JobsAware – Written evidence (FDF0043)

About JobsAware

JobsAware (c/o SAFERjobs CIC) is a not-for-profit working to protect work-seekers and non-permanent workers from labour market abuses. Starting out as SAFERjobs, a cross-Government and private sector collaboration established by the Metropolitan Police, it has built a profile and awareness of the risks of online fraud in relation to fake and scam jobs. Since its establishment in 2008, SAFERjobs has continued to grow, launching the JobsAware brand in 2021 widening its scope to ensure work-seekers as well as workers in the non-permanent space (such as agency workers and gig economy) have their rights promoted.

JobsAware encourages individuals to report instances of fake jobs and other labour market abuses via its website (jobsaware.co.uk) and has a number of committees focused on various areas of the labour market. These committees are formed of Government bodies, private sector and public sector organisations and work towards improving the rights of workers in their relevant areas.

JobsAware are providing a response to this Call for Evidence as it is alerted to potential fraud and fraudulent activity on a regular basis through its work in protecting workers and work-seekers.

Contact: lauren.edwards@jobsaware.co.uk

Fraud Landscape

1. What fraud risks are UK a) individuals, b) the Government and c) businesses particularly vulnerable to today, and what are the reasons for this?

JobsAware (c/o SAFERjobs CIC) sees the main and growing fraud risk for all of these groups as online fraud. Action Fraud saw a reported £9.6million lost by victims of cybercrime in 2020/21[1] and the UK economy as a whole is reported to have lost £2.5billion to fraud and cybercrime in 2021[2].

Increasingly more activity occurs online, and this is a growing trend, particularly in the field of jobs and employment, where most people now search for work online; the hiring process can now be conducted fully remotely and online; and more people work online with the upshoot in remote, flexible working following the COVID-19 pandemic.

To provide some context to the risk around online fraud and seeking employment, a survey from 2021 of over 1500 work-seekers showed that 74% of them believed they had applied for at least one job that did not exist. In our experience, the prevalence of fake online job adverts continues to increase, and the reason for their being is to defraud work-seekers by stealing their personal data, taking money for fake services (advance fee fraud), or leading to a range

[1] Microsoft Word - 2020- 21 NFIB Annual Assessment - CYBER - PARTNERS - Final.doc (actionfraud.police.uk)

[2] UK loses £2.5bn in fraud and cybercrime cases during 2021 (cityam.com)

of other types of criminality such as money laundering, modern slavery, or boiler room scams.

The UK's general public will continue to be particularly vulnerable to this type of online fraud due to the rising cost of living and the subsequent need to gain employment or increase their earnings.

2. What future economic and technological developments are likely to impact how fraudsters seek to commit crime over the next five to ten years, and how might these be prepared for and mitigated? What role can technology and tech companies play in combatting fraud across this timescale?

In respect of online fraud risks, certainly within the UK labour market, we estimate that the following developments will impact the prevalence and methodology of fraudsters over the coming decade.

Economic developments include the rising cost of living influencing an increased need to earn more money. Inflation and the rising energy and food prices are currently outstripping wage inflation, causing the need to find new work or get into work, encouraging more individuals to seek employment and exposing themselves to online fraudsters. In our experience, online fraudsters follow and remain ahead of economic and social trends, so we expect their presence to only extrapolate given these economic circumstances.

Technological developments include the move to more online business models following the pandemic. Many UK businesses now work at least somewhat online and remotely, with many moving to fully online business models. These online business models include fully digital recruitment processes allowing for the seamless recruitment of staff from anywhere in the country (or world). Along with this comes the ability to offshore businesses, with new and growing technology usage expanding business' ability to transact internationally. Eventually, developments in what is known as the metaverse will have an impact on how fraudsters behave, however it is too novel to understand the impact of this yet.

One of the key ways that technology and tech companies can prepare for and mitigate these developing risks, is by educating and promoting how to keep personal details safe in a digital world. Often it is a lack of understanding or awareness that exposes individuals to online fraud.

3. Is fraud and its victims treated as a priority? If not, what are the reasons for this. The Committee is particularly interested in responses that can explain any barriers preventing effective counter-fraud cooperation within Government, law enforcement, the public sector and the private sector.

In our experience, victims often tell us about losing their personal details or money in an online fraud and not getting enough support or recourse from law enforcement. This is often because the people behind the fraud are not based in the UK making proactive and effective law enforcement action difficult.

Private sector should have more responsibility to protect users of their platform or services. For example, in the case of the online jobs sector – described by former Director of Labour Market Enforcement, Matthew Taylor, as being poorly regulated – there is no onus on the private sector to a) ensure the job adverts are real, b) assist work-seekers who are defrauded or scammed as a result or c) ensure the jobs being promoted are in line with UK law. This is a particular example of a much wider challenge with the private sector.

Nonetheless, there are private sector businesses that do already reimburse their customers when they have been a victim of fraud on their platform, causing the business to become a victim itself. This could be said also for businesses that become a victim to the Insider Threat (an employee or trusted contractor defrauds an organisation). In cases such as this, it is not often that the business is able to recoup the money lost or achieve a prosecution for numerous reasons which could include reduced law enforcement resource or lack of evidence. In the case of the former, it would be ideal for any future legislation around Fraud to include a section permitting and encouraging the ability to pursue a private prosecution.

An additional barrier to effective counter-fraud cooperation is the lack of ease and method through which law enforcement and the private sector share intelligence. We believe there could be a better way for law enforcement and private sector to share intelligence, perhaps via a non-partisan organisation. Part of this issue has been exacerbated by the private sector often using the GDPR as a reason not to share information.

4. What is the role of international actors in the UK’s fraud landscape? What are the barriers to tackling borderless fraud?

Technology and the popularity of online activity enables borderless fraud, allowing international fraudsters to be able to access the UK public with little recourse for punishment, and this is only likely to increase in future as technology becomes embedded in the way of life.

The barriers that we see to tackling borderless fraud are numerous, the most compelling being the complexity of cybercrime. The online fraud that we see often includes a multitude of websites and platforms linked together, often based overseas, with various methods of communication used and international groups involved. In addition, the use of offshore bank accounts means that often the money has left the UK within seconds of it being received by a fraudster, becoming difficult to reclaim. The pace at which technology is evolving adds to this complexity, and fraudsters are able to keep up with these trends more swiftly than law enforcement or large public and private sector organisations.

An additional barrier we believe hinders UK law enforcement is the inability to co-operate cohesively with overseas law enforcement agencies, especially those in unstable economies where many of these fraudsters are located. Given the complexity of cybercrime, and often the lack of evidence available, we can deduce why it would be difficult for local law enforcement to tackle the issue alone.

Finally, we see a long-standing perception that fraud is a victimless crime, certainly when it is committed against a business. Whilst we see this changing as the issue grows and more individuals are impacted, we see that this perception leads to a less favourable experience for fraud victims, across both public and private sector, as well as within the general public.

Action to Tackle Fraud

5. How effective is the current structure for policing fraud? How successful are the City of London Police, including Action Fraud and the National Fraud Intelligence Bureau, at executing their role as the lead police force for fraud?

In our view, there are vast opportunities for the current structure for policing fraud, especially online fraud, to be improved. Through our experience, there is a perception from work-seekers that Action Fraud is not a proactive enough function. The complexity and scale of the crime has changed over the last decade, and the growing number of opportunities for fraudsters means the current structure requires much greater resource than is currently available. As part of the review of policing fraud, we would anticipate a review of the current structure and the level of involvement and resource of local police forces and other supporting organisations. We appreciate the work of City of London Police in their recent prosecution of a fraudster advertising fake jobs in the UK, and recognise that, where the evidence, resource and authority allow, the current structure is able to police fraud. This is made difficult however when you consider the barriers referenced in our response to question 4.

6. Are sufficient resources available to Government organisations (such as the Serious Fraud Office and Crown Prosecution Service) and wider police forces to tackle fraud and support victims, and how should this be addressed if not? Answers need not be limited to financial resources.

In our experience, there are not sufficient resources available to Government organisations or wider police forces to tackle fraud and support victims. The types of resource we would call for more of are firstly more people resource to be able to manage the volume and growth of fraud. In line with this, we would encourage additional training resource for local police forces, specifically around recognising and tackling online fraud in its many forms, so that fraud cases and its victims are directed to the right place with an appropriate level of support. In addition, it could be useful for specialist teams to engage with the private sector and technology companies to receive training and information on upcoming trends in the tech space, so that Government and law enforcement can be ahead of the fraudsters.

7. What are the responsibilities of the private sector in protecting the public against digital fraud? How can a balance be achieved between the need to tackle digital fraud whilst supporting the growth of these sectors? To what extent is work done to combat fraud across the private sectors undermined by siloed or independent working practices?

The private sector should firstly have more responsibility to protect its users and customers. This could take many forms, including advice on fraud, support when something goes wrong and accountability for what is provided to customers. This is already visible in the financial services sector, but could be expanded to other sectors, in our case, online recruitment and job boards. Increased legislation in some sectors, such as the online jobs sector, where there is a responsibility to ensure that products being advertised are genuine, could support this. For online fraud, the upcoming Online Safety Bill and DCMS' Online Advertising Programme are a good opening to this. Supporting and protecting their own customers is something that the private sector could and should do, and this would allow for a balance between the need to tackle fraud whilst promoting business growth. In the online jobs sector, for example, this could come in the form of business' self-regulation.

Combatting fraud in the private sector is siloed, and even within the public and third sectors, there are organisations focused on varying types of fraud, however there is nowhere bringing it all together. This way of working in the public and third sectors creates a barrier for the private sector in combatting fraud, as the private sector do not know where to go or who to contact. In addition, the private sector, especially organisations with large, recognisable brands, may avoid reporting fraud altogether to evade any repercussion or reputational damage that may ensue.

8. What are the legislative or regulatory impediments to sharing fraud risk data across and between the private and public sectors? For example, to what extent does General Data Protection Regulation (GDPR) limit data sharing?

In our experience, as an organisation encouraging the sharing of fraud risk data in the private sector, GDPR is sometimes used as a reason for private sector organisations to not to share fraud risk data, whether this is legitimate or otherwise. This could come from a fear of getting something wrong, or as a deflection to engaging with collaborative activities to tackle fraud, however it is clear that companies would rather not share data than face investigation by the ICO, for example.

9. What is the role of the individual in relation to fraud? Are consumers well informed about the risks of fraud and how to prevent them? If not, which bodies or organisations should do more to ensure this? What are the most effective methods of educating the public about fraud crime and prevention?

Consumers today are much better informed around the risks of fraud than a decade ago, that is certain. We have seen an increase in individuals coming to JobsAware having already recognised potential risks and looking for validation. Nonetheless, individuals receive and recognise the big messages around fraud risks and what to look out for, but when in the detail or the moment, it is not the first thing that they think about. Whilst awareness is greater than ever before, when pressure is applied, individuals do not recognise fraud still until often it is too late. There continues to be a lack of cohesion for individuals on where to go for advice, how to report a fraud etc.

An effective method of ensuring individuals are informed, and recognising fraud in order to prevent it, could be the action of reaching the individual at the moment that the fraud might be happening. The banking sector is a good example, where there is a requirement for individuals to review that a payment is not fraudulent before they send it. The private sector should take some greater responsibility to protect individuals, notably its customers or users, from fraud. Other methods of reaching the general public could include TV and media campaigns, and educating children in schools, who could then educate their parents, grandparents etc.

Legislative Remedies

10. What is your assessment of the Fraud Act 2006? What has been the impact of the Act and is it having any unintended consequences; if so, what are these?

The Fraud Act 2006 was an excellent and necessary step forward, as specific legislation defining Fraud and its remedies was greatly needed. It has allowed law enforcement to treat fraud as a criminal offence and the general public to recognise fraud. Unfortunately, due to the ever-changing nature of fraud, we believe the Act has reached the maximum impact it is able to have without amendments, because it does not reflect the issue and complexities of digital fraud or recognise greatly enough the Insider Threat.

11. Is existing legislation effective in tackling the increase in modern forms of fraud? If not, is there a legislative remedy, or should fraud be addressed primarily through implementation of existing provisions? Answers may refer to existing mechanisms such as increasing the scope and powers of regulators. You may refer to any legislation and are not limited to the Fraud Act 2006

Unfortunately, as referred to in our response to question 10, existing legislation is not effective in tackling the increase in modern forms or fraud. There needs to be legislation which covers the online space and digital fraud – the Online Safety Bill will likely address some of these areas, but digital fraud will need to be defined in legislation, perhaps as a new area of the Fraud Act in addition to the current three areas (false representation, failure to disclose information and abuse of position). A legislative remedy to encourage the private sector to be more engaged with combatting fraud could be to include a Failure to Prevent section, similar to what is available in the Bribery Act 2010.

12. Is the current system in place for prosecuting fraud cases working effectively? If not, what are the key barriers to prosecution?

Not answered.

13. Are sanctions and penalties for criminals who commit fraud an effective deterrent against future criminal activity, and if not, what might be more successful? Respondents may choose to refer to penalties imposed by the judicial system or by specific sectors.

We see the current sanctions and penalties for criminals who commit fraud as not being an effective enough deterrent, the main reason being that often these criminals are able to keep some or all of the assets and money they have obtained via their criminal activities. This is likely to be in part due to their use of offshore bank accounts. The publication of sanctions and penalties could also increase the impact that the sanctions have as a deterrent.

Best Practice

14. What lessons can be learned from effective policy interventions and schemes both in the UK and overseas?

Not answered.

15. Can you suggest one policy recommendation that the Committee should make to the Government?

Not answered.

22 April 2022