

## **Fraud**

### **Driver – Political, Economic, Social, Legal**

Related Drivers – Organised Crime, Recession, E-crime, Collection and Storage of Personal Information, Data Mining, Information Sharing

#### **Background**

Fraud can be perpetrated in two different forms: 'Non-fiscal fraud' and 'fiscal fraud'. 'Non-fiscal fraud' describes frauds against the financial services industry, business and members of the public. It occurs when criminals take money but fail to supply goods, services, obtain loans but fail to repay, manipulate banking systems to steal money, obtain money to which they are not entitled or subvert other systems or markets to obtain financial benefit. 'Fiscal fraud' describes frauds against the government and includes theft or evasion of revenue, mainly involving duties and taxes and welfare benefits.

This section focuses primarily on forms of 'non-fiscal fraud'. It is important to note the e-crime is treated as its own driver even though the majority of e-crime is fraud related.

#### ***Political Context***

In *Realising Britain's Potential: Future Strategic Challenges for Britain*, the Cabinet Office included fraud as one of the areas of serious crime which poses a strategic challenge in the future.<sup>1</sup>

Before the introduction of single public confidence target for the police, the Home Office set out its expectations for police activity through a series of targets. It was during this time, the Home Affairs Select Committee report, *Policing in the 21<sup>st</sup> Century*, was produced. During the evidence gathering, the Committee received written concerns about the absence of fraud, including identity fraud from police performance targets.<sup>2</sup> At the time, with the exception of the City of London Police, which has been designated as the lead force for delivering the Government's fraud strategy, forces find it difficult to dedicate resources to an area which is not designated by the Home Office as a priority. Additionally fraud investigation requires high levels of training and expertise.

The Committee stated their disappointment that fraud is not a police priority given the economic costs and is a cause of public concern. They recommend that forces are required to give greater priority to tackling fraud and are allocated sufficient resources to carry out this function.

In response to the Home Affairs report, the Attorney General published the three year National Fraud Strategy, '*A new approach to combating fraud*' on 19 March 2009. Activity undertaken via the strategy is coordinated by The National Fraud Strategic Authority and tackles four key priorities:

- Improving the building and sharing of knowledge about fraud, by the City of London Police establishing a new National Fraud Reporting Centre and National Fraud Intelligence Bureau
- Tackling the most serious and harmful fraud threats, such as identity and mass marketing fraud
- Disrupting and punishing more fraudsters while improving support to their victims, by working with the Association of Chief Police Officers and Victim Support, introducing plea negotiations and extending the Crown Courts' powers in fraud cases
- Improving the nation's long-term capability to prevent fraud, by better coordinating fraud public awareness activity and building strong, supportive partnerships among the counter-fraud community.<sup>3</sup>

## ***Economic Context***

It is estimated that fraud costs the UK £13.9 billion annually.<sup>4</sup> Statistics published by APACS, the UK payments association, showed for the six months to June 2008:

- Card fraud losses increased by 14 percent compared with the first half of 2007
- Losses from phone, internet and mail order shopping fraud have continued to increase year-on-year
- Online banking fraud losses totaled £21.4m – a 185 per cent rise on the 2007 figure. Although this increase seems marked, it is in keeping with a gradual increase seen from the second half of last year, when online banking fraud losses increased to £15.1m (during July to December 2007). The increase is largely due to criminals targeting online banking customers through phishing and spyware scams - because the banks' own systems have proved difficult to attack
- The number of recorded phishing attacks continues to increase, with more than 20,000 fraudulent phishing websites set up in the first half of 2008 – an increase of more than 180 per cent from the same period last year.<sup>5</sup>

Recent studies show that the detection of fraud is continuing to rise. The number of fraud cases filed by CIFAS, the UK's Fraud Prevention Service, during January to September 2008 rose by 15% compared to the same period in 2007.<sup>6</sup> Research carried out by CIFAS state that their members view online, staff and identity fraud as the highest priority threats during the current climate.

Analysis of fraud trends during the first quarter of 2009 by CIFAS show an increase in people being impersonated in the same period last year by 40%, as well as a rise in facility takeover frauds and false insurance claims.<sup>7</sup> The recession has been cited as reason for the increase in fraud. Pundits feel that the financial pressures created by the recession can serve as motivation for employees, customers and criminals to commit fraud.<sup>8,9</sup>

## **Social Context**

A survey carried out in 2007 by life assurance firm CPP established identity fraud as the number one worry for the public.<sup>10</sup> Even though fraud costs each person living in England and Wales approximately £231 a year, its impact stretches beyond monetary value through the stresses and inconvenience it causes to the victims of fraud.

The Financial Service Authority (FSA) warns in its 2009 Outlook paper that criminals may now target employees disgruntled by the threat of redundancy, poor pay increases and increasing financial pressures caused by the recession. Employees may become more desperate as the recession deepens, increasing the risk of crimes such as data theft, mis-marking, the manipulation of financial accounts in a desire to meet company targets, and the theft of client money.

Due in part in globalisation and fast developing technology, organised crime groups are diversifying into other areas of crime including fraud.

## **Technology Context**

The FSA Outlook paper indicates that criminals appear to be changing the way in which they commit financial crime, indicating an increasing sophistication as they require more complete data to commit such crimes. For example, CIFAS reports that 'current-address fraud' now surpasses instances of 'previous-address fraud' comprising two-thirds of all identity fraud cases filed by its members in the first quarter of 2008.<sup>6</sup>

## **Legal Context**

The **Serious Crime Act 2007** introduced a package of powers to strengthen and improve the ability of law enforcement agencies to tackle and prevent serious crime. The measures most relevant to the police service in England & Wales regarding fraud include:

- **Additional powers** are given to **accredited financial investigators** including the power to seize any property to a restraint order and the power to search for cash on a person or premises and seize it if it is suspected that it is the proceeds of unlawful conduct or intended for use in such conduct. Such powers are given to constables and officers of HMRC. Financial investigators would be granted these powers of seizure if they fell within a description of investigator specified for this purpose by an order made by the Secretary of State.<sup>11</sup>

In 2007, the Home Office has issued a new Code of Practice which provides guidance on the **use of powers of investigation in respect of confiscation, civil recovery and money laundering** provided by Chapter 2 of Part 8 of Proceeds of Crime Act 2002 (POCA).<sup>12</sup> It applies to those who have functions to apply for or execute these powers of investigation including, Accredited Financial Investigators (AFI) and Constables.

The above Code replaces the existing codes, reflecting the updates made to investigation provisions by the Serious Crime Act 2007.

In addition in March 2008 separate guidance was issued to investigators regarding the operation of the powers under Section 289 of POCA to **search for cash** which is suspected of being either the proceeds of or intended for use in crime as a result of the Serious Crime Act 2007 (Section 79) and UK Borders Act 2007 (Section 289).<sup>13</sup> These powers have been expanded to include accredited financial investigators who have been trained and accredited by the NPIA and immigration officers as well as police officers and HMRC officers.

## **Potential Skills Needs**

**Analytical skills** – to visualize, articulate, and solve complex problems and concepts, and make logical decisions based on available information

**Collaborative working skills** – working effectively with colleagues and other law enforcement agencies

**Computer forensic skills** – analysis of information contained within and created with computer systems and computing devices, typically in the interest of figuring out what happened, when it happened, how it happened, and who was involved

**Financial intelligence analysis skills** – analyse financial transactions and other financial related criminal intelligence

**Financial investigation skills** – investigate complex financial transactions combined with an in depth knowledge and understanding of the current and relevant legislation relating to financial investigations

**Fraud investigation skills** – investigate cases of fraud with an in depth knowledge and understanding of the current and relevant legislation relating to fraud investigations

**Intelligence gathering skills** – to scan multiple data sources and follow leads

**Intelligence information sharing skills** between police forces, other intelligence and security agencies

**Inter-agency working skills** – to work effectively with two or more governmental agencies

**IT skills** – general awareness and understanding of current ICT environment and changing landscape

**Multi-agency working skills** – to work with other agencies to protect the UK

**Partnership working skills** – to work effectively with other agencies to a common goal and standards

<sup>1</sup> [Cabinet Office \(2008\) \*Realising Britain's Potential; Future strategic challenges for Britain\*. London: The Stationery Office Ltd.](#)

<sup>2</sup> [House of Commons Home Affairs Select Committee \(2008\) \*Policing in the 21<sup>st</sup> Century\*. Seventh Report of the 2007-08 Session. HC 364-I, London: The Stationery Office Ltd.](#)

<sup>3</sup> [Attorney General \(2009\) \*The National Fraud Strategy: A new approach to combating fraud\*. London: Attorney's General Office.](#)

<sup>4</sup> ACPO (2007) *The Nature, Extent, and Economic Impact of Fraud in the UK*. London: ACPO.

<sup>5</sup> [APACS Press Release, 25 September 2008, 'APACS announces latest fraud figures'](#).

<sup>6</sup> [CIFAS Press Release, October 2008, 'CIFAS figures confirm that the UK's fraud landscape has changed'](#).

<sup>7</sup> [CIFAS Press Release, 26 January 2009, 'Fraud Trends 2008: Fraud on the increase'](#).

<sup>8</sup> [CIFAS Press Release, 27 April 2009, 'Fraud trends and recession go hand in hand'](#).

<sup>9</sup> [Financial Services Authority \(2009\) \*Financial Risk Outlook 2009\*](#). London: Financial Service Authority.

<sup>10</sup> BBC News Online, 11 April 2007, '*Modern life 'causes major stress'*'.

<sup>11</sup> [Serious Crime Act 2007 \(England, Wales, Northern Ireland\)](#).

<sup>12</sup> [Home Secretary \(2007\) \*Code of Practice Issued under Section 377 of the Proceeds of Crime Act 2002\*](#).

<sup>13</sup> [Home Office \(2008\) \*Proceeds of Crime Act 2002 Seizures of Cash Policy\*](#).