e-Crime continues to attract significant attention within the industry and increasingly within the regulatory sphere. Although financial institutions have implemented a number of counter-measures to reduce risk and educate customers, criminals are constantly developing new and innovative ways to gather confidential information and perpetrate fraud. The speed and agility with which they can act raises the risk of a rapid escalation in fraud losses following sustained attacks, as well as the likelihood of rapid fraud migration across the industry and to other products and channels.

Damage to consumer confidence and to businesses, especially within financial services, has been increasing, although the full impact of e-crime is not widely understood. Many incidents are never reported and building up a full intelligence picture is complex, due to the many parties involved - both internally and externally.

Typical e-crime incidents
Common attacks targeted at customers and other third parties include:

► Phishing - the indiscriminate mass distribution of unsolicited e-mails and other means to gather confidential information, through impersonation of company brands.

► Malicious Code - the use of computer viruses, Trojan horses and keyloggers specifically targeting certain banking web sites for the purpose of gathering confidential information from customers.

► Denial of Service attacks - malicious activity designed to restrict availability of computer resources to legitimate users.

► Identity theft and Card-Not-Present fraud - personal information and payment card details can be obtained through compromise of merchant and payment processor databases and used for a variety of frauds and account takeovers.

► ‘Money mule’ accounts - recruitment of genuine customers, or opening of dedicated accounts to receive the proceeds of fraudulent transactions and enable subsequent extraction of funds and money laundering.

► Stock fraud - unauthorised access to share portfolios through compromise of log-in details or use of unsolicited e-mails to dupe people into unwittingly participating in ‘pump and dump’ scams.
This fast moving and unpredictable funding and resources. Unlike traditional fraud threat areas, threat identification, vulnerability their returns. The unparalleled speed the agility and motivation to invest continuously in ways of increasing their returns. The unparalleled speed of attack and threat development puts pressure on organisations to respond in line with the agility of the criminals. This poses challenges particularly around threat identification, vulnerability assessment and rapid mobilisation of funding and resources.

Fraudsters also have very attractive risk-reward-effort considerations, with the agility and motivation to invest e-crime cuts across organisational responsibilities for product ownership, channel management, fraud, security and customer handling, presenting challenges in translating technical issues into business implications.

Challenges of combating e-crime e-Crime attacks are primarily directed at customer and third party systems which are outside the control of the targeted organisation. This means that they are difficult to track and respond to.

Unlike traditional fraud threat areas, e-crime cuts across organisational responsibilities for product ownership, channel management, fraud, security and customer handling, presenting challenges in translating technical issues into business implications.

Business needs
This fast moving and unpredictable environment presents a number of challenges to businesses, including:

- Identification of horizon risk
- Peer group analysis
- Threat identification, vulnerability assessment and response planning
- Assessment of control effectiveness
- Fraud loss reduction and crisis management
- Optimisation of fraud detection solutions and operational integration
- Specifying detailed business requirements and managing the relationship with IT
- Progressing the commercial agenda and business case justification
- Effective customer management

Developing solutions
Our approach is centred on the deep industry knowledge of our financial crime specialists, and years of experience working with and in leading global banks. We work with our clients to develop innovative and practical solutions, using teams of experienced consultants across Ernst & Young.

Our advisory services operate at a range of different levels:

- Governance
- Strategy
- Operations and performance
- Transformation and remediation
- Assurance and audit

Our specific propositions include:

- Fraud reduction and crisis management (incident response, threat investigation and forensics)
- Strategic assessment of remote channel threats, vulnerabilities and capabilities, to develop an effective e-crime strategy
- Fraud data analytics
- Financial crime systems advisory work e.g., transaction profiling
- Multi-factor authentication advisory services
- Anti-fraud operations process optimisation

Ernst & Young contacts
Jon Harvey
+ 44 (0)20 7951 2785
jharvey1@uk.ey.com

Tom Salmond
+ 44 (0)20 7951 8437
tsalmond@uk.ey.com

Ernst & Young
Assurance | Tax | Transactions | Advisory

About Ernst & Young
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 130,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve potential.

About Ernst & Young’s Fraud Investigation & Dispute Services
Fraud, unethical conduct and commercial disputes may present major reputational and financial risks to your business, as well as detracting from your company’s efforts to achieve its potential. We offer forensic and IT skills, knowledge, tools and methodologies to conduct investigations and help resolve disputes quickly, effectively and globally with minimal impact on “business as usual.” Better management of fraud risk and compliance exposure is a critical business priority - no matter the industry sector. Working closely with you and your legal advisors, we bring an objective approach to these sensitive and contentious situations. It’s how Ernst & Young makes a difference.