

# Fighting Fraud Together

The strategic plan to reduce fraud



Association of British Insurers



ASSOCIATION OF CHIEF POLICE OFFICERS



AGO

Attorney General's Office

bba

The voice of banking & financial services



British Chambers of Commerce  
The Ultimate Business Network

BRITISH RETAIL CONSORTIUM  
for successful and responsible retailing

Building Societies Association

BIS | Department for Business Innovation & Skills



Cabinet Office



PROMOTING BEST PRACTICE IN CHARITY FINANCE



Council of Mortgage Lenders



CPS

DWP

Department for Work and Pensions



Federation of Small Businesses  
The UK's Leading Business Organisation

FFA

Financial Fraud Action UK  
Working together to prevent fraud



Financial Services Authority

Fraud Advisory Panel



HM Revenue & Customs



HM TREASURY



Home Office

ifb

Insurance Fraud Bureau



Land Registry



The Law Society



Working together for a safer London



Ministry of JUSTICE



ncvo



National Fraud Authority

NHS

Protect



RICS



SFO

serious fraud office

SOCA  
SERIOUS ORGANISED CRIME AGENCY



Solicitors Regulation Authority



UK Fraud Forum

THE UKCARDS ASSOCIATION

victim support  
find the strength



# Contents

Collective statement of intent	4
Introduction	6
Section 1: The fraud challenge	9
The criminal threat	9
The future trajectory of the threat	11
Behaviours and attitudes	12
The damage caused by fraud	13
Strengths and weaknesses of our response	14
Section 2: Strategic direction	17
Our ambition	17
Strategic objectives	17
Priorities	18
Section 3: Strategic delivery	22

# Collective statement of intent

We recognise the benefits of working together to tackle a crime that affects us all and collectively costs us £38bn per annum. The criminals who attack us do not operate in silos and neither should we. Where we have worked together, we have delivered some significant results but there is much more that could be done. *Fighting Fraud Together* gives us a fresh impetus to make sure that this work is done. We, the organisations which are part of *Fighting Fraud Together* will:

- Continue with measures to prevent, detect, disrupt and punish fraudsters both within our sectors and by working collaboratively across sectors, sharing intelligence, information and good practice
- Commit to a new set of cross-cutting initiatives to provide fresh impetus in our fight against fraud
- Widen our partnership working to involve other sectors who are less advanced in their approach to fighting fraud
- Strengthen the institutional arrangements for co-ordinating our work
- Ensure that our work is informed by the best intelligence picture we can develop and continually review future as well as current threats
- Publish regular reports on our progress



**James Brokenshire MP**  
Parliamentary Under Secretary of State for Crime and Security, Home Office



**The Rt Hon Francis Maude MP**  
Minister for the Cabinet Office and Paymaster General



**The Rt Hon Dominic Grieve QC MP**  
Attorney General for England and Wales



**Lord Freud**  
Parliamentary Under Secretary of State (Minister for Welfare Reform) and Government Spokesperson, Department for Work and Pensions

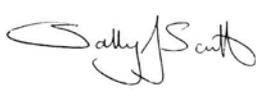
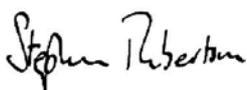


**David Gauke MP**  
Exchequer Secretary to the Treasury

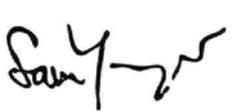


**Baroness Hanham CBE**  
Parliamentary Under Secretary of State and Government spokesperson, Department for Communities and Local Government

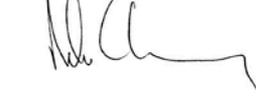
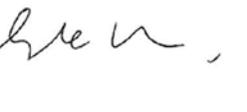
This strategy is endorsed by the following signatories

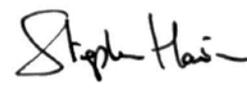






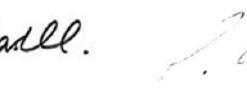















# Introduction

Recent years have seen some significant improvements in our ability to tackle fraud.

- The Government's Fraud, Error and Debt Taskforce, chaired by Francis Maude, has raised the profile of fraud in the public sector beyond the focus on tax and benefits. It will save £1.5bn by 2014/15 once fully rolled out across Government.
- In Action Fraud, victims now have a single place to report fraud, access practical advice and be referred to Victim Support – whose volunteers have been trained in meeting the needs of fraud victims.
- Law enforcement organisations now have state of the art intelligence gathering and analysis facilities such as the National Fraud Intelligence Bureau to build an improved understanding of the fraud threat and target their activity more effectively.
- Organisations and sectors are learning from lessons in other sectors such as the fraud prevention benefits of sharing data.
- The public are more aware of the threats – an essential first step in helping individuals to protect themselves from fraud.

Despite these improvements, the threat from fraud continues to have a damaging effect on our country. Individuals, charities, public services and the private sector continue to pay a high financial price with the 2011 National Fraud Authority Annual Fraud Indicator<sup>1</sup> estimating losses of £38.4bn. Overall fraud offences recorded by the police and Action Fraud have remained constant against a backdrop of generally falling rates of acquisitive crime and law enforcement organisations are facing resource challenges.

As staggering as they are, the costs of fraud cannot be measured solely in terms of monetary loss. The effects permeate throughout society. Large businesses suffer reputational damage. Small and medium sized businesses can go out of business, affecting their owners, employees and their families and damaging the country's economic prospects. Some individual victims, often among the most vulnerable people in our society, suffer serious emotional trauma; some have even taken their own lives.

The fight against fraud needs to be re-energised. We need to do more of what we know works well, such as the sharing of information to prevent fraud, and we need to find new approaches to new threats such as those posed by the increased use of, and dependence on, technology. Most of all,

---

<sup>1</sup> <http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/annual-fraud-indicator/>

## The strategic plan to reduce fraud

we need to do this together. Fraudsters attack all economic sectors and parts of our society. Our fight against them will be much more effective when working together.

*Fighting Fraud Together* sets out a new approach with the ambition that:

“By 2015 our country will be demonstrably more resilient to and less damaged by fraud through:

- Individuals, businesses, public and voluntary bodies **detecting** and **preventing** more fraud.
- Law enforcement and other partners increasing the risk of **disruption** and **punishment** to organised and opportunistic fraudsters, thus **detering** potential criminal offenders”.

We will deliver this mission through three strategic objectives:

- I. **AWARENESS:** We will prevent more fraud by achieving a step change in **awareness** of fraud among the general public and organisations in the private, public and voluntary sectors and in their ability to protect and safeguard themselves.
- II. **PREVENTION:** We will **prevent** more fraud through stronger systems and controls in our businesses, and public and voluntary services.
- III. **ENFORCEMENT:** We will strengthen our response to be **tougher** on fraudsters by **disrupting** and **punishing** them more efficiently and effectively.

*Fighting Fraud Together* is a genuine partnership between the public, government, law enforcement, the wider public sector, private sector organisations and the voluntary sector. It will ensure that:

- New activities are prioritised against those enablers that help criminals conduct many types of fraud.
- Efforts are intensified in sectors that have significant or increasing fraud risks but insufficient counter fraud activity.
- Existing counter fraud efforts are brought together and better co-ordinated.

Our strategic approach is firmly designed around our improved understanding of the fraud challenge. [Section 1: The fraud challenge](#) summarises our assessment of the criminal fraud threat and the strengths and weaknesses of our current response.

[Section 2: The strategic approach](#) sets out the strategic mission we have set ourselves over the next four years based on our assessment of the fraud challenge.

[Section 3: The strategic framework](#) sets out how we will work together to deliver our mission. This includes how we will collectively oversee our strategy, monitor delivery and measure our success.

Our key initiatives, who will lead them, who will support the lead organisations, what outcomes we will deliver and by when are detailed in our programme of activity. This includes both new cross-cutting initiatives and those which are underway but not fully delivered. The programme of activity will develop over time to reflect new initiatives and new organisations joining the *Fighting Fraud Together* partnership. We will also develop and maintain a compendium of activity which is a more comprehensive list of initiatives which are being delivered by individual organisations, sectors and local and central government. These are just as important but do not have the cross-cutting theme and impact of those in the programme of activity. The compendium will be available to members of the *Fighting Fraud Together* partnership should members wish to make contact with each other to exchange information, learn from each other's experiences or join an existing initiative.



## SECTION 1:

# The fraud challenge

We have improved our knowledge of how criminals operate, the behaviours and attitudes of victims and wider society that help fraudsters commit their crimes and the damage that fraud causes. We also understand where we have good capabilities for tackling fraud and where improvements are needed. This section of *Fighting Fraud Together* summarises our view of the fraud threat and the strengths and weaknesses of our response.

## The criminal threat

Fraud is not a new crime but the ways in which fraudsters operate have evolved significantly in recent years:

### Criminals are now more organised

The activities of criminal groups rely on significant levels of planning and coordination. Business structures are to be found within fraud networks including chains of command, defined roles and remits, suppliers and service providers<sup>2</sup>. Fraudsters are networking online to share information and build criminal enterprises across the UK and overseas. Criminal tactics are constantly changing, as the criminals respond to our interventions and take advantage of new opportunities.

### Criminals are more technically capable

Criminals exploit the latest technology in a number of ways. They compromise computers to steal personal and financial data, both from individuals and in bulk. They use social networking to build trust with potential victims who are then duped or coerced into providing information needed for fraud or to pay money to fraudsters. Devices are used to disguise voices for telephony-based frauds.

### Criminals increasingly operate across borders

Frauds affecting the UK are often linked to networks of criminals operating across the UK and overseas. Fraudsters are also investing significant time and resources to hide their criminal profits. The Financial Action Task Force estimates that fraud is now the second biggest source of global money laundering<sup>3</sup>. The increased efficiency of international financial transactions and variety of financial products means that funds can be moved across continents swiftly through different channels.

<sup>2</sup> The UK Organised Crime Threat Assessment, Home Office, 2010

<sup>3</sup> FATF Global Financial Crime Assessment, 2010

## CASE STUDY

A pro-active City of London Police investigation focused on a serious organised crime group involved in share fraud (sometimes known as 'boiler room' fraud). The criminal enterprise targeted a number of vulnerable UK-based victims to invest in fraudulent shares in excess of £20m (the single biggest victim loss was £1.4m). Suspects and victims were widespread across the UK. The criminal operation's centres were spread across Spain, Sweden and Italy and profits were laundered across Northern Europe. The criminal organiser was arrested and the organised crime group dismantled within three months of the start of the investigation.

### Fraud is linked to other serious crimes

Fraud can be a primary activity for organised crime groups or a funding device for other serious crimes. At least £9bn of the £38bn fraud losses in the 2011 National Fraud Authority Annual Fraud Indicator<sup>4</sup> is perpetrated by organised crime activity. The faceless nature of fraud contributes to the view that some members of the public see fraud as a less serious offence than other acquisitive crimes. In reality, the organisers of fraud networks are often violent criminals doing harm to our businesses, public services and communities.

Fraud has also been used as a means of funding terrorist activities. While the value of these frauds may be relatively small and thus difficult to detect, they can be sufficient to purchase bomb making materials and facilitate terrorism in other ways.<sup>5</sup>

### Not all fraud is linked to organised criminal gangs

The majority of frauds are not perpetrated by sophisticated, organised criminal gangs. They are a variety of opportunistic frauds and those which require a degree of sophisticated planning – often coupled with insider knowledge and access but without links to a wider organised criminal enterprise. The former are facilitated by dishonesty; a culture that tolerates fraudulent behaviour 'at the margins' and does not always acknowledge it as criminal; weak procedures, systems and controls in organisations; and lack of information sharing between organisations, for example about employees dismissed for fraud. Cumulatively, the financial cost of these frauds to society is greater than that perpetrated by organised criminal gangs, though the number of offenders and victims is higher (and therefore more challenging to tackle) and the size of individual losses is lower, meaning that cases may fall below thresholds for detailed investigation.

### Many frauds rely on one or more enablers to succeed

Clearly the fraud threat is diverse. There are, however, common enablers that are often used by criminals. An enabler is an instrument, process or organisation that facilitates or assists in the opportunity to commit fraud. Tackling an enabler is often a more effective way of disrupting a wider range of frauds, rather than chasing individual occurrences.

<sup>4</sup> <http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/annual-fraud-indicator/>

<sup>5</sup> FATF Terrorist Financing Typologies Report, 2008

Categories of enabler include:

- **Identity exploitation** – which includes: the theft of genuine identity information which is then used to obtain goods or services fraudulently; forging documents commonly used to prove identity such as passports, identity cards, driving licences and immigration documents: and – most prized of all by fraudsters – fraudulently obtained genuine documents (FOGs). There is also a significant organised criminal trade in identity data and documents (both forged and FOGs).
- **Online techniques** – to compromise information systems remotely, often to steal personal identity and financial information with which to commit fraud.
- **Corrupt professionals and staff** – important facilitation services to fraudsters can be provided by corrupt professionals. For example there have been instances of corrupt professionals facilitating both mortgage and insurance fraud. Staff (including contractors with access to organisations' systems and premises) can be in a powerful position to use their access and insider knowledge to commit fraud and cover their tracks.
- **Physical technologies** – which can be used to compromise systems and controls, for example the use of PIN entry devices to steal PINs to facilitate credit and debit card fraud.
- **Use of persons or products to launder the profits of fraud** – fraudsters need a variety of means to gain access to their criminal proceeds, such as the use of 'money mules' to transfer stolen funds.
- **Mass marketing approaches** – which allow a large number of victims to be targeted at relatively low cost and risk to criminals.
- **Misuse of legitimate businesses** – such as accommodation addresses to receive goods purchased fraudulently.

Enablers are often used in combination, for example corrupt staff or contractors using physical technologies to compromise systems. Our knowledge of the relationships between types of enablers and different categories of fraud (and other serious crimes) has improved. Further mapping is needed to build our knowledge further and to target effective solutions.

## The future trajectory of the threat

The factors which will most affect the future trajectory of the fraud threat are those linked to the increasing use of – and dependency on – online technologies to deliver services and the sophistication of organised criminals to exploit weaknesses and use technology to support their criminal businesses. As more people manage their personal and financial affairs online, they put themselves at risk if they do not have the requisite awareness of the risk and ability to protect themselves. As more organisations offer access to their services online the potential threat also grows if they do not adopt good practice in the design, testing and operation of their systems.

Another important factor is the risk organised criminals perceive in engaging in fraud as opposed to other types of organised crime. There is evidence that organised criminals shift activity into areas they perceive to be of lower risk, both in terms of the likelihood and the consequences of being caught.

Alongside these upward pressures on the trajectory, there is evidence that where fraud problems are well understood, targeted interventions do work – such as the introduction of chip and PIN technology for credit and debit card payments, which reduced losses on high street transactions by 69% between 2004 and 2010.

## Behaviours and attitudes

The behaviours and attitudes of businesses, individuals and public bodies and the extent to which they take account of fraud risks can determine their likelihood of being targeted by criminals. They may inadvertently make fraud easier by not taking the right measures to stop themselves becoming victims or being complicit in offending. Understanding these behaviours and attitudes and, where necessary, changing them is vital for an effectively targeted strategic approach to reducing fraud.

### Victims and wider society

The National Fraud Segmentation<sup>6</sup> divides the public into different groups depending on their experience of – and behaviour and attitude towards – fraud and their social demographics. Age, income, gender, employment and attitudes to risk are all relevant. This more sophisticated understanding of the behaviours and attitudes of victims and potential victims will help to target better prevention messages in terms of both content and how those groups prefer to receive messages. However our broader knowledge of attitudes to fraud across business sectors and the public sector is less advanced and needs to be improved.

There are also wider societal attitudes which allow fraud to fester and be tolerated. There are those who do not view low level fraud as criminal behaviour – whether it is manifested as benefit fraud and tax evasion where the community remains silent, or by people who ‘gild the lily’ when making insurance claims or who lie on application forms for credit cards or mortgages. There are also some victims who can become complicit in a scam who justify to themselves that they are not helping to facilitate the crime of fraud. Other victims can feel that it was their fault for falling for a scam and take no action to report it. Indeed the very word ‘scam’ implies something slightly less serious than a crime. This tolerance of fraud can also be manifested in the attitudes of organisations who decide not to report crime, who ‘let go’ or ‘pay off’ fraudsters rather than apply a sanction such as prosecution and dismissal (which allows them to perpetrate their crimes against other organisations), and who do not provide their employees with a secure and confidential means of whistle blowing. It is also manifested in the reluctance of some law enforcement organisations to take on fraud cases.

### Offenders

Criminals generally weigh up the risks and benefits before deciding whether to perpetrate fraud. This applies to the most organised criminals as well as opportunistic offenders. Some offenders will be deterred by the likelihood and consequences of detection and punishment; others will continue to offend even after custodial sentences. For some it is the loss of assets gained through their crimes that they fear most.

<sup>6</sup> <http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/national-fraud-segmentation>

## The damage caused by fraud

Clearly fraud causes significant monetary losses to individual citizens, businesses and public bodies. The best estimate of these losses is set out in the 2011 National Fraud Authority Annual Fraud Indicator<sup>7</sup>:



Of the £38bn of losses, £21bn is against the public sector. This has huge implications for already constrained budgets within public bodies, undermines the effective provision of public services and can contribute to a perception of unfairness in the allocation of resources.

Research conducted in 2009 demonstrated that the vast majority of individual victims face practical and monetary impacts from fraud and are focused on getting their money back. However some victims, often the most vulnerable members of our society, can suffer emotional harm from fraud. These victims require more intensive guidance and counselling.

<sup>7</sup> <http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/annual-fraud-indicator/>

Losses incurred by the private sector affect shareholders and may also be passed on to customers. It is estimated that insurance fraud adds, on average, an extra £44 a year to every UK household's annual insurance bill. The effects on small and medium sized businesses are less well understood but examples include loss of business where companies refuse to co-operate with fraudulent tendering exercises, reluctance to conduct business online because of fears of fraud risks and in some cases the complete failure of a business with loss of livelihood for the owners and job losses for employees.

## Strengths and weaknesses of our response

### Strengths

Recent investment by public and private sector organisations has resulted in genuine improvements to national capabilities to tackle fraud.

#### **Victims are better supported**

Individual victims and small and medium sized businesses are now able to report fraud either online or by phone to Action Fraud. Online, telephone and face to face advice is available to help victims repair the damage caused and to protect themselves better in the future. The volume of victims contacting Action Fraud is increasing. There have been over 420,000 website visits and calls to the contact centre since the service began and monthly volumes have risen four-fold with independently assessed satisfaction levels at over 95%.

#### **High priority frauds and enablers are being targeted**

Multi-agency programs of work are in place to prevent and disrupt the highest priority fraud enablers such as identity crime and enablers to mass-marketing fraud. The government has announced significant investment to improve the response to computer-enabled crime as part of the National Cyber Security Programme. Particular types of fraud, such as mortgage fraud and fraud against the benefit system, are being proactively dealt with by individual organisations and groups of organisations.

#### **Stronger collaboration within and across sectors**

Leading businesses, such as banks, the payments industry and insurance companies, are joining forces to strengthen their industry wide abilities to tackle frauds, as well as engaging with local and central government and law enforcement such as sharing data with the National Fraud Intelligence Bureau.

The fight against public sector fraud has been re-energised and now has a wider focus than the historical emphasis on fraud against the tax and benefit systems. The Government's Fraud, Error and Debt Taskforce has put in place a network of counter fraud champions across central and local government who are sharing good practice to tackle fraud. The Taskforce has also piloted the use of good practice which has detected and prevented, immediately, fraud losses of £12m. Once rolled out, this will save £1.5bn by 2014/15. In parallel work is underway to develop the first ever counter fraud strategy for the whole of local government in England.

### Better targeted enforcement activities

Law enforcement capabilities are being strengthened by measures such as the National Fraud Intelligence Bureau receiving and analysing increasing volumes of fraud crime data, with intelligence packages then being disseminated for targeted investigations.

#### **CASE STUDY: Integrated reporting and intelligence – combining hard-edged enforcement with preventative activity**

Action Fraud began experiencing high volumes of contact relating to a foreign based company, that operates in the UK via the internet, offering short term loans. Within just three days over 2000 reports had been received and passed to the National Fraud Intelligence Bureau (NFIB). The NFIB collated and quickly analysed the reports, before producing intelligence to ensure an investigation could run simultaneously with a public awareness campaign. Enquiries by the City of London Police identified that the personal details of a significant number of people had been stolen and used to obtain loans from the victim company.

The victim company only became aware of how many loans had been fraudulently obtained when members of the public received requests for loan repayment and began reporting to Action Fraud. Further investigation by the NFIB revealed that the fraud had affected some 9,000 individuals from across the UK and led to losses by the victim company to the value of approximately £3m. A number of suspects are now the subject of the judicial system.

### Increased awareness of fraud

The profile of fraud has been increased amongst senior decision makers in government and the private sector, resulting in increased investment and focus. More collective action across the public sector in areas such as procurement fraud is underway. The insurance industry has recently announced its intention to fund a dedicated police unit based in the City of London Police to boost enforcement, prevention and disruption activity following the example set by the UK payments industry which has funded the Dedicated Cheque and Plastic Crime Unit for nine years. This has saved the industry an estimated £370m. The telecommunications industry has provided a secondee to the National Fraud Authority and is also working to share data with the National Fraud Intelligence Bureau. Following a major survey on the cost of fraud to charities in 2010 a project on charity fraud has been commissioned to develop fraud prevention solutions and guidance for this sector.

Many of these improvements are recent and will show their full value in the coming years. There remain, however, strategic weaknesses that need to be addressed.

### Weaknesses

#### **We need to make better use of our intelligence gathering and analysis capability**

There are a number of industry, government and law enforcement fraud intelligence assessments which are not brought together to give one common, authoritative picture. Tactical intelligence/ data sharing within sectors and between the public and private sectors is not sufficiently efficient or widespread, meaning that proactive prevention opportunities are lost. Our intelligence picture is too focused on present threats and does not look sufficiently ahead to emerging trends and threats.

### Limited self protection

Too many individuals and organisations do not understand fraud threats and how to deal with them and therefore we miss considerable opportunities to prevent fraud before losses occur.

### Criminals continue to use enablers

Criminals access and use the resources they need for fraud too easily – whether these are people, materials or finances.

### Frauds are still unreported and too few reported frauds are dealt with proactively

Action Fraud took 12,269 formal crime reports in the 2010/11 financial year alongside the 145,841 reports recorded by the police in England & Wales. The service is starting to make an impact in increasing fraud reporting but it needs to become the primary route for individuals and small and medium sized businesses to report fraud.

Only 24% of the frauds reported to and recorded by the police in England and Wales in 2010/11 resulted in some form of criminal justice outcome and we know that many frauds are never reported in the first place. While serious frauds with high financial losses tend to be investigated, it is often a lengthy process to secure convictions and denial and recovery of assets remain a serious challenge. While there are pockets of good practice, overall there is insufficient use of other methods to disrupt fraudsters and recover funds such as civil litigation, ancillary orders and professional sanctions.

### There is an imbalance between prevention, disruption and enforcement

All successful crime reduction initiatives have placed a heavy emphasis on prevention. There has been too little focus on prevention, especially in the public sector where organisations' incentives can lead them to adopt a 'pay first, check later' approach. However it can still be a challenge for organisations to make the business case for fraud prevention and disruption where the benefits can be more challenging to measure than those linked to conventional investigation and criminal justice outcomes. In its interim report, published in June 2011, the Government's Fraud, Error and Debt Taskforce places prevention at the heart of tackling fraud in the public sector.<sup>8</sup>

A number of disruption tools and approaches sit within particular organisations or sectors and other organisations are not necessarily aware of how and where they could be used.

### Many organisations and sectors do not understand how fraud affects them and what they can do

Those sectors which most understand their fraud problems tend to be most active in seeking solutions, for example HM Revenue and Customs and the Department for Work and Pensions in the public sector and the payments and insurance industries in the private sector. Our collective fight against fraud needs to engage with those industry sectors and parts of the public sector where all the evidence points to considerable fraud losses but little co-ordinated action to reduce them. We need to make these sectors aware of both the problem but also how they can quickly learn from the experience from those sectors which are more advanced.

The Government's Fraud, Error and Debt Taskforce has already established a network of counter fraud champions across Government in an effort to improve knowledge of fraud against Government departments. This is being supplemented by departments now publishing their detected fraud on a quarterly basis.

<sup>8</sup> <http://www.cabinetoffice.gov.uk/resource-library/eliminating-public-sector-fraud-counter-fraud-taskforce-interim-report>

## SECTION 2:

# Strategic direction

*Fighting Fraud Together* signals a new partnership between the public, private and voluntary sectors to tackle fraud. By working collectively, the sum of our efforts will have more impact. For this partnership to succeed, we need to be absolutely clear on our strategic direction. This section seeks to provide this clarity by articulating our ambition, strategic objectives and priorities.

## Our ambition

“By 2015 our country will be demonstrably more resilient to and less damaged by fraud through:

- Individuals, businesses, public and voluntary bodies **detecting** and **preventing** more fraud.
- Law enforcement and other partners increasing the risk of **disruption** and **punishment** to organised and opportunistic fraudsters, thus **deterring** potential criminal offenders”.

## Strategic objectives

It is quite clear that stopping frauds happening in the first place is the most effective approach. This reduces the damage caused by fraud and frees up resources so businesses and the public sector can serve their customers and law enforcement can focus on areas where they can have greatest impact. *Fighting Fraud Together* increases the strategic emphasis on activities which prevent fraud. This will comprise two distinct elements:

- Promoting greater awareness of fraud risks and actions and instigating the behaviours that individuals, businesses and public services can change to enable self-protection and help to change the culture which tolerates a certain level of fraud in our society.
- Embedding stronger counter fraud controls and systems within organisations of all sizes including, in future, ways of delivering services so that fraud risks are ‘designed out’.

Greater awareness and investment in stronger fraud controls will reduce fraud, but not all frauds can be prevented. The most determined and organised criminals have the resources to beat even the strongest counter fraud controls. Opportunistic frauds will occur where criminals think they can get away with it and particularly where individuals have some insider knowledge of the weaknesses of an organisation’s processes. Therefore our drive towards greater prevention of fraud will be balanced with an enhanced, more effective and more efficient enforcement response. There will be better targeting of resources and the risk to fraudsters of disruption and punishment will be increased. This will drive up the costs of fraud to the criminals, alter their perception of risk and deter potential future fraudsters.

This balanced approach is encapsulated in our three strategic objectives:

- I. **AWARENESS:** We will prevent more fraud by achieving a step change in **awareness** of fraud among the general public and organisations in the private, public and voluntary sectors and in their ability to protect and safeguard themselves.
- II. **PREVENTION:** We will **prevent** more fraud through stronger systems and controls in our businesses and public and voluntary services.
- III. **ENFORCEMENT:** We will strengthen our response to be **tougher** on fraudsters by **disrupting** and **punishing** them more efficiently and effectively.

## Priorities

The fraud threat is wide ranging and we need to prioritise our resources where they will have most impact. Based on our assessment of the fraud challenge, our efforts will be focused in these areas.

### New activities against enablers

By tackling enablers, a cross cutting impact can be achieved on many types of fraud. We will work with industry sectors to map the particular enablers that cause them most harm, bring those maps together to confirm or identify new common threats and, most importantly, develop prevention initiatives and measure their outcome. This mapping exercise will be a high priority for the first year of *Fighting Fraud Together*. We will also continue with and introduce new initiatives on identity crime, corrupt professionals and cyber enablers of fraud. Our work on enablers contributes to all three of our strategic objectives, for example by:

- Helping people protect themselves from identity theft and computer-enabled crime.
- Ensuring that new online services have adequate protections from cyber crime attacks.
- Targeting enforcement activity against corrupt professionals who facilitate fraud.

### Supporting fraud awareness and prevention activity in more high priority sectors

Within a number of high priority sectors, such as the financial services sector, businesses are working together and collaborating with central and local government, law enforcement and their customers to tackle fraud threats. There are though some sectors where there are high risks of fraud which lack the same level of response. Through *Fighting Fraud Together*, more sectors will be encouraged to join the community and we will offer them the fruits of our experience so they can protect themselves better.

There is a particular challenge in reaching out to small and medium sized businesses which have a pressing need for more practical fraud prevention advice. We will build on the experience of our segmentation analysis of individual victims to improve our understanding of this sector and its needs.

## Improving our knowledge, and putting it to effective use

We are not interested in improved knowledge of fraud for its own sake. We will develop our knowledge where it can help prioritise and target our activities.

We will share and co-ordinate our intelligence gathering and analysis capabilities better and establish a unified common strategic view of the fraud threat which we will share across sectors. We will do this in concert with the National Crime Agency proposals for an expert analytical function, playing a more strategic role – a Joint Serious and Organised Crime Assessment Centre.

We will develop an intelligence sharing roadmap that facilitates the sharing of information on known fraud and fraudsters across the public and between the public and private sectors. The intelligence sharing roadmap envisages an intelligence sharing architecture by which the combined intelligence on known and suspected fraud – and fraudsters from across a number of public and private sector hubs – can be fully utilised to detect and prevent fraud far more effectively.

Intelligence shared through the intelligence sharing architecture will be used for three purposes:

- To drive stronger focus on prevention by giving organisations access to known fraud data from all sectors on a regular and timely basis; and to increase prevention by better coordination between sectors.
- To identify networks of organised fraud within sectors and across sectors, and link fraud intelligence to other threat areas such as organised crime and cyber crime to enable a prioritised level of operational response through the National Crime Agency and its partners.
- To optimise the enforcement response against fraud at three levels – fraud against a particular organisation, fraud against multiple organisations within a sector and the most organised cross-sectoral fraud.

The intelligence sharing roadmap will build on and enhance facilities we have established to date such as the National Fraud Intelligence Bureau, HM Revenue and Customs' CONNECT, the Department for Work and Pensions' Integrated Risk and Intelligence Service, the work of the Metropolitan Police Service's Operation Amberhill to collect and disseminate information on false identity documents, the Insurance Fraud Bureau and the Audit Commission's National Fraud Initiative – and by encouraging industry sectors and parts of the public sector to adopt solutions proven to work elsewhere. We will encourage and facilitate work within the banking industry to develop common standards for the handling of fraud information across the sector and then broaden this work to cover other sectors.

Now that we have a better understanding of the risk of fraud to particular segments of the population, we will monitor and evaluate the effect of targeted prevention messages on them. We will also work with the voluntary sector to use their networks to reach more vulnerable victims and potential victims.

We will further improve our measurement of performance in preventing, disrupting and punishing fraudsters. In particular we will seek to reflect the contribution of private sector organisations which take civil measures against fraudsters, develop measures on prevention and help bring more sectors up to the standards of the best in measuring fraud losses and the effect of interventions to reduce them.

### CASE STUDY: Sharing intelligence to identify compromise of payment cards at a specific merchant location

One of the ways the payments card industry combats fraud is through the use of data analytics to detect fraudulent transactions. The actionable intelligence it derives from these systems is used to assist with its fraud prevention strategies, to identify potential accounts at risk and to trigger investigation by the appropriate areas, whether that is the merchant acquirer, card payment schemes or law enforcement agencies.

Where a card issuer's system flags potential fraudulent transactions and detects a certain level of suspicious activity at a merchant, the card issuer sends an alert to the industry's Financial Fraud Bureau (\*FFB). The FFB then collates additional information regarding the merchant and notifies the appropriate parties of the suspicious activity in order that appropriate action can be taken to prevent losses.

*\*FFB is part of the UK Payments Fraud Control Unit and is responsible for managing the payment industry's coordinated initiatives regarding data sharing to reduce fraud, covering all types, including card, payments, lending and cheque fraud. The unit is recognised as an industry leader and enables its customer groups to share data through a secure and trusted process. It also provides data directly to police forces and law enforcement organisations.*

### Strengthening the enforcement response

In June 2011 the Government published a plan for the creation of a national crime-fighting capability, the National Crime Agency (NCA). A key part of the NCA will be an Economic Crime Command. The Economic Crime Command will ensure a coherent approach to the use of resources focussed on economic crime across the full range of agencies deploying them. Driving closer working and more effective use of resources will address the current negative effects of having separate pools of specialist expertise pursuing highly complex areas of offending in a fragmented landscape. Based on intelligence, the Economic Crime Command will draw on the NCA's overall authority to task to ensure a consistent approach to how economic crime cases are prioritised and which agency takes them on. It will work closely with the National Fraud Intelligence Bureau in the City of London Police and with the centralised intelligence functions within the NCA.

We will rise to the challenge of constraints on police resources by developing innovative, partnership solutions working across police forces, the National Crime Agency and its Economic Crime Command, other law enforcement organisations and the public, private and voluntary sectors.

We will collate and disseminate good practice on the prevention and disruption of fraud which has been pioneered by individual law enforcement organisations but has not been embedded in the national response.

We will review and strengthen our engagement with international partners, targeting those parts of the world which fraudsters exploit to run or facilitate their operations and launder the proceeds of their crimes.



Association of British Insurers



ASSOCIATION OF  
CHIEF POLICE OFFICERS

## Use of civil litigation to bring fraudsters to justice

We will work with civil litigators to raise the profile and use of civil litigation as a means to bring some fraudsters to justice and deny them access to their criminal assets. We will work particularly to encourage its use in sectors where there is little awareness and experience of its use.

## Support to victims

We will expand the Action Fraud service so that it takes more of the crime and incident reports which currently are handled by the police, passes reports of incidents as well as crimes to the National Fraud Intelligence Bureau and takes reports of financially motivated cyber crimes and incidents. This will give victims a better and more consistent service and help them to avoid becoming repeat victims.

## Further intensifying work to fight public sector fraud

The fight against public sector fraud will be further intensified around the four priorities agreed by the Government's Fraud, Error and Debt Taskforce in June 2011:

- **Collaboration** – silos must be removed; all parts of the public sector must work together by: sharing intelligence on fraudsters; developing cross-cutting capabilities; initiating joint projects using data analytics; and ensuring we jointly procure data analytics capabilities to drive down costs.
- **Assessment of risk and measurement of losses** – fraud risk must be assessed before projects and programmes are under way. Losses should also be recorded and reported via the quarterly data summary.
- **Prevention** – investment and resource should go into prevention, not just detection and punishment. When vulnerabilities are detected as part of risk assessment, they should be designed out.
- **Zero tolerance** – there is no acceptable level of public sector fraud.

## Strengthening the coordination of our response

Fraud affects so many sectors of our economy and society and can be such a complex crime that how we have structured our response has appeared to be similarly complex and uncoordinated. The creation of the Economic Crime Coordination Board in Autumn 2011, as the first tangible part of the National Crime Agency's Economic Crime Command, is an opportunity to strengthen coordination of the sharing and use of intelligence, the capacity and effectiveness of the law enforcement response and prevention activity across all sectors.

The wide range of organisations involved in fighting fraud can often mean that we do not take the time to coordinate our messages and use each other's networks to reinforce them. The National Fraud Segmentation provides a good basis on which to develop and measure the effectiveness of a more coordinated approach across all sectors, not just to prevent people and organisations become victims of fraud but as part of the wider challenge to change the culture and society's tolerance of fraud.

## SECTION 3:

# Strategic delivery

All the parties involved in *Fighting Fraud Together* are facing significant financial and budgetary challenges. We need to have a simpler, clearer delivery structure and use the opportunity that *Fighting Fraud Together* gives us to make the collective and individual, sector-specific, choices which will have most impact in reducing fraud.

### An effective strategic framework for delivery

The diverse nature of fraud offending means that there are a wide range of organisations, both public and private sector, involved in tackling it. A governance structure that embraces these organisations is key to ensure that the right people meet to get the right things done, at the right time and to the right specification. We will establish new delivery structures that will:

- Bring together key senior decision makers and organisations across **all** sectors to encourage stronger strategic collaboration to reduce fraud and help remove blockages to progress. The old arrangements did not operate at a sufficiently senior level, in particular lacking in regular and direct access to Ministers. This has changed for public sector fraud with the establishment of the Government Fraud, Error and Debt Taskforce chaired by the Minister for the Cabinet Office. The Economic Crime Coordination Board, the first elements of which will be operating by Autumn 2011, will comprise key agencies from across the economic crime landscape and will have a strong role in driving better coordination of cases and alignment of resources across agencies.
- Bring together key delivery agents in *Fighting Fraud Together* to report progress on their initiatives, to oversee delivery of the priority cross-cutting initiatives and to share information and good practice. This will also allow issues to be escalated to more senior decision makers when necessary.

We will disband some existing committees and clarify the terms of reference of others to avoid areas of overlap and duplication which have crept in over the years.

The governance arrangements we will establish for *Fighting Fraud Together* will not supplant individual organisations' reporting lines and accountabilities. They will be designed to achieve greater transparency across the different sectors of the activity which is taking place, encourage organisations to work collaboratively, validate that our activities reflect and contribute to our agreed strategic objectives and provide a means of escalating issues to senior decision makers.

### The programme and compendium of activity

There will be a programme of activity which incorporates the key – mainly cross-cutting – initiatives we will undertake to reduce fraud. Some of these initiatives will account for their delivery directly to the governance arrangements for *Fighting Fraud Together*. Others will be held accountable by other bodies for example

the Organised Crime Threat Reduction Board which focuses particularly on the law enforcement response to fraud perpetrated by organised crime and the ACPO Economic Crime Portfolio which oversees the policing response to economic crime. What is important is that lines of accountability for delivery are clear but that progress on delivery of initiatives is visible to everyone involved in *Fighting Fraud Together* without organisations having to attend many different meetings with overlapping remits to get the full picture. The programme of activity will be a living document which will be regularly updated to reflect progress and incorporate new initiatives as they are initiated. We will make as much of it as possible available publicly and also produce a summary version highlighting progress in the most important areas.

Alongside the programme of activity the National Fraud Authority will develop and maintain a log of other counter fraud activities which, while less cross-cutting in nature, still make an important contribution to tackling fraud within a particular sector, organisation or government department. This compendium of activity will, as far as is possible, be available to all the members of the *Fighting Fraud Together* partnership. The programme and compendium of activity will allow all the *Fighting Fraud Together* participants to understand better the breadth of everyone's activity and share good practice by identifying initiatives which they may want to join or learn from. It will also prevent duplicate and overlapping projects arising and foster new partnerships.

### Measuring success

We will measure the success of our work around the delivery of our three strategic objectives: awareness, prevention and enforcement. There is no one single measure of success that can reflect the size, complexity and ambition of *Fighting Fraud Together*. It is our ambition that by 2015:

- There will be greater measurable awareness of fraud, and a quantifiable step change in behaviours and attitudes which increase vulnerability to fraud, across all sectors of society and the economy – and a greater knowledge among people and organisations of how to protect themselves. During 2012, using segmentation analysis, we will baseline awareness and self-protection from fraud across vulnerable groups leading to more effective preventative measures over the course of this strategic plan.
- Future Annual Fraud Indicators will provide confidence levels in estimates of fraud loss against victims in the public, private, and not-for-profit sectors as well as against individuals. We will strengthen fraud measurement so that we have a more robust measure of the scale and breakdown of fraud losses allowing us to target fraud resources to the greatest benefit.
- For those areas where greater confidence in levels of fraud losses exist, we will have demonstrated the scale of fraud reduced and prevented. Using them as a basis, where the scale of fraud losses are less clear we will help to develop more effective measures to demonstrate how new systems and controls have led to greater levels of prevention.
- Building on the Economic Crime Coordination Board's objective to support organisations to tackle economic crime more effectively, we will establish sophisticated and comprehensive measures of disruption and enforcement activity covering both criminal and civil processes, properly acknowledging the role which the private sector plays.

We will use a basket of indicators which we expect to show improvements in performance over the next four years. The table below provides more information on the high level measures of success which we will develop in more detail as the *Fighting Fraud Together* programme of activity gets underway.

AWARENESS		
Objective	What does success look like?	How will it be measured?
<p>We will prevent more fraud by achieving a step change in awareness of fraud among the general public and organisations in the private, public and third-sectors and in their ability to protect and safeguard themselves.</p> <p>This will include targeted actions to deal with the individual behaviours and attitudes that allow criminals to perpetrate fraud.</p>	<p>Businesses, public sector and voluntary sector organisations and individuals are <b>measurably better able to detect fraud and more proactive in taking action to protect themselves from fraud.</b></p>	<p>① <i>Raising awareness</i> Regular, comparable surveys of fraud awareness, prevention awareness &amp; behaviour, victimisation and victim satisfaction. Some surveys will be targeted at particular industry sectors, especially where our current knowledge of their fraud awareness and prevention capabilities is poor.</p> <p>② <i>Specific alerting activity</i> Monitor alerting activity amongst the counter-fraud community. How quickly do we pass on messages which help to protect people and organisations and how useful do the recipients find them?</p>

PREVENTION		
Objective	What does success look like?	How will it be measured?
<p>We will prevent more fraud through stronger systems and controls in our businesses and public and voluntary services.</p> <p>This will include designing out fraud and making preventative checks before transacting with individuals and organisations.</p>	<p>Businesses, public sector and voluntary sector organisations are <b>more resistant to fraud, with more attempted frauds detected and stopped.</b></p>	<p>③ <i>Measure frauds prevented</i> We will develop much better measures of performance for fraud prevention and encourage more organisations to adopt them. We will focus initially on those sectors which measure their fraud losses well and have developed a range of interventions to prevent fraud. We will spread this good practice more widely to other sectors and help them justify investment in improved processes, controls and systems to prevent fraud.</p> <p>④ <i>Measurement of individual initiatives and approaches</i> To supplement ③ above, we will also monitor the prevention benefits of specific initiatives and approaches (such as suspending websites used by fraudsters) and use them as exemplars for other organisations to adopt.</p>

ENFORCEMENT		
Objective	What does success look like?	How will it be measured?
<p>We will be tougher on fraudsters by disrupting and punishing them more efficiently and effectively.</p> <p>This will include more effective civil and criminal processes, as well as greater early restraint of criminal assets.</p>	<p>There is more effective action against the highest priority criminals <b>perpetrating fraud</b>. Capable operational units investigate the highest priority fraud targets, using the best intelligence from both public and private sectors. The role of the private sector is properly acknowledged.</p> <p><b>Victims satisfaction rates increase as they are better supported</b> by more efficient and robust justice, strengthened care arrangements and greater monetary returns from asset recovery and compensation.</p>	<p>5 <i>Improved management information on disruption activity and outcomes.</i> Supplementing the measurement of improved fraud awareness and prevention work we will measure the amount of public and private sector disruption activity and outcomes from this.</p> <p>6 <i>Improved management information on enforcement activity and outcomes</i> We will improve the current arrangements for collection and analysis of management information on counter fraud activity from the main law enforcement agencies, specifically in the areas of the types of fraud under investigation, the time taken to bring offenders to justice (criminal and civil), disruption activity and outcomes and asset denial and recovery. We will also begin to collect information on the use of civil processes by private sector organisations.</p>

## Relationships with other strategies and programmes

*Fighting Fraud Together* is closely linked with a number of major Government strategies and programmes which themselves involve partnership working with private sector and voluntary organisations. In part this will be reflected in the *Fighting Fraud Together* programme of activity which will record where responsibility will lie for overseeing delivery of some initiatives. For example, improved reporting of cyber and computer-enabled fraud will be delivered by the National Fraud Authority under the National Cyber Security Programme with details set out in the Cyber Security Strategy. The key relationships are with:

- **National Crime Agency plan**, for the development of the Economic Crime Command. *Fighting Fraud Together* will provide the initial strategic direction for the work of the Economic Crime Coordination Board.
- **Cyber Security Strategy**. A new national Cyber Security Strategy is currently being finalised by the Office of Cyber Security and Information Assurance in the Cabinet Office. It will set out how £650m of new investment under the new National Cyber Security Programme will enhance and intensify cyber security activity across the UK, including £63m to transform our ability to tackle cyber crime. Action Fraud will become the single point for reporting financially motivated cyber crime and computer-enabled fraud.
- The Government's **Fraud, Error and Debt Taskforce** will oversee the delivery of measures to tackle fraud against Government, which will be published in the winter. It will also support efforts to tackle fraud in the wider public sector, including the NHS and local government.
- **Organised Crime Strategy, *Local to Global: Reducing the Risk of Organised Crime***<sup>9</sup>, where *Fighting Fraud Together* contributes in particular to the **STRENGTHEN** and **SAFEGUARD** pillars.

The **STRENGTHEN** pillar's objective is focussed on hard-edged enforcement through prosecutions where practicable, but also the use of a wider range of innovative disruptions. Through our current intelligence and planned intelligence architecture we will support more effective and efficient use of our law enforcement resources against organised criminals. A key part of this will be through clear links between the National Fraud Intelligence Bureau and centralised organised crime intelligence.

We are also supporting efforts to broaden the range of tools available to tackle organised criminals, including civil powers and by spreading best practice to increase law enforcement agencies' contribution to preventative initiatives. The Organised Crime Strategy's focus on enablers is also supported through a mapping of key fraud enablers many of which cross-over to other types of offending.

<sup>9</sup> <http://www.homeoffice.gov.uk/publications/crime/organised-crime-strategy>

The **SAFEGUARD** strand is focussed on reducing the vulnerability of communities, businesses and the state to becoming victims of organised crime. Given the strategic priority placed on this approach in *Fighting Fraud Together* we will play a key part in delivering this strand of the Organised Crime Strategy. Our activities will be those focused on awareness raising and behaviour change activity and alerting. Given the importance of the **SAFEGUARD** approach to tackling fraud and organised fraud we have sub-divided this into our two prevention-focused aims: **AWARENESS** and **PREVENTION**.

Under the Organised Crime Strategy the National Fraud Authority and its partners in the counter-fraud community have the following actions, which are all reflected in the *Fighting Fraud Together* programme of activity:

- The National Fraud Authority, through Action Fraud, will help coordinate the awareness raising and behaviour change activities of the counter fraud agencies for the public and business.
- The National Fraud Authority will develop and issue a best practice guide on fraud prevention to counter fraud agencies.
- The National Fraud Authority and the National Fraud Intelligence Bureau will ensure that fraud alerts to the public, businesses and the public sector are coordinated and effective, reaching the right audience at the right time.
- The National Fraud Authority will lead the development of a new strategic approach to tackling fraud across the public, private and non-profit sectors, to be published Autumn 2011.
- The National Fraud Authority and Charity Commission will develop a strategic response to reducing the threat and impact of fraud against the charitable sector.
- The National Fraud Authority and its partners will also be contributing to other actions, including on intelligence, enhancing the criminal justice approach, research, measuring impact and tackling the associates and enablers of organised crime.

