COVID-19 FRAUD MINISTERIAL BOARD

Meeting Minutes

19th October, 10.45am

Meeting Attendees

Name	Department	Role
Lord Agnew (Co-Chair)	Cabinet Office (CO)	Minister of State
James Brokenshire (Co-Chair)	Home Office (HO)	Security Minister
Julia Lopez	Cabinet Office (CO)	Minister of State
Paul Golightly in lieu of Lord Bethell, Parliamentary Under-Secretary)	Department of Health and Social Care (DHSC)	Director, Department of Health and Social Care. Anti Fraud Unit (DHSC)
John Glen	HM Treasury (HMT)	Economic Secretary to the Treasury
Will Quince	Department for Work and Pensions (DWP)	Minister for Welfare Delivery
Paul Scully	Department for Business, Energy and Industrial Strategy (BEIS)	Parliamentary Under Secretary of State
Nick Burkitt (in lieu of Simon Clark, Minister of State)	Ministry of Housing, Communities and Local Government (MHCLG)	Director, MHCLG
Laura Clayton (in lieu of Matt Warman, Minister for Digital Infrastructure)	Department for Digital, Culture, Media and Sport (DCMS)	Head of EU Future Funding, DCMS Grants and Fraud (DCMS)
	Secretariat Officials	
Lyn McDonald	Cabinet Office	Director, Fraud, Debt and Grants Functions
Mark Cheeseman	Cabinet Office	Director of Public Sector Fraud
NR (in lieu of Duncan Tessier)	Home Office	Deputy Director, Fraud Policy, Serious and Organised Crime Group
Graeme Biggar	National Crime Agency	Director General, National Economic Crime Centre
NR	Cabinet Office	C-19 FMB Secretariat (Counter Fraud Function)
	Cabinet Office	C-19 FMB Secretariat Support (Counter Fraud Function)

Agenda

Agenda Item	Paper
1. Welcome and Refresh	**N/A**
2. Intelligence Sharing	**Paper 1** - Investment in Intelligence Sharing
3. Lessons Learned	**Paper 2** - International Lessons Learned
4. Bounce Back Loan Threat Assessment	**Paper 3** - Criminal Exploitation of the Bounce Back Loan Scheme
4. AOB, Risks and Meeting Close	**N/A**

Actions & Agreements

Agenda Item 2: Intelligence Sharing.

Agreement: The principles and recommendations within the Intelligence paper were agreed. Specifically;

- **Access to criminal intelligence** is increased and provided through a central team. The central team will coordinate information to and from the public sector, and support better sharing of information within the public sector.
- **An intelligence capability rating is introduced**, managed by the central team, to identify which departments in central government have the capability to (i) access relevant intelligence and (ii) respond to it appropriately.

Note: this is subject to the spend review approval and the board asked for consideration of how Local Authorities could access criminal intelligence through the central team and how we can build in additional sources of data (e.g. CIFAS) and focus on prevention..

Agenda Item 3: International Lessons Learned.

Agreement: The principles within the International Lessons Learned paper were agreed and support given that they should be adopted for any new COVID-19 financial support package and economic recovery schemes. Specifically;

- That fraud risk assessment should be undertaken by skilled people before funding is agreed.
- When large or priority schemes are set up, it should be accompanied by fraud and compliance activity.
- That a clear plan to check the funding should be in place at the start of the scheme.

Agenda Item 4: Bounce Back Loan Threat Assessment.

Action: The Board requests that the actions and next steps of the BEIS led Cross Government Senior Officials Meetings on Bounce Back Loans Fraud be reported to the Board with clarity on roles and responsibilities of the organisations involved.
Action: The board requests that HMT and BEIS look at what further checks using can be taken on those applying for a Bounce Back Loan to accelerate this work.

Agenda Item 5: AOB

Action: There is an increased risk from wider scams related to fines being issued for non-compliance with other legislation (such as self-isolating). BEIS are to ensure the public awareness activity that Citizens Advice are undertaking is shared with HO.

Minutes

1. **Welcome and Refresh**

   Lord Agnew, welcomed attendees to the meeting.

2. **Intelligence Sharing**

- JB: This paper sets out the options proposed to strengthen our collective intelligence sharing capabilities to better deal with the fraud threat, understand it, and act accordingly. Do we agree there is insufficient capacity and capability which has hindered our counter fraud investigative capability and whether we support the two proposals outlined? The concern is whether, even if we have a better understanding of intelligence, will it take us far enough to confront and block the fraud?

- MC: The paper we have today looks at one of the 4 areas that this board said it will look over: 1) legislative options, 2) post-event assurance, 3) intelligence and 4) lessons learned.

  This isn't looking at funding, but principles and concepts. From where I sit as head of the Counter Fraud Function, we look centrally at what work departments are doing on fraud. Traditionally, intelligence between the public sector, banks and law enforcement bodies has been limited. It has been about those who have the confidence and capability to do it.

  Covid has shown us the power of intelligence sharing, for example through the work that DHSC did on PPE procurement fraud. The links built between NCA and DHSC showed us that fraudulent payments worth £72 million had been made. The intelligence shared allowed us to act a lot quicker that we might have.

  The main principle in the recommendations is to increase public sector access to intelligence (such as access to SARs, PND and PNC databases).We shouldn't be satisfied with the current level of access to intelligence across the public sector.

  If we want to do this, we must do it in the most efficient way. It will take much longer to invest in each public body and ALB and build up its intelligence capabilities and it is an expensive process to carry out across our diverse system. The best way is to have a central place, not necessarily the Cabinet Office, that has the power to take intelligence and disseminate it across the public sector.

  The other principle is to build up departments' capability and awareness to be able to respond to intelligence. Transparency of departments' levels of capabilities will help ministers and senior ministers to understand what areas need more intelligence sharing support.

- JB: The work with NCA and DHSC gives us a strong evidence base of the importance of intelligence sharing. It also shows what alerts we'd need to send out to other government agencies to ensure that departments are made aware of fraudsters that may target more than one agency. We also need to think about how to build insights from other third parties (e.g CIFAS) as we know that this work will be stronger if there is a blend of intelligence.

- NR Thanks Minister I support that. The first stage is advising on schemes as they are being set up to reduce the risk from the start. The second stage, like when people fraudulently applied to supply PPE, is recognising fraudulent applications upfront. The third stage is where SARs reports k can identify a transaction when it is happening and allow action to be taken soon after. The fourth stage is investigating once you see a fraud has taken place.

  The key is to do as much of stages 1-3 as possible. Investigation is expensive once the money has gone out. We've designed the intelligence piece to hit the top layer first and then the other ones consequently.

  There is more that can be done to share information between departments so that we know what is happening. With BBLs we see references to Romanians and Albanians, suggesting that there is a Balkan nexus, which links to self-assessment tax return fraud and furlough scheme fraud. We can spot this and take action if we join up on the intelligence.

- JB: There is an emphasis on protection and prevention, so it is much better to stop money going out in the first place rather than going out and trying to recover the money afterwards.

  Lyn Owens flagged a challenge in relation to BBLs. There are certain elements of data being held in a redacted format, meaning some of the sharing we're discussing may not be as useful as it seems. We want to discuss this to know in what format the intelligence is held, and if there are any residual regulatory concerns that others may have in terms of the ability to share data (notwithstanding the legal gateway allowing the sharing of data in the prevention of crime).

  We also have a question on the timing. If we have to wait for SR bids we're talking next year. What can we deliver using our existing systems and structures that lay the ground in order so that we can have a new configured system envisaged by the paper and feel the effects sooner rather than later?

- JG: Firstly, I've seen a lot of this commentary on BBL as if there was a willful disregard to the risks from the outset. This wasn't the case. Counter fraud and KYCs were designed into the scheme from the start with a system to avoid duplicate applications to multiple lenders, and authority to work at identifying risks. The issue is what is then done with SARs, how that is processed and how to effectively move on.

  In the NCA letter, it said that there was no agreed reporting channel for Bounce Back fraud, but this isn't true as British Business Bank does have something operational.

  I'm supportive of the move to improve fraud analytics and GIAA. The challenge in the design is if you give people self certification mechanisms, you create risks. Where will this monitoring lead to effective enforcement action rather than just claiming there is a risk? When it comes to designing we can't operationalise this, but we can work with delivery partners to amplify concerns and get a better understanding of where the risks are.

- PS: We have a good relationship in BEIS in terms of intelligence sharing with Local Authorities regarding business grants. It is important to remember this shouldn't all be looking at central government. We need to look at delivery partners. This worked well with Local Authority grants. Because of the policy decisions to move at speed, we need to see how to get intelligence sharing to the lenders at the sharp end. I want to see more proposals consulting with delivery partners based on their needs.

- NR Do Local Authorities have the capacity and capability - no. The point raised in the paper is that we need expertise in the particular department setting up the schemes. With the business grant scheme, Local Authorities were used to dealing with large businesses because of business rates so they could check legitimacy. But more recent work on self-isolation fines for example, is new to Local Authorities. It is important that expertise is given to the leading department as the impact on lives can be enormous.

- JB: As we look to create centralised reports, it isn't just about inputs coming in, but also how intelligence flows outwards so that all agencies are properly informed on the decisions they're taking so we can prevent and protect.

- PG: I am supportive of the paper and direction. As mentioned earlier we benefited from the intelligence flow that came through, which helped us avoid unnecessary PPE contracts. There may be possible benefits here in including intelligence in the profession. This would give us the mechanism to assess the capability of departments early on and highlight gaps. That body of evidence may help with reassurance around the redaction of intelligence reports. Where there is confidence, more intelligence can be shared.

- LA: We've set up a legal advice team at the Centre for anyone worrying about GDPR with regards to sharing this data. If any department is worried about this, there is a central resource run by DDaT to try and get data to flow faster and more efficiently through departments.

- JB: Knowing this resource is here should ensure people don't have an excuse to not share data, when clear gateways are available to enable this.

- MC: In terms of doing this in the short term, CO has funding from HMT to support departments with covid and we have an intelligence function to help this. In terms of redacted data, the legislation paper at the next Board will reference discuss this in more detail. There is also scope to include Local Authorities in order to bring together the broader public sector.

- **JB: [Agreement]:** The recommendations within the Intelligence paper are agreed subject to consideration of how Local Authorities could access criminal intelligence through the central team.

3. <u>Lessons Learned</u>

- MC: Cabinet Office leads the International Public Sector Fraud Forum, which is made up of the Five Eyes and comes together to talk about public sector fraud and how it's dealt with strategically and in practice. We meet almost every other week at the moment to discuss how we're dealing with Covid19 fraud, discussing intelligence and country-specific cases. The key points in the paper are:
    - That fraud risk assessment should be undertaken by skilled people before funding is agreed.
    - When large or high profile schemes are set up, funding should be set aside for fraud and compliance activity at the outset.
    - A clear pan to retrospectively check payments should be in place at the point the scheme starts to distribute spend.

  These are things that can happen quickly. When funding decisions are made quickly it is difficult to get a skilled person to undertake an FRA, but it can be done soon afterwards. In relation to funding set aside for fraud and compliance activity, high profile schemes in the US had funding and compliance set up immediately. Finally, the clear plan for retrospective checking in those high risk schemes aligns with the post event assurance activity we're discussing in this Board, which will then be formalised in our future way of working.

  The practical plans needed to implement these lessons are first, we need the Board to say if they are comfortable or not. If they are, we'll take it forward with GIAA, HMT and lead departments to talk about how to put these in place. We can apply these to new schemes as they come up and report back the future lessons learned.

- MC: The FRA is complementary to the process of accounting officers seeking ministerial directions. The fraud risk assessment can inform the conversation between ministers and officials.

- LA: The accounting officer certification is a neat and tidy way for HMT to know where responsibility lies. But officers are overloaded with responsibilities and don't have a view of the whole landscape, particularly with something like fraud that is fast moving. We need structures to work automatically as we don't want officers working on things they don't have time or expertise to comment on.

- **LA: [Agreement]:** The Board agrees on these lessons learned and this will influence any future discussion with HMT on how to manage schemes and how to work on existing schemes by strengthening procedures in place.

4. Bounce Back Loan Threat Assessment

- JG: The commentary at the moment is about conceptual risk without quantification. I want to get into the practicalities of what can be done to mitigate the risk going forward.

- LA: At the moment there is a disjunction between the political imperative to get money out quickly and the ability to do two or three more checks that would prevent money going out in less than 48 hours. Why don't we do a job properly and get money out a bit later but carry out two or three more checks?

- JB: What tensions are in the system that mean some of the normal fraud checking is not being done? In terms of risk, if the bank has not done the checks, you'd say they are guaranteed to not operate in that environment. It is important to understand where the bar has been set on that and whether there has been confusion, or whether the banks properly understand that. The conditions on how people behave should be germane to how bank credit committees are acting.
- **NR** Taking John's point into consideration, the pushback is if the risk is conceptual or real. The risk has been conceptual since the beginning, but we're keen to understand what the risk is, which is the hard part. That's why our paper doesn't come up with a definitive figure. Other helpful figures and summaries however, are that:
  - So far, 10,000 SARs have been reported to us (this was where the figure stood a few weeks ago, so it has probably increased by about 2000 since then). This is a small figure in terms of the number of applications, but it is not representative as they come from only one bank that has chosen to report itself to us. As a result, we think there'll be at least as many SARs from all of the other banks, which when added together, present large figures.
  - The banks also tell us that they're seeing ten times more fraud in these applications than in typical loan applications. The indicators are that the risks are large. The challenge though, is whether the risks within a scheme are aligned with the necessary capability or responsibility. For example, SARs come in from the furlough scheme, HMRC then analyses them with their strong intelligence capability and then takes action. With BBL, there isn't the force or organisation there with the responsibility and capability to do the same, hence BEIS has worked with NATIS on the risk. The question here however, is whether they have the capacity.
  - The key is to: 1) reduce more fraud going forward (ultimately a political decision because it requires slowing down money going out the door when it is imperative to get it out); 2) consider whether we need to increase the effort to reclaim money or investigate people (NATIS is doing some of this work, BEIS is getting help from the insolvency service, NECC is working with HMRC); 3) learn from lessons and align responsibilities and capabilities when future schemes are set up.

- JB: In terms of where the risks lie, whilst there is the desire to get money out of the door quickly, we still expect banks to conduct KYC and due diligence.

- JG: There is the need for collaboration with banks to look at patterns of behaviour and fraud. The tension between the political imperative of rapid delivery and how this is being distorted by fraudulent applications and vehicles needs to be discussed. The rate and volume of money going out has declined significantly, but the scheme will still be going out so I am supportive of anything to invigorate KYC and due diligence checks within the framework of immediate access.

The issue of SARs is how they're taken up in relation to Graeme Biggar's third point. The need is to demonstrate the real risk of fraudulent applications in terms of the consequences and create an engine of motivation to respond.

The risks of duplication, KYC checks and cooperation between lenders to refine practices has been built into the BBL scheme. We'll continue to work with banks and all other organisations involved to work out what more needs to be done. The main challenge is the gap left by the credit check that was intentionally designed out of the scheme at the start for political reasons. We need to invigorate the NATIS work and move forward with data rather than conjecture.

- PS: We agree we need more action with CO and HMT to support businesses. We are currently:
    - Increasing funding to expedite sampling work done by PWC to better understand the scale and nature of fraud.
    - Our Secretary of State also agreed to double fund the NATIS work with the option of scaling up capacity in future years based on results.
    - Working with HMRC on frauds that straddle loan and furlough schemes, with the Insolvency Service tackling misconduct. There is also the option to scale this up in future years based on results.
    - Lenders saw billions in fraudulent cases in the first place and they will see the cost of where they failed to put in checks. They therefore need to separate instances of fraud by OCG and legitimate business that inflated turnover figures but used funds to sustain jobs. We are working with HMT to review this.
    - Working on a comms strategy to get the messages out that we'll take action on fraud.

- MC: In agreement with John Glen, we do want more data behind this work. We do have a workstream already that is doing pilots with banks looking at key fraud risks. I recommend we accelerate this work. Banks have counter fraud capability, but it would be good to see pilots finishing every other day and sharing information on a weekly basis so that decision makers can flex the system when necessary.

- JB: There are some issues where the credit risk lies, and as discussed with JG, the way banks are operating. We're coming towards the end of the scheme, and timing wise, it's not as acute as getting money out of the door as it was earlier in the scheme. Therefore the extent to which we can step up and do more to apply the credit checks and therefore prevent money actually leaving, the better.

  Secondly, we need an understanding of who is doing what here to ensure we're all acting in alignment and recognising the different interests and capabilities. The work that Paul and the BEIS team is doing links to NECC such that if an OCG link is detected, NCA will pick it up. Clarity is needed on who is doing what to prevent conflict and ensure the efficient use of resources, and data is also needed to give a clearer picture.

  There are case studies with shelf companies, multiple accounts and IP addresses for multiple applications. How best can we feed practical outcomes into the system to better equip people to know what they're looking out for with applications?

- JL: [comment made on chat] "*Afraid I have to go but wanted to make a point that it is for us to anticipate the change of politics in this. We are moving into a different stage of the pandemic - urgency was required and understandable at outset. Now it will be expected of us that we will be tightening up procedures, whether contracts, fraud risk etc. We are losing huge sums of money at a time when we are anticipating tax rises. Colleagues will start to press us on that before long. Apologies that I cannot stay for the whole meeting.*"

- **JB:** The Board is clear on steps to be taken **[Action]**

- **Action:** The Board requests that the actions and next steps of the BEIS led Cross Government Senior Officials Meetings on Bounce Back Loans Fraud be reported to the Board with clarity on roles and responsibilities of the organisations involved.
- **Action:** The board requests that HMT and BEIS looks at what further checks can be taken on those applying for a Bounce Back Loan

5. AOB, Risks and Meeting Close

- JB: One thing to highlight is to keep an eye on an increased risk from wider scams related to fines being issued for non-compliance with other legislation (such as self-isolating). Law enforcement is linking with DHSC, but we need to keep an eye as these risks may emerge over time. We also need to think about how to respond to these risks with the messaging. This is something to be vigilant about at this stage.

- PS: Citizens Advice are working on this. I will make sure they're passing back information back to us. **[Action]**

  - **Action:** There is an increased risk from wider scams related to fines being issued for non-compliance with other legislation (such as self-isolating). BEIS are to ensure the public awareness activity that Citizens Advice are undertaking is shared with HO.