

Critically examine the challenges associated with investigating the different types of cyber-crime and police responses designed to combat these challenges.

Introduction:

Ever since the internet first got created it has opened up new doors to criminals to commit crimes in more efficient manners. Some of the most common online crimes in the UK were crimes involving cyber security attacks with 'four in ten businesses (43%) and three in ten charities (30%) reported having any kind of cyber security breach or attack' (Department for Science, Innovation and Technology, 2025) The reason as to why these businesses and charities get targeted more often is because there is a bigger network of money coming in. For example Macmillan cancer support raised £239.7 million in 2024, and if they were to get breached that's £239.7 million that the hackers could steal and considerably more if they were to also target those who donated to Macmillan using their cards. To help prevent these breaches and better protect the public, there have been legislations put in place like the Data Protection Act 2018. The Data Protection Act 2018 entails making sure that companies or business are "processing personal data lawfully and fairly" (Legislation.gov, 2018).

Main body:

Fraud makes up about 'an estimated 41% of crimes in England and Wales' (NSA, 2025) so it is no doubt one of the UK's biggest issues. About 67% of fraud is also cyber enabled according to the National Strategic Assessment 2025 meaning that technology has helped enable over half of fraud in the UK. This can be seen through online shopping scams where a product would be advertised, and when a victim buys it, either the quality of the product they receive is well below what they paid, or the buyer simply does

not receive the item at all. The scammers would also have the victims payment details to possibly carry out further fraud. Online shopping scams make up about '26% of online fraud' (Citizens Advice, 2025). Another very popular method is the 'get rich quick' schemes, otherwise known as investment scams. These scams promise the victim a large amount of money but firstly they must make a small payment to kickstart it. Of course, nothing comes of it and once again the scammers run off with the money and possibly take even more from the victim resulting in many finding themselves in financial difficulty as '12% of victims of online fraud report that they fell into debt'. (Citizens Advice, 2025).

There are challenges when it comes to policing online fraud. The police simply do not have the right resources a lot of the time "...under resourced and lacking the skills required to deter and detect online fraudsters" (The Police Foundation, 2024). The methods used to commit fraud changes so quick, resulting in difficulties to create a plan that works for everything especially with the recent emergence of AI. The attitude towards policing it are also not on par as with online fraud. Even though it one of the biggest crimes in the UK, it is not treated as one with more physical crimes are being focused on, "Despite fraud making up over 40% of all crime in the UK, fraud has been under-prioritised for a decade." (The Police Foundation, 2024). The underreporting of fraud is another major issue the police face with policing fraud, "only 13% of cases get reported to Action Fraud or the police." (Watch Your Pocket, 2024). This could have an impact on how fraud is policed because not only is it underreported, it could also send the message that Fraud is not actually that big of a deal in the UK, therefore other cases get more focused on.

To respond to this the police and Government has developed legislations and plans to try and tackle fraud. The Police Foundation created a report about how the UK should tackle fraud as time and time again the 'national response to fraud does not match the scale of the threat' (The Police Foundation, 2024). In March 2025, Lord Hanson, the Fraud Minister, announced a new fraud strategy as part of the Government Plan for Change. This strategy will also focus on "tech-enabled fraud including emerging tech like AI" (Home Office, 2025). It would be great to try and

tackle AI especially when it comes to fraud as AI is a very fast-growing piece of technology that is already fooling people, and with the rapid development being seen with AI it will only be a matter of time before it will be virtually impossible to tell something is AI or not.

Emergence of AI can be a great threat to organisations and people, including police officers. Everything now is digitised and stored on some type of technology, and with the way police carry out their work, some of it such as body worn cameras and police phones would be stored in this way. Personal details of victims and criminals and even cases are also kept on a police database, so this can run the risk of getting hacked into and leaking this information (bring in case where a place got hacked where names were released). Although most scams are easy to detect, AI can have the ability to make them seem even more real than ever, especially with AI's ability to clone faces and even voices. "Widely reported cases of AI being used to perpetrate fraud and scams...included cases where voice clones appeared to have been used against an energy company" (PWC, 2023).

Attacks have already been seen on big UK companies such as the NHS where a cyber-attack in 2024 attained patient data and leaked 400 gigabytes of the stolen data. "A sample of the stolen data seen by the BBC included names, dates of birth, NHS numbers and descriptions of blood tests. (BBC, 2024). If these attackers targeted a national health service, it would not be far out to assume that they could try to hack police systems to try and gain information or to try and threaten for money, except it has actually happened. In the September of 2023, there was a cyber-attack on Greater Manchester police where "identity badges and warrant cards including names, photos and identity numbers" (Security Week, 2023). The breach in data happened due to the identity card company that the Greater Manchester police used, being hacked. The police experienced another cyber-attack where identities were revealed just a month before, showing that it is possible to hack into the secure police systems and with AI could help make that easier for hackers.

Another newer act that the government has implemented is the Online Safety Act 2023. "The Act requires all companies to take robust action

against illegal content and activity (including fraud).” (Department of Science, Innovation and Technology, 2025). Although this Act was quite controversial to the UK public, the main focus was to assure that platforms that are allowed in the UK have a duty that the content they have on their platforms cannot harm its users in anyway. This a step in the right direction and may have even directly impacted with lowering the numbers of online fraud and its victims.

Even though the focus on the tackling of fraud has not been the best in the UK, there still has been crackdowns on it. One example of this would be Operation Falcon. This operation was carried out by London Metropolitan police, with the aim of tackling cyber-crime and fraud in London. They managed to make “significant disruptions of cyber-criminal activities and make arrests of high-profile hackers and fraudsters” (Government Events, 2024). They managed to execute this through using cyber threat intelligence and digital forensics to help identify the criminals, showing that there is a need for these tools when it comes to taking down cyber-crimes such as online fraud.

Operation Henhouse is another more recent operation that the police used to crack down on fraud. It involved multiple police services around the UK plus other agencies like the financial conduct Authority, the National Crime Agency and National Trading Standards. The operation managed to arrest 433 individuals and take back over eleven million pounds from these fraudsters and “disrupt the highest harm of organised crime groups who use technology to launch frauds on an industrial scale.” (National Crime Agency, 2025).

Comparing the two operations above, it can be seen that the best way to tackle fraud and online fraud is by working together with other agencies with different specialties as the police simply do not have the correct resources to deal with the issues, at least not head on like these two operations. Tackling fraud should be done more often, as it is the highest reported crime in the UK and will only grow with the development of technology and especially AI which is becoming more and more realistic by the day. Whilst Operation Falcon was highly successful, it was not on the scale Operation Henhouse was which, given the resources and agencies

involved, is the best way to tackle fraud. This was not only due to the sheer number of arrests and money returned, but also the message it gives out to potential fraudsters.

Conclusion 300:

To conclude, it can be seen that fraud and online fraud makes up over 40% of the UK's total crime. Due to this the Government and police have had to find ways to tackle this through Acts like the Online Safety Act 2023 and operations like Operation Falcon. Although operation Falcon was successful, it is obvious that the Government needs to focus more on fraud if it is seen as the highest performed crime in the UK. It can also be seen that it can be very hard to police due to limited resources and limited reporting by the public.

The risks of carrying personal technological items when working within the police and storing sensitive information in a cloud based system or on technological devices was also looked into and reviewing what dangers and issues could occur due to the possibility of being hacked, which has happened to the police before where their identities got leaked due to a cyber-attack. Overall, the takeaway is that the government and police need to do more when it comes to fraud as it will only be a problem that will get bigger if not policed efficiently.

References:

BBC 2024, *NHS England confirm patient data stolen in cyber attack*, available at: [NHS England confirm patient data stolen in cyber attack - BBC News](#) (accessed on 06/11/2025).

Citizens Advice 2025, *Millions stung by scams with online shopping the top trap, says Citizens Advice*, available at: [Millions stung by scams with online shopping the top trap, says Citizens Advice - Citizens Advice](#) (accessed on 05/11/2025).

Department of Science, Innovation & Technology 2025, available at: [Cyber security breaches survey 2025 - GOV.UK](#) (accessed on 21/10/2025).

Department for Science, Innovation & Technology 2025, *Online Safety Act: explainer*, available at: [Online Safety Act: explainer - GOV.UK](#) (accessed on 06/11/2025).

Government Events 2024, *How Six Police Forces Are Tackling Technology-Driven Crimes*, available at: [How Six Police Forces Are Tackling Technology-Driven Crimes • Government Events](#) (accessed on 06/11/2025).

HMICFRS 2023, *Fraud: Time to Choose- An inspection of the police response to fraud*, available at: [Fraud: Time to Choose - An inspection of the police response to fraud - His Majesty's Inspectorate of Constabulary and Fire & Rescue Services](#) (accessed on 06/11/2025).

Home Office 2025, *Lord Hanson unveils ambitious new approach to tackling fraud*, available at: [Lord Hanson unveils ambitious new approach to tackling fraud - GOV.UK](#) (accessed 06/11/2025).

Legislation.gov 2018, *Data Protection Act 2018*, available at: [Data Protection Act 2018](#) (accessed 03/11/2025).

Macmillan Cancer Support 2024, *Our annual reports*, available at: [Our annual reports | Macmillan Cancer Support](#) (accessed on 31/10/2025).

National Crime Agency 2025, *Fraud*, available at: [NSA 2025 - Fraud - National Crime Agency](#) (accessed on 05/11/2025).

National Crime Agency 2025, *Operation Henhouse: 433 arrests and £7.5m seized in national crackdown on fraud*, available at: [Operation Henhouse: 433 arrests and £7.5m seized in national crackdown on fraud - National Crime Agency](#) (accessed on 06/11/2025).

PWC 2023, *Impact of Artificial Intelligence on Fraud and Scams*, available at: [Impact of Artificial Intelligence on Fraud and Scams](#) (accessed on 06/11/2025).

TwentyFour 2025, *UK Cybercrime Statistics 2025*, available at: [UK Cybercrime Statistics 2025 | Online Security | TwentyFour](#) (accessed on 31/10/2025).

Security week 2023, *A Second Major British Police Force Suffers a Cyberattack in Less Than a Month*, available at: [A Second Major British Police Force Suffers a Cyberattack in Less Than a Month - SecurityWeek](#) (accessed on 06/11/2025).

The Police Foundation 2024, *Turning the tide: A plan to tackle online fraud*, available at: [NEW REPORT: Turning the tide: A plan to tackle online fraud - The Police Foundation](#) (accessed on 06/11/2025).

The Police Foundation 2024, *Turning the tide: A plan to tackle online fraud*, available at: [NEW REPORT: Turning the tide: A plan to tackle online fraud - The Police Foundation](#) (accessed on 06/11/2025).

Watch Your Pocket 2024, *The underreporting of fraud cases in the UK*, available at: [The underreporting of fraud cases in the UK - Watch Your Pocket](#) (accessed on 06/11/2025).