new fraud typologies.

Traditionally, fraud monitoring systems have been designed to address specific fraud risks, products or delivery channels. As the need to connect these silos becomes more apparent, a more strategic approach is needed. Implementing systems which operate across the business and provide greater flexibility to integrate new data sources and detection models in response to new threats is a worthwhile objective. Accordingly, financial institutions are seeking to use intelligence to inform preventative actions, improve detection of fraud and make investigations more efficient and effective in understanding the scope and nature of fraud, reducing losses.

Drivers to inform the fraud management systems strategy and deliver a better integrated approach to fraud risk management include:

- The need to improve performance of existing systems which typically exist in silos
- A desire to join up disparate systems in order to improve the intelligence picture and move to a more proactive, preventative approach based on activity across product lines and channels
- A changing risk profile driven by new clearing and payment mechanisms
- The need for increased agility to deal with new threats and fraud migration to lesser protected products, channels and customer segments
- Improve the efficiency of fraud operations to support straight through processing and faster fulfilment
- Maintain and strengthen the customer experience

Key components
Key components within the fraud systems architecture include:

- Verification of a claimed identity and product application fraud checks
- Transaction monitoring to identify abnormal processing and patterns, indicating fraud
- Intelligence and case management to enable investigators to focus on the areas of greatest risk
Key questions when evaluating your fraud monitoring systems strategy

► How well do existing systems control current and emerging risks?
► What is the three year vision?
► How can the relationship with IT be used to support implementation of this vision and manage IT and operational costs? How will you obtain adequate change capacity from IT to ensure prioritisation is given to these projects?
► How responsive are your current systems to new threats and how quickly can they be adapted to detect new fraud patterns? Do they allow business “power users” to make changes to detection rules without the need for involvement from IT?
► How great is the level of automation within operational areas? Where can operational benefits be realised and customer service improvements be made through improving case management capabilities?
► How can the business case process be managed to ensure timely allocation of funding to enable you to meet future fraud challenges, linked to the strategic investment process?
► Does your fraud system support effective customer care and support?

Proving the case for investment using data analytics

Prior to investing in a fraud monitoring system, performing a targeted data analytics exercise enables firms to rapidly validate the level of risk exposure, test the practical issues involved in a deployment and understand the data possibilities as well as limitations. A key outcome of this is assistance in short listing systems technologies and this can inform the system design and implementation.

The Ernst & Young Service Offering and Approach

Ernst & Young are able to offer a comprehensive service offering across the fraud monitoring systems spectrum:

<table>
<thead>
<tr>
<th>Strategy Definition</th>
<th>Market Review &amp; Package Selection</th>
<th>Implementation Support</th>
<th>Analytics &amp; Tuning</th>
<th>Independent Quality Review</th>
</tr>
</thead>
</table>

The Ernst & Young approach is centred on the deep industry knowledge of our Financial Crime team, based on years of experience at leading global financial institutions and successful client engagements. We work with clients and their supply partners to form innovative and practical solutions, building teams of experienced consultants from across Ernst & Young, teaming with client specialists to ensure successful deployment and attainment of benefits.

Ernst & Young is able to draw upon consultants with a range of subject matter experience including:

► Financial crime strategy
► Fraud risk management
► Data analytics
► Information technology and architecture
► Programme management and change delivery
► Process design and performance improvement
► Regulatory compliance
► Law enforcement
► Fraud operations
► Credit risk operations
► Outsourcing and supply management

Why Ernst & Young

► An independent, vendor neutral perspective
► Detailed market and vendor knowledge
► An integrated delivery team with relevant experience of similar projects
► We have helped clients successfully deliver major financial crime systems projects around the world
► Improved confidence in delivery and benefits realisation
► Improved effectiveness of fraud response and faster speed to market.
► Global team able to evaluate risk and provide deployment support by teaming with client resources and their suppliers globally