**NAO Podcast on Online Fraud Transcript**

**The NAO has conducted a study into the rapidly growing threat of online fraud. The study examined how the nature and scale of the threat of online fraud is growing and changing; and how the Home Office is working with police forces and police and crime commissioners; other government departments and agencies; and industry experts to prevent and reduce online fraud. I’m joined by Louise Bladen, a director who worked on the report. Thank you for joining me Louise.**

**Firstly, what does your report cover?**

Well our report covers two main themes: It explores the nature and scale of online fraud, which is a rapidly growing threat; then it looks at how government and others have responded to that threat, as you’ve mentioned. So just turning to the nature and scale of the crime: In 2016, we found there were an estimated 2 million online fraud incidents, which is about 16% of all crime and it’s the mostly commonly experience crime in England and Wales. At least 6% of adults are victims of fraud and it can affect anyone. We were surprised by this actually, we were expecting that it was going to be particular types of people, but actually everyone is equally affected.

What’s interesting is that online fraud now has lots of different variants. For example, it can be criminals accessing peoples bank accounts, it can be using there plastic card details or actually just tricking them into transferring money themselves. What’s also interesting is that online criminals target thousands of people from anywhere in the world, so they’re really hard to trace and prosecute. That means the true cost of online fraud is unknown, but it’s likely to be billions - one estimate to the annual cost to individual is £10 billion.

We also looked how Government and others responded to the threat, so the principle body is the Home Office, which is responsible for reducing and preventing online fraud and our report looks at how it is working with others to do this, including through its new joint Fraud taskforce which it set up in 2016. Overall we were concluding that online fraud is high volume, often low value crime and it’s been overlooked for far too long by government, by law enforcement and by industry, and the response just hasn’t been proportionate to the scale of the threat.

**So what makes online fraud so challenging to tackle?**

I think there are three key things here. The massive scale and hidden nature of the crime, which I have already talked about. So there were 2 million incidents last year, but the crime is really severely under reported as only 20% of victims report it to the police. We found that in 2016 only 623,000 incidents were recorded by the police. Also criminals are anonymous, they can commit fraud from overseas –it’s an international crime, so its not easy to pursue and prosecute. There’s also a lot of different organizations playing a role across the private and public sectors. So in government alone you’ve got: The Home Office, The Ministry of Justice, The Cabinet Office, The National Cyber Security Centre; you’ve got police forces, you’ve got industries, for example the banks and retailers. Now some of these organizations come together under the new Joint Fraud Taskforce, but we found the Taskforce has quite a narrow focus just on the banking industry and we felt it needed to grow. There’s also a lack of data, so as well as the underreporting, even where data is available, we found its not always reported or shared between industry, law enforcement or government.

**And who is responsible for policing online fraud?**

Well it’s actually quite a complex picture here. So the City of London Police is the national lead police force, and that force overseas a body called Action Fraud, which is the UK’s national reporting center for fraud. There’s also the National Fraud Intelligence Bureau, which leads on reporting and it passed cases onto police forces for investigation. At a more local level you’ve got police forces themselves, who are responsible for reporting fraud cases to Action Fraud and investigating cases passed to them by the National Fraud Investigation Bureau. Those forces are accountable to Police and Crime Commissioners, so these are the people at a local level who set a force’s priorities and work with local partners to prevent crime. At a more national level you’ve got the National Crime Agency, which leads, supports and co-ordinates the response to serious and organized crime, including cyber- enabled fraud. Then you’ve also got the banks and industry who’ve got a role to play in terms of making sure they protect the public from fraud. So quite a number of bodies involved here.

**Would you say there are geographical disparities in the way online fraud is dealt with?**

Well the Home Office as the lead department, now sees online fraud as a national priority, and it expects local police forces to respond as such. But when we looked we found only 27 of 41 of police and crime commissioners actually referred to online fraud in their police and crime plans, so that was quite surprising no one else had picked up on this.

We also found that the local police response varies. So some forces are not really aware of their responsibility for reporting to Action Fraud. Others may not prioritize or investigate cases, and that’s usually due to a lack of skills and capacity. At a more local level, it’s interesting because online fraud requires a new and different type of response, but the focus is still very much on neighborhood policing, so one in six police officers main function is neighborhood policing. This compares to one in 150 whose main function is economic crime. We did find some examples of good practice- Sussex Police is a good example here – they had an initiative to help bodies such as banks and charities identify potential victims.

**And what part does educating consumers play in helping to reduce the risk of online fraud?**

So the growing scale of online fraud suggests many people are still no aware of how to keep safe online, so education is needed here, but there’s a lack of consistency and co-ordination in how these education campaigns are run. So we found in March 2017, Government and other bodies were running over 10 different campaigns. So there were different organizations running the campaign, there were different messages not tailored for specific groups, and that can actually confuse the public and reduce the impact of the campaigns. There’s also something about going beyond education, so that makes sense and that’s something Government needs to do, but it also needs to think about how it protects citizens so how does it make the internet and email more secure. And the banks need to think more about how to protect customer data.

**What does your report recommend?**

All our recommendations center around how the Home Office works with other partners. Firstly the Home Office needs to work with partners on its task force, including banks and law enforcement agencies to publish information on its performance and future plans. It needs to be clearer about the different responsibilities of all the partners involved in preventing and reducing online fraud; and also think about expanding its membership so it goes beyond banks to retail and digital sectors.

We also recommend the Home Office and the Task Force partners need to think about how its establishing arrangements for identifying success – so how does it measure and track benefit, how does it set beachlines for knowing what good looks like. Then there are intelligence gaps; the Home Office needs to work here with the City of London Police and the banks to improve the collection and reporting of data on fraud. It should also work with Police and Crime Commissioners and Chief Constables in local police forces to identify and share good practice models of policing and tackling online fraud – and really helping police forces making fraud a strategic priority. One thing we think could be useful here is if the Home Office commissioned HM inspectorate of constabulary, because they would be able to undertake and national, thematic inspection of police forces performance in tackling fraud.

And finally the Home Office needs to think about working closely with the Ministry of Justice to improve data on fraud prosecutions to help inform future prosecutions and also to examine the sentencing guidelines on fraud and whether the impact on vulnerable victims is taken into account sufficiently in sentencing.

**If you would like to find out more about this report, the full report and an executive summary are available on our website,** [**www.nao.org.uk**](http://www.nao.org.uk)**. Or you can follow us on twitter @NAOorguk or on Facebook www.facebook.com/NAOorguk/**

**Thank you for listening**