Inspecting policing in the public interest

HMRC's use of information and intelligence to counter fraud in the tax credits system

May 2011

www.hmic.gov.uk

Contents

1: Executive summary

1.1 HMRC is clearly on a journey as it re-mobilises and prioritises around its new strategy to ‘check now then pay’. The overall direction of travel is to be applauded, and the Senior Management of Benefits and Credits (BC) deserve much credit for turning the ship around. When tax credits were introduced in April 2003, little attention was given to whether the right money was going to the right people. The system has now been stabilised and the new strategy has been well received and is achieving results, with losses to incorrect payments (referred to by HMRC as ‘yield’) progressively controlled, leading to savings of £250 million in 2008/09 to £650 million in 2009/10 and £1 billion in 09/10.

1.2 Staff show genuine energy and enthusiasm in wishing to engage with the new strategy and detect and prevent fraudulent attacks on the system. However, this report concludes that unstructured governance and co-ordination of the overall anti-fraud strategy and resources, coupled with the focus on yield, are compromising HMRC’s ability to mobilise and deliver the most appropriate intelligence interventions.

1.3 This report also considers whether HMRC Benefits and Credits (BC) is properly structured and aligned with its key stakeholders to maximise the flow and utilisation of all available intelligence. It also examines whether, in the emerging fight to combat large-scale fraudulent attacks, HMRC BC is being asked to deliver in a specialist area in which it has no real experience, expertise, or therefore competence – which is perhaps understandable, given that its core business has always been to manage an outward-facing tax regime where payments of awards have historically come above considerations of fraud.

1.4 Whilst HMRC makes attempts to measure error and fraud in singleton claims there is evidently no overall picture of loss, because the extent of organised criminal attacks on the system remains unknown. Current estimates of loss to organised criminal attacks lie between £20 million and £400 million.

1.5 HMRC does not seek to hide the fact that their Error and Fraud Assurance Programme (EFAP) does not include the unquantified organised fraud losses (e.g. identity fraud is not included). However, as the only published measure of fraud in the system HMRC risk creating a public perception that that all ‘Error and Fraud*’* is being measured and consequently any progress toward their key strategic objective to reduce ‘error *and fraud’* from a central estimate of 8.9% in 2008/09 (of final award by value) to 5% by 2011 could also be construed as misleading. HMRC should therefore aspire to develop a more holistic fraud measurement methodology and consider ways and means of doing so as a matter of priority.

1.6 There is also no underlying picture of criminality behind the organised attacks, and therefore there can be only a piecemeal picture of overall exposure to fraud in the tax credits system. This risks producing a misleading picture for HMRC’s Executive Committee (Excom) and for Government of the true extent of losses to fraud, and may lead to an inaccurate and unrealistic prioritisation of the problem and the resources required to combat it.

1.7 HMRC now needs to implement a proper anti fraud strategy, supported by a robust and transparent performance management regime if they are to effectively tackle crime within Tax Credits. They should also provide transparent publicity and feedback to the public relating to both the scale of the problem and its achievements in tackling it.

1.8 This report recognises that there are a number of examples of good practice operationally, in relation to intelligence-sharing, new initiatives and ways of working. However, it is clear that the Benefits and Credits Directorate (BC) – and the Organised Attacks Group (OAG) in particular – is not sufficiently ‘wired in’ either to the existing HMRC intelligence capability or to the wider intelligence law enforcement community.

1.9 Relationships with stakeholders tend to be disorganised and accidental and need to become better driven and better focused, with a clearer idea about who BC can or should engage with, for what purpose and with what outcome in mind. In the meantime some key stakeholders are being under utilised, leading to missed operational intelligence opportunities.

1.10 The wealth of data available to BC needs to be worked and used more effectively to identify and counter tax credit fraud. There is little strategic or tactical use of intelligence, which is instead mainly being used operationally to effect disruption and intervention. Intelligence should be being used to identify how fraudsters are defeating the system, and effective tactical solutions developed to meet the threat.

1.11 The Organised Attacks Group in particular is being overwhelmed with incoming intelligence with no opportunity to develop a more ‘front foot’, proactive approach to develop profiles, make strategic or tactical interventions, and learn from previous cases. In both singleton and organised frauds the myriad tactics, initiatives and projects lack overall governance and co-ordination.

1.12 There is also no clear single point of accountability or tactical oversight of all fraud and intelligence activity, and no visible ‘champion’. Proper organisation and clear lines of accountability are vital if BC is to make the best possible use of all intelligence, information and stakeholders available to it. The currently disparate range of initiatives, relationships and intelligence flows require better overall governance and would benefit from being harnessed and directed in a more focused and coordinated manner. We have suggested a possible framework for HMRC to consider in helping them achieve this.

1.13 Organisational learning in respect of criminal attacks is poor and there is a clear need for a strategy to ensure that processes are evaluated, intelligence is made available to those who need it, cases are de-briefed, and any lessons learned are stripped out and recycled back into the front end of the business. Where staff identify their own effective solutions to combat fraud there needs to be a mechanism to ensure these can be rolled out across the business for the benefit of others. In respect of training, there is an over-reliance upon the accrued expertise of experienced staff with no apparent means of transferring learning to support business continuity.

1.14 For the future, a key consideration for BC (and OAG in particular) is whether to retain and develop their ‘in-house’ intelligence capability, as ‘core business’ or limit their future involvement in favour of a greater reliance upon more established law enforcement/intelligence-led business partners such as HMRC’s Risk and Intelligence Service (RIS).

1.15 Given the subject matter expertise, proximity to the process and progress made so far, it is our conclusion that BC should retain its developing internal intelligence function, but that this should be supported by RIS expertise and an improved governance structure. This report and the recommendations made are intended to assist HMRC (and BC in particular) in positioning themselves for the future to ensure that they make best use of all available information and intelligence in their fight against criminal attacks upon the tax credit system.

2: Background

2.1 The White Paper "Universal Credit: welfare that works", published on 11 November 2010, sets out the Coalition Government's plans to introduce legislation to reform the welfare system by creating a new Universal Credit (UC), to be introduced from 2013 onwards.

2.2 This is underpinned by the Government's longer term strategy paper *'Tackling Fraud and Error in the benefit and tax credit systems' –October 2010* which puts forward a number of measures to ensure that HMRC and DWP work together to prevent, detect, correct, punish and deter benefit fraud. Proposals include an integrated risk and intelligence function (which is already being progressed via joint initiatives, (see Chapter 4: Good Practice) and a single fraud investigation service by 2015.

2.3 **Child Tax Credit (CTC)** can be claimed, irrespective of personal circumstances, whether a person is in or out of work, by anybody who has a responsibility for a child. It is means tested and paid in addition to any other benefits a family may receive.

2.4 **Working Tax Credit (WTC)** can be claimed by people who work but have a low income, and can be paid with most other benefits. To claim, individuals have to fulfil certain age and working hour's criteria.

2.5 CTC and WTC were introduced in April 2003 to replace Working Families' Tax Credit, Disabled Person's Tax Credit and Children's Tax Credit. The new regime was introduced quickly, and as a result HMRC struggled to cope with the sheer complexity and scope of tax credit awards as well as the political imperative to maintain a basic level of customer service and, in the majority of cases, prioritise payments above preventing error and fraud.

2.6 The rush to implement the new system left it vulnerable to fraud and organised criminal attack. Between 2003 and 2007 incremental attempts were made to address a developing legacy of error and fraud in the system. By the end of 2007 HMRC was confident that it had begun to control the situation.

2.7 In 2009 the new Error and Fraud Strategy was launched. This new strategy represented a marked shift in policy, from a post-payment checks regime to a more prevention-focused 'Check First, Then Pay' approach, whilst balancing HMRC's commitment to improving customer satisfaction.

2.8 In 2007/08 the already established Random Enquiry Programme was renamed the Error and Fraud Analytical Programme (EFAP) to better reflect its purpose as an indicator of the scale of error and fraud within the tax credit system and as a tool to measure achievement against HMRC's key strategic objective to reduce error and fraud from a central estimate of 8.55% (of final award by value) in 2007/08 to 5% by March 2011.

2.9 The Strategy also looked to address the organised and criminal attacks on the tax credit system, much of which (e.g. identity fraud) is not included within the Error and Fraud estimates. HMRC accept that there are currently no robust estimates for the level of organised tax credit fraud.

3: Strategic overview

3.1 During the inspection some have argued that both practically and in terms of outcomes there is no need to differentiate between fraud and yield, because ultimately they both equate to the same thing: limiting exchequer losses. However, it is HMIC's view that, without robust pursuit of wrongdoing there is simply no deterrent for repeat or 'would be' offenders. The may lead to the credibility of and confidence in the system being compromised which can be further exacerbated by a lack of robust action against fraudulent attacks. A transparent and meaningful sanctions regime (see Chapter 11: Sanctions), is also vital to the health and credibility of the system.

3.2 Therefore it is very important that HMRC has a standalone, clearly stated and clearly understood strategy to deal with fraud in its own right, not just as a by-product of delivering yield. The fraud element of the 'error and fraud' programme and organised fraud would benefit from a much closer relationship, if not alignment, under a single Head of Fraud and Intelligence, supported by discrete commands to address Prevention, Analysis and Intervention capabilities (see also Chapter 8:'Operational').

3.3 As well as very low levels of civil penalties (see Chapter 11: Sanctions), HMIC considers that there have been too few criminal prosecutions brought against organised fraudsters. There are a number of reasons why this has not been happening but the net result is that HMRC appears to be pursuing a policy to disrupt rather than prosecute. This is leading to a lack of clarity of purpose 'on the ground' about where the priority lies. There is also widespread confusion and inconsistency about what actually constitutes a fraud.

3.4 There is a strongly held view in the wider HMRC law enforcement community that 'fraud is fraud' and should always be treated as such, irrespective of any competing priority to identify yield. These views should not necessarily drive business decisions but, nevertheless, it is interesting that HMRC's own analysts are clear that serious non-compliance in tax credits should be determined as a fraudulent attack on the system, as the claimant is deliberately attempting to claim monies they are not entitled to.

3.5 In summary, whilst there is an Error and Fraud Strategy it really only relates to singleton fraud cases that may or may not come to light from the application of the EFAP process (see Chapter 6: EFAP). EFAP exists as a fraud *measure* but was never designed to *combat* fraud in itself. The organised fraud strategy remains embryonic and, as such, is limited in its effectiveness. As such it is open to scrutiny and criticism as long as the true extent of organised fraud remains unknown. Either way, there is currently no holistic fraud strategy for tax credits and no single point of accountability for fraud and intelligence within BC.

3.6 In the meantime, Excom may not be sufficiently sighted on the true extent of fraud losses in the tax credit system. As a result, there is a risk that organised tax credit fraud in particular may sit artificially low in HMRC's National Risk Overview (an evidence-based analytical ranking of the key compliance risks faced by HMRC) as the underlying picture of criminality and associated losses prevented continues to emerge.

4: Good practice

4.1 The overall new strategy to 'Check First, Then Pay' has been well communicated and very well received:

> "……*It's a challenge, but there is a lot of enthusiasm for it [the new 'check first pay later' strategy], I'd say the head is old but the heart is new."*

4.2 A number of innovative and evidently effective 'projects' have been scoped and delivered by BC in support of the new Strategy. Although the main driver appears to be yield these projects promote the necessary anti-fraud ethos and culture, and the inspection team recognised them as examples of good practice in terms of intelligence-sharing, new initiatives and ways of working. Examples witnessed included:

- The introduction of **Risk Quality Standards** in July 2010 to improve the quality of electronic suspect information packages (e-sips), to act as a guide for risk and interventions staff and to maintain standards and consistency;

- The establishment of a network of **Embedded Compliance Officers** to raise fraud awareness amongst staff and provide 'on hand' support from floor walkers;

- **Teleconferences** between officers in Contact Centres across different locations to identify and disseminate fraud trends and current issues;

- **Bar coding** of all Tax Credit application forms and general activity to tighten up and address the risks in respect of bulk allocation of application forms. (NB: see Chapter 8 'Operational' for further opportunities identified by HMIC to tighten the system)

- The development of a new front-end risk engine for new applications. The Fraud and Error Assessment System Tool programme (FEAST) effectively brings together some of HMRC's existing risk rules and combines them with Experian checks.

- Whilst FEAST is an undoubted step forward as a preventive profiling measure, as any screening tool, it only identifies claims that ‘don’t look right’ and cannot distinguish fraud from error, although its capabilities do seem to be achieving a measure of success against identity fraud. It does not operate (as yet) at Change of Circumstances (CoC) or renewals stage of the process, and should be developed to do so if it is to be become truly effective. BC should also guard against over-reliance upon FEAST: it should not be allowed to completely replace the human element of the checking process.

4.3 There is also a number of forward-looking **joint HMRC/ Department of Work and Pensions (DWP)** projects involving HMRC Criminal Investigation, BC staff and the DWP, as set out below. These projects, witnessed during the inspection, are not only practical examples of valuable joint working and intelligence-sharing but also support the direction of travel advocated in the Government’s new joint working strategy for Organised Fraud, **‘*Tackling Fraud and Error in the Benefit and Tax Credit Systems*’** (published in October 2010).

- **Joint Benefits and Credits/Criminal Investigation Singleton fraud prosecution pilot:** Started in April 2010, this pilot project aims to generate more singleton fraud prosecutions, with approximately 40 live cases on hand at the time of inspection. The pilot is managed by an experienced CI Senior Investigation Officer who provides the criminal justice oversight, with BC support staff involved in gathering evidence and preparing the cases.

- Some early cases have reached the Courts, serving as a deterrent to those minded to commit singleton fraud. It is important that arrears in serial and persistent offender cases are put before the Courts in these cases, because they are seen as a valuable indicator of offending patterns of behaviour, which helps support the prosecution and inform sentencing. It will also be important that disposals from these cases receive maximum publicity to serve as a deterrent to others.

- However, the pilot has not been without its difficulties. In particular it was evident that the team has struggled to secure a regular flow of quality cases, on occasion having to resort to ‘trawling around’ for work. This was often because compliance staff across the BC regimes either didn’t know about the pilot, or if they did know of it, weren’t clear about what it seeks to achieve or how to make a referral. Therefore, this pilot may benefit from being more widely publicised if it is to continue to succeed.

- **Joint HMRC/DWP Intelligence Team (JIT**). This joint venture had been trialled for some time before its formal launch in October 2010. Co-located in Birmingham, HMRC and DWP staff work together to develop intelligence referrals in support of DWP-led prosecutions. At present the team is designed to work on referrals only and does not have the proactive capability to generate work for itself.

- **Joint HMRC/DWP prosecution team**. This is another joint HMRC/DWP initiative which had also been trialled for nearly two years. The team is led by a seconded experienced CI officer, supported by six BC staff. They aim to directly support DWP prosecutions if a tax credit element of the fraud is also identified. This initiative is a direct response to previous judicial criticism that DWP and HMRC were failing to present both aspects of benefit fraud in a single prosecution.

4.4 It should be stressed that these initiatives and areas of good practice form only a small part of HMRC's overall response to crime in Tax Credits which is supported by resources in RIS and CI also involved in responding to Tax Credits fraud.

5: Error and Fraud Analytical Programme (EFAP)

5.1 HMRC began measuring the official level of error and fraud as part of finalised entitlement in 2003/04, via what was then called the ‘random enquiry programme’. The new ‘Check First, Then Pay’ strategy was introduced in 2009 and represented a marked shift in policy, from a post-payment checks regime to a more prevention-focused approach.

5.2 In 2007/08 the already established Random Enquiry Programme was renamed the Error and Fraud Analytical Programme (EFAP) to better reflect its purpose as an indicator of the scale of error and fraud within the tax credit system and as a tool to measure achievement against HMRC’s key strategic objective: to reduce error and fraud from a central estimate of 8.55% (of final award by value) in 2007/08 to 5% by 2011, approximately £1.4 billion a year.

EFAP: Process

5.3 The EFAP sample is a selection of 5,000 singleton finalised award cases. HMRC assesses the selection to be a ‘stratified sample’ of claims. It is not entirely random but is drawn from four award groups:

- NIL awards (effectively dormant previous claimants);
- family element on claims and what HMRC call ‘2nd taper’ cases paying less than £10/week;
- working tax credits only; and
- the balance (ie everyone else).

The sample sizes extracted from the four constituent groups vary according to risk, with the ’working tax credits’ and ‘the balance’ being the larger sampled groups.

5.4 An excel spreadsheet of the selected cases is produced by HMRC’s Knowledge Analysis and Information team (KAI), which is then sent to BC, for distribution to designated EFAP sample casework teams in a number of separate locations. After working the case, these teams categorise them according to apparent customer behaviours to make a decision about whether a selected case can be categorised as being erroneous *or* fraudulent. These results are then recorded on an EFAP stencil and returned to KAI.

5.5 The initial spreadsheet is issued from KAI in early September, and BC has until May the following year to return worked outcomes. The majority of the cases are worked intensively between October and November in the year of receipt; however not all the cases are always worked and returned. For final award year 2008/09 between 4,100 and 4,200 (out of 5,000) were returned to KAI.

5.6 KAI then analyse the sample results and make an extrapolation of the sample data to arrive at an indicative overall figure for fraud in the system.

EFAP: Conclusions

> *"….Trying to detect or identify in any way the fraud element of 'error and fraud' is a largely pointless pursuit."*

5.7 This year BC took the decision to reduce the sample further from the usual 5,000 to only 3,000 cases. This was apparently due to pressure of work and shortage of resources. Although we understand from HMRC that EFAP sample sizes are statistically valid, accepted by Parliament and reviewed annually by the National Audit Office (NAO) this means that the sample now represents only 0.05% of the 6.5 million tax credit client base. We understand from KAI, that the indicative split for the worked EFAP samples averages out at approximately 80% error and 20% fraud. Based upon a 5,000 case sample, KAI estimate the fraud element of the sample to be £450 million. With the reduction to a 3,000 sample, this extrapolated figure becomes progressively less robust.

5.8 By way of comparison, DWP operates a similar sample and mark-up exercise to arrive at their indicative error and fraud figures. However, they take a representative sample of 30,000 (nearly 1%) of cases from their 4.5 million client base. These samples are then evaluated via one-to-one interviews if there is a suspicion of fraud.

5.9 HMRC accept that their EFAP estimate of fraud losses of only £450m in 2009/10 out of a total of £27billion paid out in awards does not include the emergent organised criminal attacks losses, which they estimate to be somewhere between a further £20 and £400 million.(see Chapter 9 :Organised Criminal Attacks).

5.10 Therefore, given that EFAP is only published measure of fraud in the system, HMRC risk creating a public perception that that all ‘Error and Fraud’ is being assessed and measured. Consequently any stated progress against their key strategic objective to reduce ‘error *and fraud’* from a central estimate of 8.9% in 2008/09 (of final award by value) to 5% by 2011 could also be construed as misleading. HMRC should therefore aspire to develop a more holistic fraud measurement methodology and consider ways and means of doing so as a matter of priority.

6: The 5% target

6.1 The key strategic objective to reduce error and fraud from a central estimate of 8.9% (of final award by value) in 2008/09 to 5% by 2011 was set in 2009 with the launch of the newly revised Error and Fraud strategy which emphasised the need to 'Check First, Then Pay'.

6.2 The setting of a measurable, quantitative target was clearly sensible and well intentioned, as was the decision to set proxy yield targets to measure progress against that target 'in year'. However, for HMRC, 'yield' effectively means anything that reduces the amounts paid out incorrectly and that can be scored accordingly.

> *"…It's all about yield, yield and more yield, we don't have time for fraud."*

6.3 Whilst this may be an appropriate prioritisation and emphasis for a revenue-collecting department, the focus on yield to ensure the 5% goal is met appears to have become all-consuming, and almost something of an obsession, a view expressed many times during the inspection, by BC staff at all levels. This is not necessarily a problem in itself, but becomes so when it begins to drive behaviours that militate against the anti-fraud agenda and could also compromise the business delivery, such as:

- Failing to pursue 'prima facie' fraud cases because staff have neither the time nor encouragement to do so. There is an evident climate of reluctance on the ground to look for/refer fraud because of the need to meet yield productivity and related targets. Obstructing factors include time taken to fill out forms, lack of understanding and awareness of the Evasion Referral Team (ERT) system, and – based upon their previous attempts to make fraud referrals – no staff confidence that anything will get done, and that they will receive no feedback either way.

- Some yield and fraud 'projects' are competing against each other. An example of this is that BC compliance officers may threaten civil penalties in their correspondence with individuals, which can then tie the hands of those running the CI singleton Prosecution pilot to pursue criminal sanctions (because the threat to impose a penalty may constitute an offer to settle the case).

- Discontinuing use of the CONNECT data profiling tool because it actually generated '*too many*' potential fraud leads and a management decision was taken to work on higher priority cases as BC was falling behind in achieving the E and F targets (see Chapter 8: Operational)

- Staff conducting a reduced number of one-to–one home visits to clients (despite the fact that these were seen by many officers spoken to as a very effective tool in testing the credibility of suspected fraudulent claimants). Whilst we recognise the value and success of 'one-to many' exercises, one-to-one visits still add value as a risk-based tool and should not be dispensed with completely.

7: Tactical

7.1 As reflected in the introduction to this report, nobody could doubt the enthusiasm of the staff across BC to engage with the new strategy to ‘Check First, Then Pay. We encountered many officers who were genuinely relieved that HMRC had adopted this new approach after several years of frequently being left with no option but to pay claims that their experience told them were fraudulent, or at least suspicious.

7.2 However, in both singleton and organised frauds the myriad of tactics, initiatives and projects lack overall fraud-focused governance and co-ordination.

> *“.....I would sum up the whole thing [the fight to counter fraud in the tax credit system] as being ‘enthusiasm without process.”*

There is also no clear governance or tactical oversight leading to:

- An absence of de briefing/lessons learnt from previous cases or attacks on the system

- A failure to strip out accumulated intelligence to inform tactical interventions.

- The Organised Attacks Group being overwhelmed with incoming intelligence, with no opportunity to develop a more ‘front foot’ proactive approach to developing profiles, making strategic or tactical interventions, and learning from previous cases.

- Intelligence only being used operationally to effect disruption and intervention. Simply ‘cutting off the heads’ of individual claims does nothing to root out organised fraud and those behind it. Intelligence should be used to identify how fraudsters are defeating the system, so that tactical solutions can be developed accordingly

- Yield rather than intelligence-driven tactics (such as leverage exercises), which by their nature encourage ‘light touch’ interventions with a pure yield focus. These run the risk of engaging only the compliant majority with no time available to pursue ‘non responders’, more likely to represent the fraud risk.

8. Operational

Operational: Overview

8.1 There is an overall lack of co-ordination of all fraud-related activity, and a general sense of being overwhelmed by the level of incoming intelligence. Despite the introduction of embedded compliance officers, there is also no visible intelligence or fraud champion, a point borne out by the overwhelming majority of case workers spoken to who had no idea who, if anybody, was the business lead or 'champion' for intelligence and fraud.

> "…..*We don't have a designated intelligence lead; we just try to cover all the intelligence bases between us."*

8.2 BC also lacks the specialist knowledge and experience to ensure that it engages with the right people in the right way to make the best of what is available to them, both within HMRC and in the wider law enforcement community.

8.3 This is symptomatic of an overall lack of structure and governance of fraud and intelligence across the business. The proposed new governance structure put forward in this report (see Chapter 8: Operational) seeks to help address these organisational shortcomings.

Operational: Fraud awareness

8.4 It follows that if caseworkers are to engage with and confront 'fraud', they must have a reasonable understanding of what it is.

8.5 Whilst the legal definition of fraud as defined by the Fraud Act 2006 Section 2 is clear (i.e. where *a person makes any representation as to fact or law, express or implied which they know to be untrue or misleading*), there is widespread confusion and inconsistency across BC about what constitutes a fraud and how to deal with it (see also Appendix C: Fraud and Corruption Definitions).

> *"…There are innumerable numbers of singleton fraud in the system being renewed every year. If it looks like fraud and smells like fraud, then it's probably fraud!"*

8.6 Even senior officials charged with the responsibility to lead and deliver the 'Error and Fraud Strategy' were unclear about the legal definition of fraud, and were therefore unable to say whether BC's own range of definitions and applications in this area reflect the law. EFAP caseworkers spoken to (who are expected to make judgements about whether a referred case appears to be error or fraud) considered identification and demonstration of fraud to be outside of their ability. This is perhaps not surprising given that they receive no training in fraud or in the use of intelligence and information to inform decisions.

8.7 However, this response is in part understandable given that even if caseworkers had both a clear definition to work to and adequate training, (see Chapter 14: Training), they are not routinely provided with available intelligence to help inform their suspicions. Inflated childcare costs or false income data were examples given by staff interviewed that would be considered to be 'serious error' or 'serious non compliance' (SNC), not fraud.

8.8 Internal guidance ('HMRC Child and Working Tax Credits Error and Fraud statistics 2010 Annexe A') states that '*to be classified as fraud a caseworker needs to have found evidence that the claimant deliberately set out to misrepresent their circumstances to get money to which they are not entitled'*. This puts a significant burden upon caseworkers who are already under time constraints; it also sets the bar so high as to deter them from making a referral and significantly lessens the likelihood of caseworkers taking the time to identify suspicious cases in the first instance.

8.9 Without a basic awareness of the required ingredients for an offence of fraud, HMRC operational staff cannot be confident that any referrals they make are robust enough to support securing penalties or convictions in any tribunal or criminal court. At the very least, they should be trained and encouraged to identify and report suspicious activity or patterns of behaviour.

8.10 We therefore recommend that a fraud awareness 'golden thread' be established and embedded throughout BC. This should embrace generic fraud awareness sessions, clearly and regularly communicated trend alerts and updates, and the inclusion of fraud-related objectives in performance and development agreements (PDEs].

Recommendation 1: HMIC recommends that BC establish a fraud golden thread. This should include generic fraud awareness sessions and clearly and regularly communicated trend alerts and updates. Fraud-related objectives should also be included in performance agreements (PDEs).

Operational: Processes

8.11 We identified that the following operational processes and intelligence tools are not being fully exploited to counter the fraud risk. To note: these processes are listed alphabetically for ease of reference and assume no priority.

8.12 **Application forms [Supply and Control]:** HMRC has already worked hard and with some success to tighten the application form process (see Chapter 4: Good Practice). However, having walked through the system, including visits to contractors, distributors and HMRC, we identified the potential to tighten the tracking and tallying of application forms further by scanning the bar code on each claim form before it is sent out.

Recommendation 2: HMIC recommends that BC scans the bar code on each unique claim form (TC 600) prior to despatch so that it can be tracked and tallied upon receipt.

8.13 **Call Monitoring Analysis (CMA):** CMA is a call monitoring system that retains live voice recordings and logs call numbers from claimants. We witnessed an example case whereby a member of staff in an embedded compliance team had proactively (and successively) interrogated the system

8.14 The initial suspicion was raised by frontline staff at Netherton who had recognised suspect claims. These details were then worked up into a spreadsheet and referred on to an analyst in the Organised Attacks Group.

8.15 This was an excellent practical example of a member of staff using their initiative and the available intelligence to identify a possible organised attack on the system. However, this was only possible because the individual knew of the system, and what it could do, from a previous job. This is indicative of the fact that there is no co-ordination and communication across BC to ensure that all intelligence tools and techniques are being considered and deployed.

Recommendation 3: HMIC recommends that BC raise awareness of the Call Monitoring Analysis (CMA) system and promote and expand its use as an intelligence tool.

8.16 **Complaints:** Complaints can be a valuable source of information and intelligence – but do not appear to be recognised or treated as such. The following are examples of potential opportunities lost:

- Repeat 'successful' fraudsters, calling to complain that an award has been stopped, which in itself can be a valuable performance indicator in assessing the success (or otherwise) of anti-fraud measures and exercises.

- Identifying complaints as an intelligence source for fraudulent claims and challenging accordingly may also serve to deter vexatious and repeat fraudsters if they know that to complain may focus attention upon their current and previous claims.

8.17 At present, some complaints teams are hampered in validating any suspicions because they do not have direct access to the National Tax Credits Database (NTC). We therefore recommend that all complaints teams are given some direct access to NTC data so that they have the opportunity to validate and build their own concerns and therefore provide better quality, better informed referrals to compliance colleagues. Finally, feedback should be given to complaints teams when they make a referral.

Recommendation 4: HMIC recommends that all complaints teams should be given direct access to NTC so that they can make quality, well better informed referrals to compliance colleagues. Feedback should be given to those who have made a referral.

8.18 **CONNECT – ICE/ACE:** HMRC already has a sophisticated data profiling, mining and matching capability at its disposal in the form of the CONNECT system.

8.19 CONNECT (which has been signed off by Excom as the strategic risk solution of choice for HMRC) brings together 28 existing HMRC and external databases which can build a series of visual networks, joining people, places, identity numbers and documents. This visual representation is known as ICE (Integrated Compliance Environment) and can focus on individual cases and related intelligence. CONNECT is also supported by ACE (Analytical Compliance Environment), a bulk data profiling tool, capable of giving a more generic 'read across' and allowing for the identification of claimant profiles and patterns.

8.20 HMRC has set up five processing centres to interact with and support CONNECT, with the aim of delivering enhanced 'upstream risking', with KAI analysts embedded in each centre. These profiling centres have been built to support specific HMRC regimes such as VAT, Corporation Tax and Hidden Economy. HMIC acknowledge that BC has its own TC profiling *capability*, but there is no bespoke 'profiling centre' for tax credit work. This is primarily because the NTC sits alone (ie outside of other HMRC databases) and was not included in the original 'build', and is therefore not currently included as a data source within CONNECT.

8.21 The option exists to 'hotlist' datasets into CONNECT from the NTC (see below). However, bringing the entire NTC database within the CONNECT network, with the resultant case building and data profiling capabilities, could bring significant benefits for BC. We understand that this integration is technically entirely possible, and would cost HMRC in the region of £750k to effect the necessary system changes. Given that CONNECT has delivered £900m of additional revenue for HMRC since it was first trialled in 2007/08 (for an initial investment of £45m), a further investment of £750k to integrate NTC would appear to be money well spent for HMRC, and would provide a significant addition to their intelligence capability in identifying fraud in the TC system.

Recommendation 5: HMIC recommends that HMRC considers investment to incorporate NTC data within the scope/capability of CONNECT (ICE and ACE). In the meantime HMRC should explore the feasibility and benefits of developing a TC-specific CONNECT profiling centre.

8.22 **CONNECT – Hotlisting: '**Hotlisting' is the process of temporarily lifting a specific data set (ie from NTC) into CONNECT for profiling or analysis. The imported data subset can be up to 500,000 records (or 1 GB of data).

8.23 In 2009 BC undertook such an exercise when 80,000 records were 'hotlisted' in to CONNECT using the ICE facility. The results of this exercise, made available in autumn 2009, delivered 1,500 suspect cases, of which only 346 were taken up by BC. Of these, 344 cases were settled, but a decision was taken by BC that the average yield was too low to justify continuing with the remainder of the cases.

8.24 Despite the availability of this resource and its evident effectiveness as a profiling tool, correspondence from autumn 2009 reveals that managers who commissioned the work were concerned that the exercise had actually produced *too many* fraud leads to work and that this and any future exercise would therefore adversely effect productivity. The position was taken that, after one trial and on balance with other initiatives, the process was 'unproven'.

8.25 We understand that at the time of this exercise only the ICE (which allows individual case building) tool was available to staff. Since then, the ACE (generic bulk data matching and profiling) has also become available. We consider that both ACE and ICE (as part of CONNECT) represent invaluable tools for BC as it tries to move onto the front foot in terms of proactive profiling of potential fraudsters and suspicious patterns of activity (see below). In the meantime, we recommend that BC make more regular use of the 'hotlisting' facility within CONNECT for intelligence profiling and analysis purposes.

Recommendation 6: HMIC recommends that BC makes more regular use of the 'hotlisting' facility within CONNECT for intelligence profiling and analysis purposes.

8.26 **CONNECT – Licences:** We understand that BC currently has only 36 ICE licences allocated to it, out of an overall HMRC allocation of 3,000. This seems very low given the emergent tax credit fraud threat and the potential benefit ICE could bring to tackling it. However, BC remains in the process of a 'stocktake' to ensure that, in more general terms, the right licences are allocated to the right people. It will be particularly important that BC ensure their 36 ICE licences are deployed to maximum effect.

8.27 BC currently does not have any ACE licences. HMRC has 100 licences, of which 99 are currently allocated. We understand that the one remaining licence could be made available to BC, subject to the necessary business case being made.

8.28 On the face of it, one licence may seem woefully inadequate; however, one person with one ACE licence can produce significant analytical output. A recent example provided to us by HMRC showed that two people generated 70,000 suspect case referrals in a period of six months using ACE. This is made possible because ACE facilitates access to the so-called 'sandpit' (a 3% data sample of the entire UK data cell) which can then be developed to run live on a 100% sample of the UK data cell. With the attendant training overheads, each ACE license costs in the region of £70,000 per annum.

8.29 The relatively low allocation of ICE licences to BC – and the complete lack of ACE licences – is a concern. This may attributable in part to the governing HMRC body that controls the allocation of such licences, the Bulk Data Governance Group. This Group generally 'makes the call' as to where such IT tools are deployed but, as we understand it, they do not currently have tax credit fraud on their prioritisation schedule.

8.30 We therefore recommend that the number of CONNECT (ICE and ACE) licences allocated to BC is reviewed and that BC makes a business case for at least one ACE licence.

Recommendation 7: HMIC recommends that the HMRC allocation of CONNECT (ICE and ACE) licences to BC be reviewed and that BC make a business case for at least one ACE licence.

8.31 **Document verification:** A robust and effective document verification process is a vital part of any strategy to counter fraud that is predicated upon an individual's ability to prove their identity. Detective controls must be a match for the sophistication of fraudsters.

8.32 The document verification process operated by HMRC is a valuable facility for BC; and we were surprised to learn that BC (and the OAG in particular) was not a more regular client of the National Document Verification Unit (NDVT). This is particularly unexpected given that a considerable amount of what BC OAG deal in will inevitably involve identity – and therefore document – fraud.

8.33 Operationally, we learned of one example whereby a local 'document champion' had built their own light box on their desk from a cardboard box, having bought a UV pen from the local pound shop. It is important that the evident enthusiasm and commitment of the staff to engage in the fight against fraud is met with the appropriate investment from HMRC.

8.34 We understand that the 2009/10 investment to cascade train a further 30 BC staff to Tier 1 and others to Tier 2 achieved £9m in savings. It is not unreasonable to assume that further savings would be possible with the right investment. This not only plays to the anti-fraud agenda but also contributes to removing error and fraud from the tax credits system.

8.35 We recommend that BC use the services of the NDVT whenever they have irreconcilable suspicions about the bona fides of key documents that have been presented to support suspected fraudulent claims, BC should also conduct a cost benefit analysis of further investment in training staff in the document verification process at Tiers 1 and 2.

Recommendation 8: HMIC recommends that BC use the services of the NDVT whenever they have inconcilable suspicions about the bona fides of key documents that have been presented to support suspected fraudulent claims. BC should also conduct a cost benefit analysis of further investment in training staff in the document verification process at Tiers 1 and 2.

8.36 **HUMINT:** HUMINT awareness has been greatly enhanced across BC, but there is still a good deal of ignorance about what it looks like, and what to do with it. A particular example of concern was brought to the attention of BC senior management by HMIC during the process of the inspection. This involved a substantial amount of unsifted material (approx 30,000 pieces) which had come to light as a result of an earlier awareness visit (or visits) from the National Humint Centre team (NHC).

8.37 By the time of inspection, all potential HUMINT material identified as a result of the NHC visit had been brought together in a single place. However, we were concerned that although the backlog was being processed and the stockpile reduced, there was no apparent process to risk assess what was ‘on hand’ and prioritise accordingly.

8.38 Aside from the general risk of unactioned and unassessed material, failure to at least examine and risk assess each piece of material in the backlog may compromise HMRC’s ability to give the necessary disclosure assurances for prosecutions. This could specifically undermine the CI/BC singleton prosecutions pilot (which is bringing its first cases before the Courts), as well as any other larger scale CI or joint DWP tax credit prosecutions.

8.39 BC senior managers reacted swiftly to address the matter once it had been brought to their attention. However, we remain concerned about the situation, and recommend that an urgent review and risk assessment be conducted of all backlogged and unactioned HUMINT material. This should include an impact assessment against the singleton fraud prosecution pilot cases and any other larger scale CI lead or joint DWP tax credit prosecution cases.

Recommendation 9: HMIC recommends that an urgent review and risk assessment be conducted of all backlogged and unactioned HUMINT material. This should include an impact assessment against the singleton fraud prosecution pilot cases and any other larger scale CI lead or joint DWP tax credit prosecution cases.

8.40 HUMINT material continues to arrive in BC at a rate of approximately 3,000 pieces per month. BC needs to recognise that this is now an ongoing reality and an integral part of their business for the future, and ‘gear up’ accordingly. This should include a more permanent and integrated solution for identification and management of all HUMINT material.

8.41 **Licences (IT):** Poor allocation or lack of IT licences was a recurrent issue for staff. It is vital that the right people have the right IT, so that access to invaluable intelligence sources (such as ADD and ICE) is made best use of. Even basic internet access can be invaluable to compliance officers when verifying a range of tax credit claims.

8.42 BC recognises the importance of having the right licences allocated to the right people. Indeed, BC Senior Managers commissioned a ‘stocktake’ of all existing licenses across the business, which asked managers to identify their own business priorities, so that if necessary licenses could be recalled and reallocated to those with the highest business need.

8.43 We understand that the quality and completeness of responses was poor, and that consequently the value of this extremely useful exercise was undermined. A further exercise is now being run to show which Personal Identification Numbers (PIDs) have access to which system (X500 list) and this list has gone to managers, who are responsible for re prioritising their needs.

8.44 The poor response rate to this exercise has made it impossible to complete; and this continues to fuel staff perception that the issue is not being gripped. More importantly, there can be no assurance that the right intelligence tools are in the right hands. We therefore recommend that this exercise be satisfactorily completed as a matter of priority.

Recommendation 10: HMIC recommends that the BC IT licences stocktake be satisfactorily completed as a matter of priority.

Operational: Structure

8.45 Governance is the way in which an organisation (or function within it) is controlled, and should define ownership, roles and responsibilities, decision-making procedures, and how relevant objectives are set and progress against them measured.

8.46 The recent change of management structure to keep organised fraud in a management silo apart from 'Error and Fraud' makes little sense on the face of it. In reality the current Grade 6 'Error and Fraud' strategy position appears to have little to do with fraud and even less to do with intelligence.

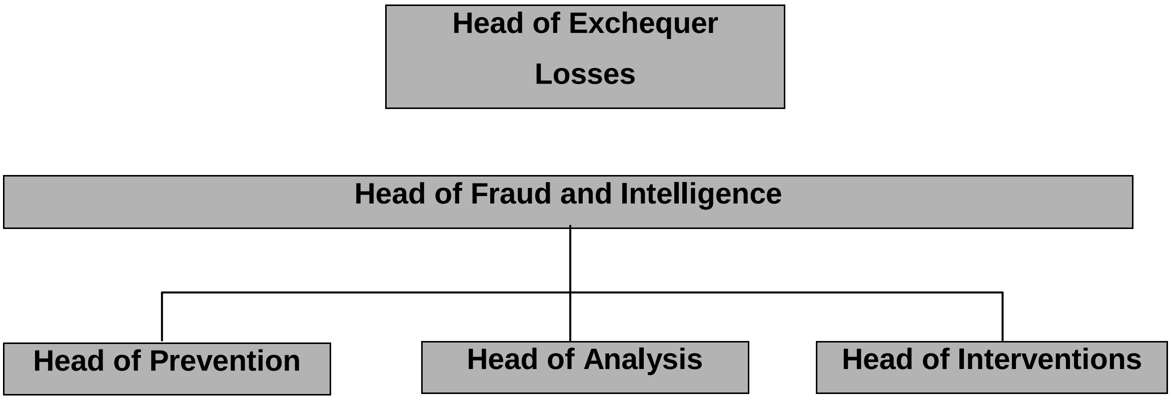
8.47 In order to combat fraud in the tax credit system, BC need to keep pace with the developing sophistication and level of the threat. Proper organisation and clear lines of accountability are vital, as is ensuring that it make best possible use of all intelligence, information and stakeholders. The currently disparate range of initiatives, relationships and intelligence flows would benefit from being harnessed and directed in a more focused manner.

8.48 To deliver this focus we have put forward for consideration a new organisational governance model, with a single point of accountability for all fraud and intelligence issues across the BC business portfolio (including all data and stakeholder management).

8.49 The fraud element of the 'error and fraud' programme and organised fraud would benefit from a much closer relationship, if not alignment, under a single Head of Fraud and Intelligence, supported by discrete commands to address Prevention, Analysis and Intervention capabilities (see also Chapter 8:'Operational'). Any person appointed to this position should be an experienced specialist in their field.

Recommendation 11: HMIC recommends that BC consider a new organisational governance model to coordinate all aspects of fraud and intelligence activity. The appointment of a single Head of Fraud and Intelligence should be considered, supported by discrete functional commands to address Prevention, Analysis and Intervention capabilities.

8.50 The following chart sets out a new organisational governance model for consideration, with clearly delineated roles and potential responsibilities which are outlined below and on the next page.



Roles and responsibilities

Head of Prevention:

- Internal fraud and corruption SRA
- Debriefing
- Organisational learning
- Systems
- Guidance and training
- MOUs/SLAs etc
- Feedback to staff on fraud referrals

Head of Analysis:

- Proactive profiling/data mining
- CONNECT/ACE/ICE profiling tools and techniques
- Patterns/trend analysis
- KAI/RIS liaison
- OF analysis/assessment
- TPI lead
- HUMINT
- Review of outstanding intelligence assessments

Head of Interventions:

- Case specific investigations
- Liaison with CI
- Prosecutions (CPS/DWP)
- Civil/criminal interventions
- Penalties
- Feedback to staff on fraud referrals

8.51 Adopting this kind of governance model would:

- Harness, direct and reward all currently disparate ‘fraud’ and intelligence activity and knowledge;
- Set direction and purpose and clearly delineate roles and responsibilities;
- Import best practice (organisational and operational);
- Enhance law enforcement and fraud networking opportunities; and
- Provide independent fraud and related intelligence assurance to the Head of Exchequer Losses

9: Organised criminal attacks

HMRC position

9.1 The intelligence capability and understanding of organised criminal attacks on HMRC's systems is more developed and mature in RIS than in BC, which is a relatively new player.

9.2 HMRC's *Fiscal Fraud Delivery Plan* (FFDP) sets out very clear priorities for criminal attacks, as follows:

- To identify, target, disrupt and dismantle those behind the criminal attacks through effective profiling, sharing of intelligence and joint working, and by tackling criminal finances;
- To increase understanding of the behaviours and modus operandi of organised criminals;
- To design fraud out of HMRC systems;
- To robustly police entry to HMRC systems;
- To secure HMRC systems from, and to tackle, the internet threat; and
- To make best use of appropriate powers, both civil and criminal

BC position

9.3 An Identify Fraud team has been in existence in BC from as early as 2005 when identify fraud first rose to prominence. In 2009 a fraud pilot was established to address a particular threat, and ran for 4/5 months with the full support of BC Senior Managers; and in April 2010 the 'Organised Attacks *Group*' (OAG) was formed in recognition of the increasing threat of organised criminal attacks upon the TC system.

9.4 The OAG comprises 207 people, out of the 5,774 in BC as a whole: this represents a direct investment of 3.5% of BC total resource in organised criminal attacks upon the tax credit system. Whilst it could be argued that this small percentage reflects the embryonic state of the organised fraud function, it could also be viewed as a significant under-investment. This investment ratio should be regularly reviewed by BC Senior Managers to ensure that it is commensurate with the developing risk.

9.5 The BC *Organised Attacks Strategy* (delivered in May 2010) sets out their assessment of the challenge and puts forward a number of commitments, which largely mirror the FFDP priorities (outlined in 9.2 above). Furthermore, a paper commissioned by the Head of Exchequer Losses in October 2010 (*Organised Fraud in Benefits and Credits*) 'self-assesses' both the threat and the measures required to counter it, and makes 26 internal recommendations. These range from the need for more robust suspension and termination powers, to the requirement for clearer communication channels with law enforcement agencies outside HMRC.

9.6 The organised attacks/fraud group seems focused primarily on 'interventions', which appear to be selected and delivered on a fairly ad hoc basis from rapidly rising levels of single strand intelligence. BC OAG acknowledges being completely overwhelmed with work and incoming intelligence, and accept that there is no forward-looking strategy to manage and direct activity:

> *'….It's like we've tapped a well since we started this [organised fraud intelligence work]…it just keeps on coming and coming, we're pinned to the wall really and it's just piling up!'*

9.7 It is also clear that, contrary to the FFDP priority to develop '*an increased understanding of the behaviours and modus operandi of organised criminals',* there is currently no discernible picture of criminality, although we were told that BC have commissioned RIS to produce a more up-to-date organised attacks 'situation report'. There is also no robust assessment of the true loss to organised criminal attacks, which, as previously stated, HMRC estimates to be between £20 and £400 million.

9.8 We were also concerned that even within the OAG there was a prevailing view that their main objective is to 'stop the money', and that finding out who is behind the organised attacks was less of a priority.

9.9 Overall, this presents a picture of random interventions that are intelligence led but yield based. A developed understanding of the picture of the organised criminality behind the attacks on the system is fundamental to any current or future strategy if BC is to play its part in aligning with the FFDP commitment to '*Identify, target, disrupt and dismantle those behind the criminal attacks'.*

9.10 In conclusion it is evident that there is no organised fraud strategy in place, no clear objectives and milestones, and still no accurate baseline of the true extent of organised fraud. Without these, there can be no proper assessment of the intelligence requirements to combat organised fraud.

Recommendation 12: HMIC recommends that BC produces a clear, coherent and credible organised fraud delivery plan, based upon a robust assessment of the loss to organised criminal attacks with key performance indicators and agreed milestones.

9.11 There is also no published organised fraud **policy** in which to anchor any strategy. We learned that policy in organised fraud is '*being made up as we go along'* and is effectively no more than a collection of evolved practices and bespoke pieces of advice. Whilst it is appreciated that operational policy is by its nature an evolving product, there needs to be a clearly stated and published organised fraud policy statement, informed by operational policy drawn from the various ad hoc advices and identified best practice to date.

Recommendation 13: HMIC recommends that a clearly stated Organised Fraud policy statement be established and published. This should be informed by operational policy drawn from the various ad hoc advises and identified best practice to date.

Organised fraud: Intelligence assessments

9.12 A number of internal HMRC risk assessments in respect of organised tax credit fraud have been commissioned and delivered, with recommendations made. However, we were unable to identify clear audit trails to establish that these assessments had been considered and acted upon. In particular there was no clear evidence of ownership, of co-ordination of any response or of action plans put in place.

9.13 In addition to reports carried out by HMRC Risk and Intelligence Service (RIS) in October 2010, senior managers in BC commissioned their own assessment of the tax credits situation. The subsequent report (*Organised Fraud in Benefits and Credits*) stated that the figures available at the time of writing '*fail[ed] to show the serious nature of the organised criminal attack threat to Tax Credits and is therefore at odds with the views and experiences of all those involved in organised fraud work*'. It went on to conclude that BC was still unable to say how much is actually lost to organised crime – even in the face of increasing demands to know this.

9.14 As previously mentioned, this recent internal report makes a total of 26 recommendations; but again we were unable to identify what became of these recommendations, who took ownership of them, which were adopted, whether any were dismissed and, if so, why. Coupled with the RIS assessments highlighted in the table above, we were unable to gain assurance that all intelligence reports were being properly considered and acted upon. We therefore recommend that a review be conducted of all outstanding analyses of organised fraud (intelligence reports/threat assessments etc), with any recommendations evaluated and assessed.

Recommendation 14: HMIC recommends that BC conducts as a priority a review of all outstanding HMRC analyses on organised fraud (intelligence reports/threat assessments etc). All recommendations should be evaluated and addressed.

9.15 It is also clear that organised attacks on the tax credits system are often connected with attacks upon other HMRC systems. Therefore a tax credit award can act a 'gateway' to further organised fraud. We therefore believe there would be value in HMRC commissioning some analysis of the role tax credits frauds may play in establishing gateway attacks on other HMRC regimes.

Recommendation 15: HMIC recommends that HMRC commissions some analysis of the role tax credits frauds may play in establishing gateway attacks on other HMRC regimes (such as ITSA, SSP/SMP/HiPG).

10: Stakeholders

Overview

10.1 Effective and consistent engagement with key stakeholders – both within HMRC and in the wider law enforcement and intelligence community – is vital if BC is to make best use of all available information and intelligence in order to counter tax credit fraud.

> *'….Sometimes we just feel organisationally isolated from the rest of HMRC law enforcement community, it's like working in a vacuum'*

10.2 At this stage relationships may still be embryonic (to reflect the new status of the strategy). However, they need to become driven and better focused, and BC must have a clearer idea about who it can or should engage with, for what purpose and with what outcome in mind.

10.3 The challenge of managing and coordinating stakeholder engagement on the scale faced by BC should not be under-estimated. The table below is not intended to be an exhaustive list of all stakeholders whom BC is (or should be) engaging with, but is indicative of the range and number of potential sources of intelligence. For indicative purposes we have split these into categories or 'streams':

Stream 1 Internal HMRC	Stream 2 External: Law Enforcement	Stream 3 External: General	Stream 4 Other Third Party Information
NCU NHC RIS IG CI	SOCA Police Europol RIUs	Banks Utilities Other Government Departments	Local authorities Child minders Schools Valuation office Ofsted

10.4 The suggested new governance structure (see above) advocates that a new Head of Fraud and Intelligence should act as ringmaster for all stakeholder engagement. BC should consider bracing this arrangement further by allocating nominated stream leads.

This would:

- manage the current tendency toward disorganised, random and accidental engagement with other law enforcement and intelligence stakeholders;
- nurture and develop mature relationships;
- manage the risks of duplication and of failure to break out available intelligence and lessons learned to the wider BC group;
- provide BC with the required helicopter view of what's available to it; and
- ensure that BC is properly 'on the radar' of all key intelligence providers.

10.5 However, there is clear and encouraging evidence that key stakeholders are increasingly engaging with BC – although this may be more as a consequence of establishing the OAG rather than any explicit and deliberate engagement strategy. The data in the table below shows the number of Intelligence Logs received by BC from its key stakeholders in 2010/11, compared to those received before the creation of the OAG in June 2010:

Source	2009/10	2010/11	Totals
HMRC CI	5	156	161
RIS CIG	25	185	210
DWP	9	21	30
FCLO	2	11	13
NCU	0	7	7
Police	6	19	25
SOCA	1	19	20
UKBA	1	4	5
BC (Internal)	1	51	52
Europol	0	9	9
Home Office	0	2	2
Other	3	13	16
TOTALS	53	497	550

10.6 It is noticeable that the greatest increase in intelligence has been from internal sources. HMRC should task stream leads with prioritising a small number of external sources, perhaps two or three each year, for active relationship development and management to achieve a similar growth in intelligence as seen from internal sources.

Recommendation 16: HMIC recommends that BC nominates ‘stream leads’ to better facilitate the engagement with and management of stakeholders. HMRC should prioritise two or three external sources each year for active relationship development and management to achieve a similar growth in intelligence as that seen from internal sources.

Memoranda of Understanding (MOUs)

10.7 MOUs can be important in establishing and managing relationships and mutual expectations with a stakeholder. However, these and similar types of agreements (such as joint intelligence protocols and service level agreements) need to be carefully coordinated, and may already exist at a more senior/corporate level.

10.8 We witnessed many examples of BC apparently duplicating effort by attempting to build their own agreements and protocols from scratch to meet their own needs, sometimes even in parallel with others in the team. This can on occasion aggravate those with the established HMRC lead. Therefore there is a need to take a step back to assess what already exists, at what level and whether any existing arrangement would provide the umbrella MOU to meet the business or individual needs.

10.9 Therefore, we recommend that BC conducts a ‘stocktake’ of all existing MOUs, service level agreements, joint intelligence protocols and reciprocity issues between BC and law enforcement, overseas authorities and intelligence partners in general. This stocktake should take account of the existing legislation and of any arrangement already in place at a corporate/higher level between HMRC and key law enforcement stakeholders.

Recommendation 17: HMIC recommends that BC conducts a ‘stocktake’ of all its existing MOUs (and similarly intended arrangements such as joint intelligence protocols etc) with key law enforcement stakeholders to regularise current engagement and identify future needs.

10.10 We also identified some examples of BC apparently failing to reciprocate with other intelligence agencies and sources, for example with other European member state authorities who were expecting a response to intelligence they had provided (or at least confirmation of amounts claimed in the UK by their nationals) to help them better understand if the offence of parallel claiming had been committed in their country.

> *"...We don't give feedback on incoming referrals, because we don't have time, we're too busy firefighting."*

10.11 An example was also cited whereby, because of lack of response or any feedback from the Polish authorities had signed a joint intelligence protocol with the Metropolitan Police. This protocol was primarily in respect of people trafficking rather than tax fraud; but trafficking can often be the catalyst for UK benefit fraud-related intelligence, and vice versa. This stands as an example that failing to reciprocate fully with intelligence providers risks valuable intelligence being channelled between third parties, to the possible detriment of HMRC.

Missed opportunities

10.12 Clearly the BC portfolio of current and potential stakeholders is wide and varied. We identified the following stakeholders who (not necessarily through any direct fault of BC), are being under utilised, leading to missed operational intelligence opportunities. Again, these have been listed in alphabetical order for ease of reference:

10.13 **Evasion Referral Teams:** There is widespread ignorance about the ERT process which requires staff to refer suspected fraud in excess of £10k. People had either not heard of it or simply didn't understand what was required of them.

10.14 This patchy and inconsistent application of the ERT process was recognised by HMRC's own Fiscal Fraud Group which, in January 2010, assessed the position across the whole of HMRC as follows:

- *The system (of ERT referrals) is unsatisfactory given the level of criticism received across the department.*

- *The misunderstanding regarding the referral criteria and selection meant staff are not 'buying in' to the system.*

- *There is too much time taken to consider criminal action, often resulting in the referral finding its way back to the originator, meaning that opportunities for action were being lost which was driving a lack of engagement from staff to use the system.*

10.15 Despite the evident weaknesses in the system, the ERT process exists to encourage, facilitate and escalate concerns of serious fraud within HMRC. Therefore, it remains a vital conduit through which BC should be making referrals about suspected tax credit fraud. However, their ability and inclination to do so is seriously hampered by the patchy understanding and application of the process.

10.16 Therefore, we recommend that BC raise the awareness and understanding of the ERT process across the business and work to encourage, facilitate and reward ERT referrals.

Recommendation 18: HMIC recommends that BC raises the awareness and understanding of the ERT process across the business, and works to encourage, facilitate and reward those who make referrals of suspicious activity.

10.17 **EUROPOL:** Each member state has its own bureau at Europol, which has very good analytical resources underpinning it. Work is divided into analytical work files.

10.18 There continues to be a steady stream of actionable intelligence about UK benefit fraud, which needs to be stripped out carefully from the primary intelligence without compromising any investigation. Other member states are also likely to have good intelligence which may be of use to BC, often with full detail of claims made and extensive personal data. In the latter half of 2010, 18 such full intelligence logs were passed from Europol to BC OAG regarding suspected organised attacks upon the tax credit system by crime groups from Eastern Europe.

10.19 The opportunity also exists for BC to task Europol via the HMRC link officer; but we understand that this has only ever happened once. Therefore, we are drawn to the conclusion that BC could make more of this relationship, which at present appears to be mainly ‘one-way traffic’. Therefore, we recommend that BC engages with and tasks Europol more often in respect of suspected organised attacks on the tax credit system by crime groups from Eastern Europe in particular.

Recommendation 19: HMIC recommends that BC engages with and tasks Europol more often in respect of suspected organised attacks upon the tax credit system by crime groups from Eastern Europe in particular.

10.20 **Fiscal Crime Liaison Officers (FCLO):** This network exists to facilitate the flow of fiscal crime intelligence between HMRC and overseas authorities. It does this via a series of overseas placements of HMRC officers, supported in the UK by link officers who facilitate the exchange of information and intelligence in support of HMRC's fiscal priorities and risks.

10.21 Where BC and tax credit fraud sit within those FCLO priorities is a topical issue. At present we understand them to be '*well down the pecking order*', behind the more traditional HMRC priorities of tobacco, alcohol and MTIC fraud. Because of this relatively low priority, TC fraud issues tend not to feature or even register with the overseas network.

10.22 However, there is clearly some appetite for tax credit fraud work in some of the Eastern European/Balkan countries; interest is also anticipated from a newly opened office in the region. The UK FCLO network can readily absorb incoming tax credit-related intelligence but, by its own admission, it struggles to meet other member states' expectations and reciprocity requests in relation to tax credit fraud. There also appears to be no strategy to allow the network to feed back or 'break out' tax credit intelligence from the UK to other member states. An example was given whereby, in the absence of any feedback, the Polish authorities could not understand why the UK was apparently not using specific intelligence they had provided about Polish nationals exploiting the UK tax credit system.

10.23 There is evidence to suggest that attitudes amongst FCLOs are changing as HMRC realises the true worth to UK PLC of detecting and disrupting tax credit fraud and the common organised fraud denominators. However, organised tax credit fraud needs to be seen as a developing priority for FCLO and should be promoted as such in FCLO planning, resourcing and training.

Recommendation 20: HMIC recommends that BC needs to engage with the FCLO network to promote the true worth of tax credit fraud with a view to developing its relative priority in FCLO planning, resourcing and training.

10.24 **Knowledge Analysis and Information (KAI):** KAI plays a major role in supporting BC with its EFAP sampling analysis. More recently, BC OAG has begun to engage with KAI in respect of qualitative analysis around organised attacks: for instance, they have been tasked to arrive at more robust estimates of the loss to organised fraud.

10.25 HMIC recognises and supports the wider use of KAI resource, but there appears to be a lack of appreciation of just what KAI may be able to do for BC in respect of organised fraud. There are currently 20 full-time equivalent (FTE) staff years dedicated to tax credit work, with an end-to-end data processing capability which enables them to offer significant operational support to identifying intervention opportunities. We therefore recommend that BC make better and more regular use of KAI resource and capability to identify and counter organised tax credit fraud.

Recommendation 21: HMIC recommends that BC makes better and more regular use of KAI resource and capability to identify and counter organised tax credit fraud.

10.26 **Regional Intelligence Units (RIUs)**: RIUs are collaborative units involving the four main organised crime agencies (ACPO, UKBA, SOCA and HMRC). The organised crime group (OCG) mapping process is the main driver for the RIUs, and HMRC has an officer embedded in each of the 10 units (which are aligned to the 10 ACPO regions).

10.27 In theory, each unit should represent regional organised crime priorities. However, in practice the police tend to dominate the RIU agenda. Again, there is evidence that BC OAG has begun to engage with the RIU process; but the perception is that ever-changing and inconsistent HMRC priorities are dictating what HMRC decides to bring to the table on each occasion.

10.28 BC may also struggle to get organised tax credit fraud on the RIU agenda and taken seriously because most RIU representatives are drawn from the former ‘Customs’ arena of HMRC, and so instinctively have more experience, knowledge, and perhaps enthusiasm for more traditional organised financial crime activity (such as VAT and MTIC fraud).

10.29 It is highly likely that there will be links between organised tax credit frauds and more general criminal, and the potential intelligence generated could be a valuable commodity for the RIU network. Similarly, HMRC stands to learn from a more robust engagement with the RIU process. Therefore, we recommend that HMRC RIS does more to raise the profile of organised tax credit fraud across the RIU network via its RIU-embedded officers.

Recommendation 22: HMIC recommends that HMRC RIS does more to raise the profile of organised tax credit fraud across the RIU network via its RIU-embedded officers.

11: Sanctions

11.1 A penalty regime should aim to encourage voluntary compliance; but ultimately sanctions should hold an individual to account and serve to deter. This is essentially what distinguishes fraud from error and why fraud matters in its own right, not just as a potential revenue stream or contributor to delivering yield.

11.2 We found relatively few examples of individuals being fined or civil penalties being imposed, and even fewer prosecutions.

> *"…..We tend not to bother anymore (with penalties), it's too much aggravation and only really affects those who can afford to pay and bother to get back to us!"*

The table below summarises the number and value of penalties imposed for tax credit fraud, and the total number of prosecutions brought and convictions secured for the period 2007/08 to 2009/10.[1]

Year	Award (£bn)	Number of penalties imposed	Value of penalties imposed (£)	Prosecutions	Convictions (number of defendants)
07/08	21.595	1,007	746,587	112	118
08/09	25.117	401	321,609	123	114
09/10	*	348	429,631	54	65
TOTAL	**46. 712**	**1,756**	**1,497,827**	**289**	**297**

* 2009/10 total award not yet available at time of writing.

11.3 Overall the current sanctions regime appears toothless and ineffective, with operational staff citing a number of aggravating factors that block or actively deter them from pursuing penalties. These include:

- Different approaches (i.e. to threaten/impose a penalty or not) being adopted in different campaigns;

[1] In 2009/10 a total of 1221 penalties with a value of £1,787,610 were waived which, set against total accruals from 07/08 until 09/10 indicates a net 'debit' of £0.3 million.

- Staff perception that productivity targets mean they do not have time to consider the required underpinning behaviours to establish fraud (state of mind and intention etc);

- Directions to staff that confuse or deter, such as '*Compliance Note 04/10: Changes to the s.31 Penalty Model'* which states that '*the distinction between failure to take care and serious error is impossible to define consistently'*; and

- An overall view 'on the ground' that penalties are just too much aggravation, are often hamstrung by hardship considerations and are generally too complicated and time-consuming to impose.

11.4 The evident confusion, practical barriers and reluctance to pursue penalties is, to some extent, understandable. However the reality of the situation appears to contradict the following stated HMRC policy, local guidance, and legislation:

- **HMRC Policy**: **Purpose Vision and Way Statement**. *'…We are relentless in pursuing those who bend or break the rules.'*

- **BC Policy**: **Serious Non Compliance**: *'We will take the strongest possible action that the legislation allows in cases of serious negligence or serious noncompliance and we will use the full extent of our powers to correct all years of award and charge penalties without regards to means.'*

- **Legislation: Tax Credits Act 2002 s.31** *'…where a person negligently or fraudulently makes an incorrect statement or they give information they know to be false HMRC can charge a penalty of up to £3,000.'* ***s.35****: 'those found guilty of an offence of fraud face penalties of up to 6 months imprisonment on summary conviction or up to 7 years imprisonment on indictment.'*

11.5 The current weakness of the sanctions regime is recognised and acknowledged by senior mangers. They have commissioned a piece of work, sponsored by the Exchequer Losses Error and Fraud Delivery Group, to deliver a more robust penalty regime, which will be transparent to claimants, simple to understand and operate for both customers and staff, and consistent and proportionate in its application.

11.6 However, the fact remains that the sanctions regime needs to be more robust if HMRC are to deliver against their commitment to be *'relentless in pursuing those who break the rules'* and if they are to deter and prosecute fraudsters.

Recommendation 23: HMIC recommends a more robust use of sanctions (civil and criminal) and of the underpinning legislation to deter and prosecute fraudsters.

12: Internal fraud

12.1 Whilst not the intended focus of the inspection, the risk of HMRC's own staff being involved in tax credit fraud, and the intelligence required to identify and combat that threat, merits some attention.

12.2 If there is a suspicion or intelligence of internal involvement in tax credit fraud, the matter is referred to HMRC's Internal Governance function (IG) for consideration. We established that in general terms, any referrals to IG involving BC staff are of alleged dishonesty and tend to fall into two categories: inflated childcare costs and under-declared income.

12.3 Whilst there are cases involving BC staff inappropriately accessing tax records, there is no evidence in the last two years of them being involved in more serious incidents, such as facilitation either of organised criminal attacks or of deliberate infiltration.

12.4 Between 2002 and mid-2010 there were 31 cases of singleton tax credit-related offences perpetrated by HMRC staff, involving inappropriate access to tax records including TC, ITSA, and PAYE. Approximately half of these cases related to tax credits systems or people. The amounts involved have ranged from (most commonly) a few hundred pounds to several million in one particular case. IG and HMRC's Anti Fraud Assurance Team (AFAT) are BC's key stakeholders in respect of internal fraud, and regular and effective communication between BC and both parties remains vital.

12.5 Where an HMRC member of staff is identified as being involved in a potential 'singleton' fraud of this nature IG will routinely conduct a series of intelligence checks, to look for any links to wider organised crime groups. Conversely, where intelligence received indicates a criminal conspiracy or organised attack the personal details of all suspects are checked against HMRC HR data to ensure that individuals implicated are not serving members of HMRC.

12.6 All tax records of HMRC employees, along with any other sensitive records, are held separately within a secure unit. Any member of staff who deliberately or inadvertently attempts to access such a record will be prevented from doing so by the system and a warning will be displayed. A log will also be automatically created with

AFAT and the individual will be challenged about the attempted access and asked to explain their actions.

12.7 In 2008 IG conducted a Strategic Risk Assessment (SRA) of internal fraud and corruption across HMRC, and it is evident from this that BC is considered to be one of the more proactive directorates in tackling internal fraud. Of the 14 self-assessed risks identified in BC's original SRA response, six remain outstanding. The remainder have been addressed, controls put in place and ownership allocated. BC continues to play an active and constructive part in the SRA process and has attended a number of IG-led case de-briefs and organisational learning workshops in which BC systems or people have been involved.

12.8 The main internal fraud risks for BC are inappropriate access to systems and the value of the data they store. BC must remain vigilant to the risks created by so-called 'toxic combinations' whereby an individual is given access to one or more systems (or processes within a system), the combination of which creates an opportunity for fraud (e.g. an individual having the right both to make a payment, and to confirm it).

12.9 It is therefore vital that BC completes its recent stocktake of the allocation of IT licences across the business, which should provide an effective preventive control against the 'toxic combination' risk.

13: Organisational learning

13.1 Organisation learning should be a continuous process that enhances the organisation's collective ability to accept, make sense of, and respond to existing best practice, lessons learned, and internal and external change. It is more than the sum of the information held by employees and requires systematic integration and collective interpretation of any new knowledge, leading to collective action. BC's own internal guidance explains that intelligence is more than simply the information received, but also what you have 'learned' from that information.

13.2 Given that BC is in the early stages of establishing itself in the intelligence community, it follows that their organisational learning may be similarly embryonic. However, some basic principles should apply and already be in place. These include a clear strategy to ensure that processes are evaluated, intelligence is made available to those who need it, cases are debriefed, and any lessons learned are stripped out and recycled back into the front end of the business.

13.3 As mentioned above, BC is not sufficiently 'plugged in' to the wider intelligence/law enforcement community, and there is much it could learn from others. In particular, there has been little (if any) engagement with CI and/or RIS, who have considerable experience that BC could draw upon in respect of 'organised attacks' upon other HMRC systems in areas such as alcohol, tobacco and MTIC. The collective HMRC experience gained in identifying, measuring and countering these organised attacks could be invaluable to BC in developing an effective organised fraud counter strategy; but this resource does not appear to have been tapped.

13.4 Systems and processes to debrief cases, identify and disseminate best practice, learn lessons and recycle that learning back into the business need to be embedded into the BC structure and governance model at the earliest opportunity.

Recommendation 24: HMIC recommends that BC coordinates and delivers a fraud-focused organisational learning strategy for BC. This strategy should address the need to debrief cases, identify and disseminate best practice, and ensure that lessons learned are recycled back into the business.

14: Training

14.1 It is up to the business to decide how much investment it wishes to make in specialist intelligence training or in raising general fraud awareness. Ideally, any investment should be commensurate with the fraud threat, potentially with generic fraud awareness training for compliance officers and more specific targeted investment in training for specialist roles such as intelligence officers in the OAG.

14.2 However, at this stage of BC development our assessment of the training position is summarised as follows:

- There is an over-reliance upon the accrued expertise of experienced staff, with no apparent means to transfer learning to support business continuity;

- There is little evidence of any bespoke intelligence or fraud training. As a general rule, training for those involved in this kind of work was 'on the job';

- Since 2009 there has been a programme of development for compliance officers. There is some belated evidence of Guided Learning Units (GLUs) in respect of the EFAP programme, which have been developed and published since we started the inspection; and

- We found patchy evidence of generic training needs analysis (TNA) being conducted in some areas, but of nothing specific to address intelligence needs or fraud risks, even within the Organised Attack Group.

14.3 Any intelligence or anti-fraud training investment has to be informed by a wider strategy. However, as a first step, a TNA needs to be devised and delivered to 'baseline' the training need. The results should be used to ensure targeted investment in intelligence and fraud training across BC, commensurate with the risks and business requirement.

Recommendation 25: HMIC recommends that a fraud-focused Training Needs Analysis (TNA) be devised and delivered as a matter of priority. The results should be used to ensure targeted investment in intelligence and fraud training across BC, commensurate with the risks and business requirement.

15: Recommendations

Recommendation 1: HMIC recommends that BC establish a fraud golden thread. This should include generic fraud awareness sessions and clearly and regularly communicated trend alerts and updates. Fraud-related objectives should also be included in performance agreements (PDEs].

Recommendation 2: HMIC recommends that BC scans the bar code on each unique claim form (TC 600) prior to despatch so that it can be tracked and tallied upon receipt.

Recommendation 3: HMIC recommends that BC raise awareness of the Call Monitoring Analysis (CMA) system and promote and expand its use as an intelligence tool.

Recommendation 4: HMIC recommends that all complaints teams are given direct access to NTC so that they can make better quality, better informed referrals to compliance colleagues. Feedback should be given to those who have made a referral.

Recommendation 5: HMIC recommends that HMRC considers investment to incorporate NTC data within scope/capability of CONNECT (ICE and ACE). In the meantime HMRC should explore the feasibility and benefits of developing a TC-specific CONNECT profiling centre.

Recommendation 6: HMIC recommends that BC immediately adopts the ‘hotlisting’ facility within CONNECT for intelligence profiling and analysis purposes.

Recommendation 7: HMIC recommends that the HMRC allocation of CONNECT (ICE and ACE) licenses to BC be reviewed and that BC make a business case for at least one ACE license.

Recommendation 8: HMIC recommends that BC use the services of the NDVT whenever they have irreconcilable suspicions about the bona fides of key documents that have been presented to support suspected fraudulent claims. BC should also conduct a cost benefit analysis of further investment in training staff in the document verification process at Tiers 1 and 2.

Recommendation 9: HMIC recommends that an urgent review and risk assessment be conducted of all backlogged and unactioned HUMINT material. This should include an impact assessment against the singleton fraud prosecution pilot cases and any other larger scale CI lead or joint DWP tax credit prosecution cases.

Recommendation 10: HMIC recommends that the BC IT licences stock take be satisfactorily completed as a matter of priority.

Recommendation 11: HMIC recommends that BC consider a new organisational governance model to coordinate all aspects of fraud and intelligence activity. The appointment of a single Head of Fraud and Intelligence should be considered, supported by discrete functional commands to address Prevention, Analysis and Intervention capabilities.

Recommendation 12: HMIC recommends that BC produces a clear, coherent and credible organised fraud delivery plan, with key performance indicators and agreed milestones.

Recommendation 13: HMIC recommends that a clearly stated Organised Fraud (OF) policy statement be established and published. This should be informed by operational policy, drawn from the various ad hoc advises and identified best practice to date.

Recommendation 14: HMIC recommends that BC conducts as a priority review all outstanding HMRC analyses on organised attacks (intelligence reports/threat assessments etc). All recommendations should be evaluated and addressed.

Recommendation 15: HMIC recommends that HMRC commissions some analysis of the role of tax credit frauds may play in establishing attack gateways on other HMRC regimes such as AT, ITSA, SSP/SMP/HiPG.

Recommendation 16: HMIC recommends that BC consider nominating ‘stream leads’ to better facilitate the engagement with, and management of stakeholders.

Recommendation 17: HMIC recommends that BC conducts a ‘stocktake’ of all its existing MOUs (and similarly intended arrangements such as joint intelligence protocols etc) with key law enforcement stakeholders to regularise current engagement and identify future needs.

Recommendation 18: HMIC recommends that BC raises the awareness and understanding of the ERT process across the business, and works to encourage, facilitate and reward those who make referrals of suspicious activities.

Recommendation 19: HMIC recommends that BC engages with and tasks Europol more often in respect of suspected organised attacks upon the tax credit system by crime groups from Eastern Europe.

Recommendation 20: HMIC recommends that BC needs to engage with the FCLO network to promote the true worth of tax credit fraud with a view to developing its relative priority in FCLO planning, resourcing and training.

Recommendation 21: HMIC recommends that BC makes better and more regular use of KAI resource and capability to identify and counter organised tax credit fraud.

Recommendation 22: HMIC recommends that HMRC/RIS does more to raise the profile of organised tax credit fraud across the RIU network via its RIU-embedded officers.

Recommendation 23: HMIC recommends a more robust use of sanctions (civil and criminal] and of the underpinning legislation to deter and prosecute fraudsters.

Recommendation 24: HMIC recommends that BC coordinates and delivers a fraud focussed organisational learning strategy. This strategy should address the need to debrief cases, identify and disseminate best practice, and ensure that lessons learned are recycled back into the business.

Recommendation 25: HMIC recommends that a fraud-focused Training Needs Analysis (TNA) be devised and delivered as a matter of priority. The results should be used to ensure targeted investment in intelligence and fraud training across BC, commensurate with the risks and business requirement.

Appendix A: Acronyms and abbreviations

ACE	Analytical Compliance Environment (profiling tool)
ACPO	Association of Chief Police Officers
AFAT	Anti Fraud Assurance Team
BC	Benefits and Credits Directorate (HMRC)
CI	Criminal Investigation Directorate (HMRC)
CIFAS	Credit Industry Fraud Avoidance System
CMA	Call Monitoring Analysis
CoC-	Change of Circumstances
CONNECT	HMRC Data Profiling Tool
CPS	Crown Prosecution Service
CTC	Child Tax Credits
DSO	Departmental Strategic Objective (HMRC)
DWP	Department of Work and Pensions
EFAP	Error and Fraud Assurance Programme
ERT	Evasion Referral Team
E-SIP	Electronic Suspect Information Package
Europol	European Police
EXCOM	Executive Committee of HMRC
FCLO	Fiscal Crime Liaison Officer
FEAR	Fraud and Error Austerity Response
FFDP	Fiscal Fraud Delivery Plan
FTE	Full Time Equivalent (staff measure)
GLU	Guided Learning Unit
HEL	Head of Exchequer Losses
HiPG	Health in Pregnancy Grant
HUMINT	Human Intelligence
HVR	High Value Renewals
IAD	Internal Audit Division
ICE	Integrated Compliance Environment
IFIG	Insurance Fraud Investigators Group
IG	Internal Governance
ITSA	Income Tax Self Assessment
JIP	Joint Intelligence Protocol
JIT	Joint Intelligence Team (HMRC/DWP)
KAI	Knowledge Analysis and Information

MI	Management Information
MTIC	Missing Trader Intra Community (fraud)
MOU	Memorandum of Understanding
NAO	National Audit Office
NCU	National Coordination Unit
NDVT	National Document Verification Team
NDVU	National Document Verification Unit (UKBA)
NHC	National HUMINT Centre
NINO	National Insurance Number
NRO	National Risk Overview
NTC	National Tax Credits (Database)
OAG	Organised Attacks Group
Ofsted	Office for Standards in Education
PAYE	Pay As you Earn
PDE	HMRC Performance Agreement
PID	Personal Identification Number (HMRC)
RIS	Risk and Intelligence Service
RIS CIG	Risk and Intelligence Service – Criminal Intelligence Group
RIU	Regional Intelligence Unit
SLA	Service Level Agreement
SMP	Statutory Maternity Pay
SNC	Serious Non Compliance
SOCA	Serious and Organised Crime Agency
SRA	Strategic Risk Assessment (of Internal Fraud and Corruption)
SSP	Statutory Sick Pay
TNA	Training Needs Analysis
TPI	Third Party Information
VAT	Value Added Tax
WTC	Working Tax Credits

Appendix B: Terms of reference

Inspection Aims and Objectives

The inspection will assess the effectiveness of HMRC's strategy, systems, processes and behaviours in:

- Identification, development and use of information and intelligence in respect of tax credit fraud;
- Working with internal and external stakeholders to maximise the use of available information and support decision making and risk profiling; and
- Learning lessons, identifying and recycling identified best practice to inform organisational learning.

This will be undertaken through a review of key issues, including, but not necessarily limited to:

- Strategic direction, governance and assurance;
- Analysis of intelligence sources and flows to inform resourcing to risk decisions;
- Guidance and training;
- Effective determination and use of intervention options, including the application of the civil/criminal threshold; and
- Relationships and gateways with key stakeholders (internal and external).

Appendix C: Fraud and corruption definitions

Fraud Act 2006

This categorises fraud in three ways**:**

- 'Fraud by false representation' is defined by Section 2 of the Act as a case where a person makes 'any representation as to fact or law...express or implied' which they know to be untrue or misleading.

- 'Fraud by failing to disclose information' is defined by Section 3 of the Act as a case where a person fails to disclose any information to a third party when they are under a legal duty to disclose such information.

- 'Fraud by abuse of position' is defined by Section 4 of the Act as a case where a person occupies a position where they are expected to safeguard the financial interests of another person, and abuses that position; this includes cases where the abuse consisted of an omission rather than an overt act.

Institute of Internal Auditors

The Institute defines fraud and corruption as follows:

- Fraud: Any intentional act or omission designed to deceive others, resulting in the victim suffering loss and/or the perpetrator achieving gain.
- Corruption: The misuse of entrusted power for private gain, usually characterised by intentional deception or misrepresentation.

NB: So called 'noble cause' corruption would not necessarily sit with this definition of corruption in that it does not pre suppose '***private*** gain'.