



**Objectives: By the end of this lesson you will be able to:**

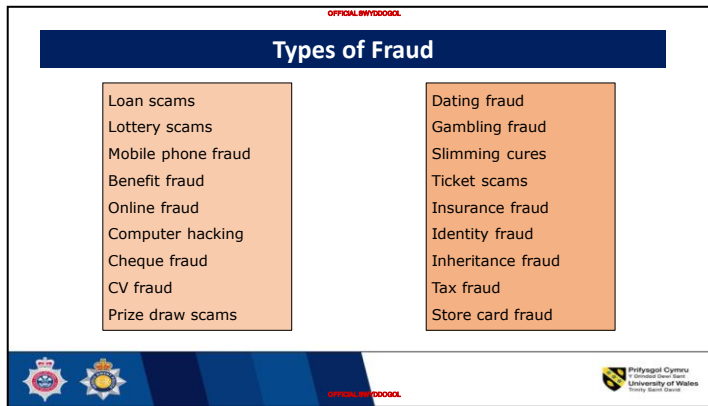
1. **Identify** the legislation relating to Fraud offences. (Secs, 2,3,4,6,11 and Making off without Payment – Sec 3 Theft Act 1978)
2. **Describe** the impact of Fraud on (vulnerable and non-vulnerable) victims
3. **Explain** how the police deal with initial reports of Fraud
4. **Apply** legislation covered in the lesson to complete scenarios.

**QTS - What is Fraud?**

**Fraud is when trickery is used to gain a dishonest advantage, which is often financial, over another person.**

There are many words used to describe fraud: Scam, con, swindle, extortion, sham, double-cross, hoax, cheat, ploy, ruse, hoodwink, confidence trick. These are just a few words you might hear in relation to fraud.

Fraud can be committed against individuals or businesses



Prior to showing PPT slide 2...

**QTS – can you give me examples of different types of fraud?**

Trainer to board blast the answers then compare to the PPT slide

It is recognised across policing and government that fraud is a significant threat to the UK economy and policing is struggling to keep pace with the increasing demand and complexity of fraud in a digital age which is not restricted by geographic or other boundaries. Fraud includes low value and localised offending as well as complex and organised fraud. Fraud can be carried out remotely with perpetrators targeting UK citizens and businesses from abroad. Victims, offenders and enablers can be based across multiple force areas and

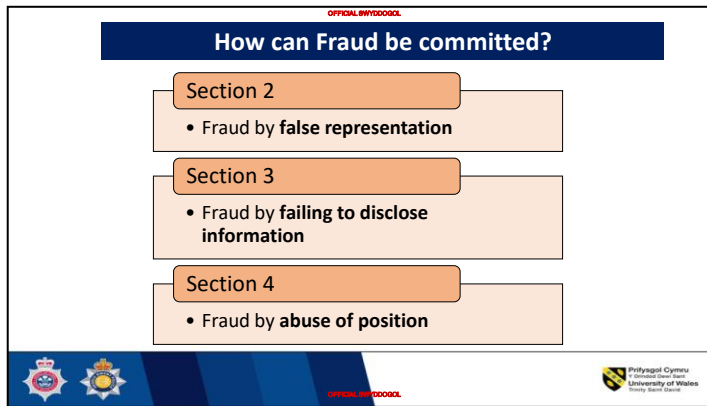
international jurisdictions.

Anyone can become a victim of fraud – individuals, SMEs, large corporates, charities and public sector organisations. Fraudsters deliberately target some of the most vulnerable in our society. They repeatedly target victims, sharing details of the susceptible and vulnerable across criminal networks.

The financial loss from fraud can be life changing for victims. Fraudsters do not only take victims' money, they take their sense of security, confidence and well-being. Victims suffer financial hardship, anxiety, depression and other mental and physical health problems. This has led to victims feeling suicidal and taking their own lives. Fraud losses put small businesses at risk, jeopardising the livelihood of proprietors and their employees.

Technology has enabled new ways to defraud people, E.g. complex software such as keylogging viruses are designed to record computer use and capture personal information, like bank account passwords, which are secretly sent to a host computer and can then be sold on for profit, or social phishing, where the online offender gains access to an individual's social media account and then accesses their 'friends' list.

'Traditional' frauds can also be enabled online. Many people experience buying goods online, such as tickets for events, that turned out not to be genuine, or goods that then didn't arrive. More elaborate and lengthy frauds can be committed involving romance and investment scams online, where victims being met via online dating sites.



Section 1 of the Fraud Act 2006 states that the offence of Fraud can be committed in 3 distinctive ways.

- a. By false representation e.g. returning stolen goods to a shop to try and obtain a refund
- b. By failing to disclose information e.g. omitting important information when applying for a job or health insurance
- c. Through abuse of position e.g. whilst driving a local authority minibus, demanding fares from local residents when the service is actually free.

For all of these offences the intent remains the same:

- to make a gain for himself or another
- To cause a loss to another
- Or to expose another to risk of loss

The gain or loss can be temporary or permanent and can involve personal property, real property, intangible property or things in action. (Similar to the Theft Act)

Dishonesty - Subsection (1)(a) makes it clear that the representation must be made dishonestly. This test also applies to [section 3](#) and [section 4](#). The current definition of dishonestly was established in [R v Ghosh \[1982\] Q.B. 1053](#).



OFFICIAL #WYDGOGL

## Fraud Act (2006): Section 3

A person is in breach of this section if they:

**Dishonestly** fail to disclose to another information which he is under a legal duty to disclose and **intend** by failing to disclose the information to make a gain for himself or another, or cause loss to another or to expose another to risk of loss.

OFFICIAL #WYDGOGL

Prifysgol Cymru  
Prifysgol Deu Fawr  
University of Wales  
Trinity Saint David

### Fraud by failing to disclose information

Failure to disclose can be made by oral or written omission.

The legal duty to disclose comes from:

- Statute e.g. a company must publish the yearly accounts under company law but fails to do so
- Good faith e.g. disclosing serious illness to reduce health care premiums
- Terms of contract e.g. estate agent not revealing all bids for a property to a client

OFFICIAL #WYD200GL

## Fraud Act (2006): Section 4

A person is in breach of this section if:

He occupies a position in which he is expected to safeguard, or not act against, the financial interests of another person **and** dishonestly abuses that position and intends to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss.

OFFICIAL #WYD200GL

Prifysgol Cymru  
University of Wales  
Trinity Saint David

### Fraud by Abuse of Position

The offence could apply to anyone who has knowledge of someone's financial affairs such as an employer or trustee.

Abuse is not defined in law but is held to have a normal everyday meaning. It can be an act or a failure to act

e.g. a person who has access to the bank account of a vulnerable relative and takes money for their own use, or where house mates pool money to pay bills and one of them is entrusted to pay the bills but instead uses the money to go on holiday.

OFFICIAL #WYDGOGL

## Fraud Act (2006): Section 6

A person is guilty of the offence if he has in his **possession** or under his **control** any article for use in the **course** of or in **connection** with any fraud.

OFFICIAL #WYDGOGL

Prifysgol Cymru  
Prifysgol Deu Fawr  
University of Wales  
Trinity Saint David

This offence is similar to the offence of going equipped.

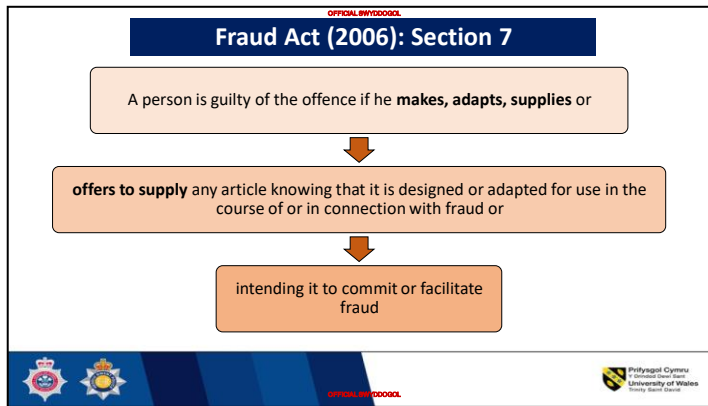
The articles can include clothing to imitate company representatives, mechanisms to slow down electricity meters, as well as false identity cards, credit cards, cheque books, till receipts passports and driving licences. It may also include a computer programme or data held in an electronic form.

Section 6 covers possession or having the article under his control.

**Possession** – the person must have immediate physical control over the article and know that it is there.

**Control** – includes having physical control at a distance e.g. possess a key to a cupboard where the item is kept and knowing the article was there

This offence can be committed anywhere, including when the items are located within a suspects home.



Section 7 of the Fraud Act 2006 makes it an offence to make, adapt, supply or offer to supply any article knowing that it is designed or adapted for use in the course of or in connection with fraud, or intending it to be used to commit or facilitate fraud.

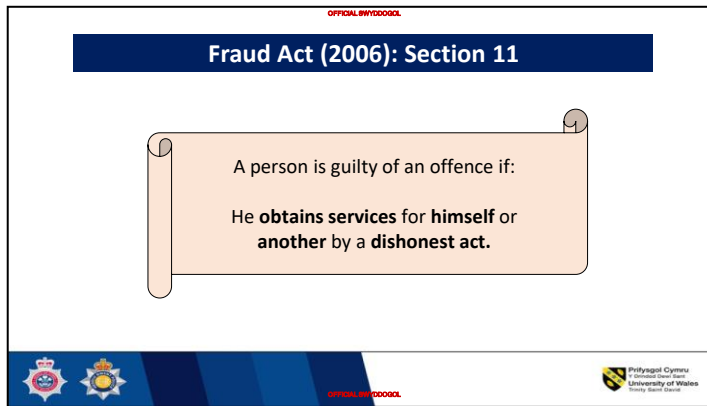
#### Note

*For example, a person makes devices which when attached to electricity meters cause the meter to malfunction. The actual amount of electricity used is concealed from the provider, who thus makes a loss.*

Either way

Summary: maximum 6 months imprisonment and/or fine

Indictment: maximum 10 years imprisonment and/or fine



In the previous sections of Fraud the gain or loss has been related to property of a tangible and intangible nature.

**Section 11** is an additional offence for when a service is obtained by dishonest means. If services have been provided e.g. a taxi ride where there is no gain or loss of property

This service must be a type for which payment is required and could include bus rides, haircuts and a stay in a hotel room. The service must be obtained through a dishonest act and this would include using a false credit card, giving false personal details and making false promises or agreements. The services are made available on the basis that payment either **has** been made **is** being made or **will** be made

The services are obtained without either any payment being made or payment being made in full. When they obtained the services they knew the basis upon which the services were made available (i.e. that they were expected to pay)

They **intend** either **not** to make **any payment** or **not** to make **payment in full**.

The person must know that the services are made available on the basis that they are chargeable, or that they might be and it can be committed only where the dishonest act was done with the intent not to pay for the services as expected. The offence requires the actual obtaining of the service.

### Examples:

Data or software may be made available on the Internet to a certain category of person who has paid for access rights to that service. A person dishonestly using false credit card details or other false personal information to obtain the service would be committing an offence under this section.

The offence would also cover a situation where:

- a person climbs over a wall and watches a football match without paying the entrance fee - such a person is not deceiving the provider of the service directly,

but is obtaining a service which is provided on the basis that people will pay for it.

- a person attaches a decoder to their television to enable viewing access to cable/satellite television channels for which they have no intention of paying.

OFFICIAL #WYDGOGL

**Making Off without Payment**

A person who **knowing** that **payment on the spot** is required for any **goods** supplied or **services** done is expected from him **dishonestly** makes off without having paid as required or expected with **intent** to avoid payment of the amount due shall be guilty of an offence.

Section 3 Theft Act 1978




OFFICIAL #WYDGOGL

If no dishonest representation takes place and a person had every intention to pay for the goods before the property was obtained, but then makes off without paying, the above offence has been committed.

This offence is sometimes referred to as “Bilking”

**E.g.** A person fills their car with petrol, but upon seeing the staff engaged with other customers, decides to leave and drive off without paying.

This offence only applies if “payment on the spot” is the norm in that particular situation, such as collecting goods when work has been done (shoe repairs) or paying when a service has been done (haircut).

**Good supplied or services done** - The goods or services must be lawful. It does not apply to goods or services which are not legally enforceable. E.g. non-payment of a gambling debt is not an offence under these provisions and you cannot make off from a prostitute.

It includes allowing a motorist to fill his tank at a self-service petrol station, which was one of the main areas of offending for which this provision was created.

The provision of overnight hotel accommodation for which a charge is levied is also covered by this offence.

**Intent to avoid payment** – this can be proved either by an admission of guilt from the suspect or by inference or a combination of both - (eg how far they were found from the petrol station but a motorist who forgets to pay for petrol, but then remembers and goes back to pay, would not commit this offence).

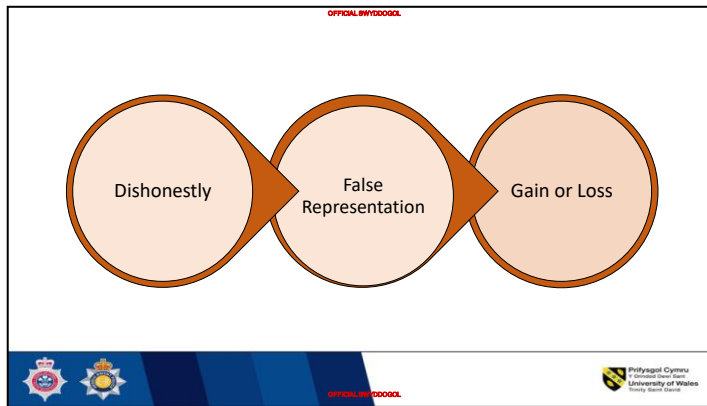
It must be proved that suspect knew payment was required on the spot and it also must be proved that they intended to avoid payment

**Making off** - Involves dishonestly leaving the place (or spot) where payment is required. It has been held to be 'passing the point where payment is required', such as a cash desk, but it can be interpreted more widely than that, depending on the circumstances. It can be likened to a 'dishonest departure'.

The dishonest element of this offence refers specifically to the offender making off

dishonestly, not to his conning the victim into thinking the money will be paid later. In such circumstances this offence is not committed and the Fraud act 2006 should be considered.

(ii) **Payment on the spot** - It is important that the person knows (by whatever means) that he is required or expected to pay at the time. It can just be commonly accepted practice, such as paying for a meal at a restaurant after it has been eaten.



The term **Dishonestly** is not defined in the Act, but in case law it has been held to relate to the test of whether the dishonesty would challenge the standards of a reasonable and honest person. The current definition of dishonesty was established in **R v Ghosh 1982**. This also applies to Section 3 and Section 4.

**Note:**

Where a person is charged with dishonesty the jury must decide as to his guilt in the following manner –

1. Whether, according to the ordinary standards of reasonable and honest people, what was done was dishonest. If it was not, then that was the end of the matter
2. However, if it was dishonest by those standards, then the jury must decide whether the person realised that what he was doing was by those

*The case of [Ivey v Genting Casinos \(UK\) Ltd \(trading as Crockfords\) 2017](#), has held that the test for dishonesty should be objective and has **partly overruled the test outlined in Ghosh (above)**. It was held that the subjective element of the test for dishonesty in Ghosh did not correctly represent the law and as such, directions based upon it ought no longer to be given. The principal objection to the second leg of the rule was that the less the defendant's standards conformed to what society in general expected, the less likely he was to be held criminally responsible for his behaviour.*

A **representation** is false if:

- it is **untrue** or **misleading** and
- the person making it **knows** that it **is** or **might be** either **untrue** or **misleading**.

**Representation** means any representation as to fact or law, including a representation as to the state of mind of -

- a. the person making the representation, or
- b. any other person.

A representation may be **express** or **implied** and can be communicated in words or in conduct.

- The person must make the representation with the intention of making a gain or causing loss or risk of loss to another. The gain or loss does not actually have to take place.
- There is no limitation on the way in which the words must be expressed. They could be written or spoken or posted on a website.

### Example:

1. An example of a **representation by conduct** is where a person dishonestly misuses a credit card to pay for items. By tendering the card, they are falsely representing that they have the authority to use it for that transaction. If they know that they do not, or might not, have that authority, then they are committing an offence under this section. It is immaterial whether the cashier accepting the card for payment is deceived by the representation.
- This offence would also be committed by someone who engages in '**phishing**', i.e. where a person disseminates an email to large groups of people falsely representing that the email has been sent by a legitimate financial institution. The email prompts the reader to provide information such as credit card and bank account numbers so that the 'phisher' can gain access to others' personal financial information.
2. A further example covered by this section is where a person sell goods claiming that they are genuine 'designer' items, but knows this might be untrue.

A representation may be also be regarded as being made if it is submitted in any form to any system or device designed to receive, convey or respond to a communications (with or without human intervention).

The main purpose of this provision is to ensure that fraud can be committed where a person makes a representation to a machine and a response can be produced without any need for human involvement such as where a person enters a number into a 'CHIP and PIN' machine.

3. Another example would be if with coin operated dispensers where foreign coins or objects are used to get the contents from the machine **or** it can be misleading by assuming the identity of a charity worker and shaking a stolen collection tin in public.

Any representation must be one of fact or law, so a broken promise is not in itself a false representation. However, a statement may be false if it misrepresents the current intentions or state of mind of the person making it or anyone else.

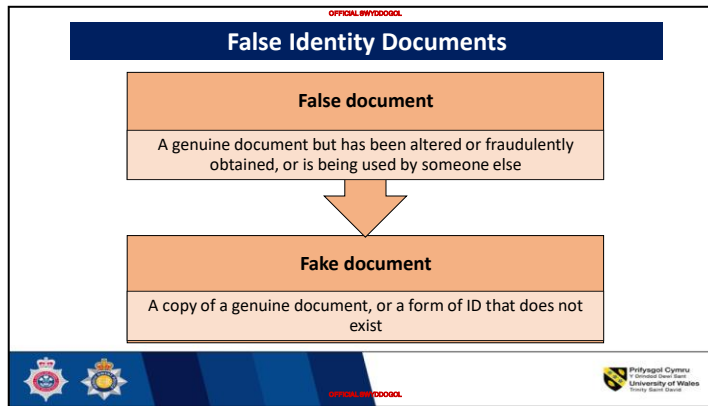
**Example:** D visits V's house and tells V that he (V) needs emergency work carried out on his roof. D states that he is in a position to do the work immediately but only if he pays V £1000 there and then. V gives D the money and then D leaves without

carrying out the work. The truth of the matter being that D never intended to carry out the work. Such a 'promise' by D would amount to false representation as he never intended to keep his promise.

The offence is complete the moment the representation is made.

### **Gain or Loss**

Recent case law makes it clear that the suspect **must intend** that the false representation will cause the gain or loss.



Since the Licensing Act 2003 introduced a requirement for an age verification police for all licensed premises, some young people have resorted to using ID documents from older members of their family or friends or obtain fake ID from the internet., in order to purchase alcohol.

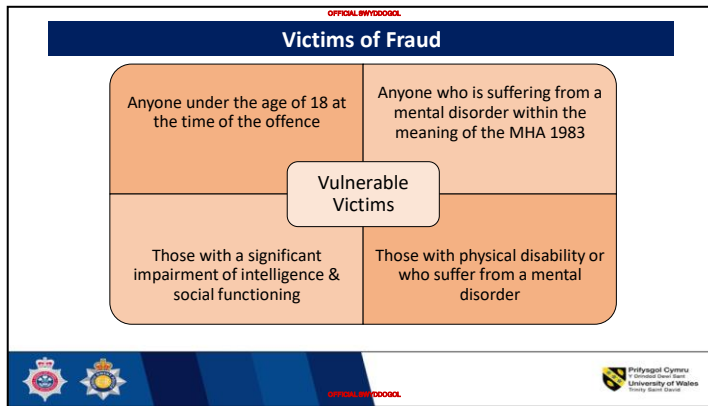
A document is **false** when it is a genuine document but has been altered or fraudulently obtained, or is being used by someone else.

A **fake** document is a copy of a genuine document, or a form of ID that does not exist

There are five types of false document:

- Genuine document which is being used by someone else,
- Genuine document which has been altered,
- Genuine document which has been fraudulently obtained,
- Fake document which is a copy of a genuine document, and
- Fake document which is a form of ID that does not exist.





## QTS – Can you now identify who victims of fraud are likely to be?

Trainer to debrief and highlight that **Vulnerable** victims are susceptible to Fraud.

The Victims' Code also makes an enhanced service available to vulnerable victims. Under the code, a vulnerable victim is classified as:

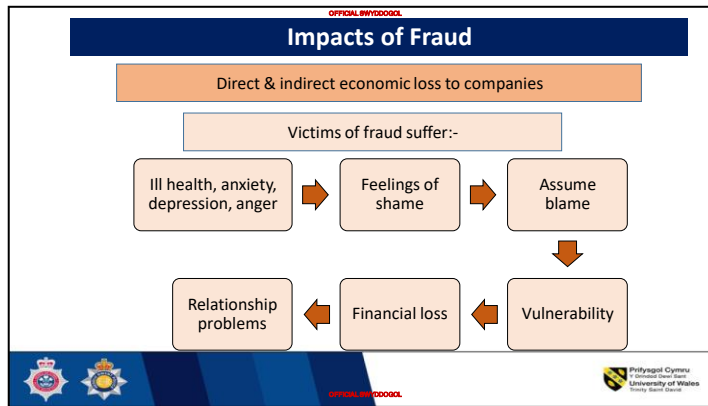
Anyone under the age of 18 at the time of the offence.

Anyone who is suffering from a mental disorder within the meaning of the Mental Health Act 1983.

Those with a significant impairment of intelligence and social functioning.

Those with a physical disability or who suffer from a mental disorder.

Victim Support offers support to victims of Fraud.



Trainer to put students into small groups/pairs to discuss short and long term effects of the impact of fraud on victims. Trainer to debrief using PPT slide and notes.

### Lasting Impacts of Fraud

- Direct and indirect economic loss to companies (financial loss and reputational loss)
- Loss of business
- Companies become more vulnerable due to the weaknesses in their systems and processes
- Loss of jobs/redundant

### Long term & Short term Impacts on Victims

- **Ill health** – Emotional and psychological effects, as they are susceptible to stress due to financial problems.
- A fraud victim may **feel embarrassed** because of a change in social status.
- Victims suffer a loss of a sense of security, self esteem and dignity which make take years to overcome
- Victims may feel panicked, angry, afraid, anxious and ashamed
- Victims may **assume blame** after the offence has been committed
- Victims feel **vulnerable**, and depressed in the most extreme circumstances suicidal as a result of the fraud they have experienced
- **Financial Loss** - many victims find it difficult to recover from financial loss following identity theft.
- It may cause **relationship problems** and prevent a victim from providing adequate support for their dependants.
- Victims of Fraud may find it difficult to be able to trust others

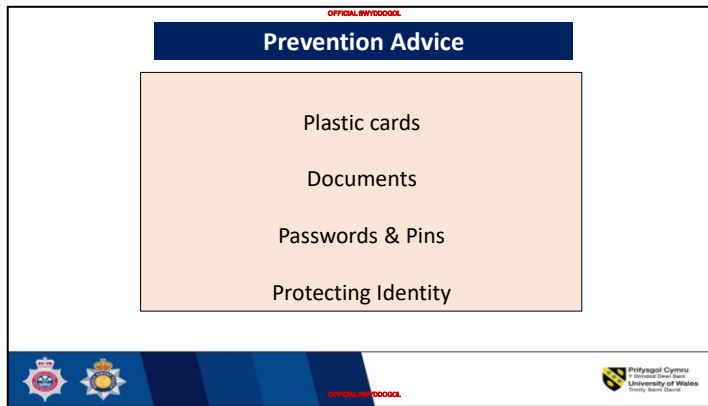


Eliminate risk of digital contamination by officer keeping notes in PNB of any actions taken at the scene i.e. turning the computer off.

Liaise with force digital forensic services – request to attend the scene

Authorisation is required under RIPA 2000 to inspect the data on the devices

2012 ACPO Good Practice Guide for Digital Evidence refers



## **Plastic cards**

If your plastic cards are lost or stolen, cancel them immediately. Keep a note of the emergency numbers you should call.

When giving your card details or personal information over the phone, internet or in a shop, make sure other people cannot hear or see your personal information.

## **Documents**

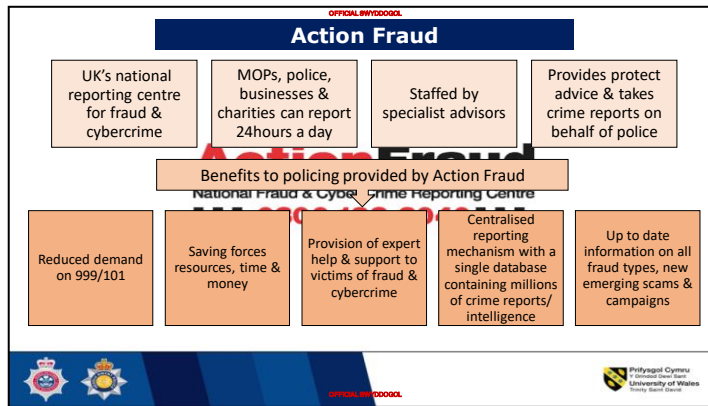
Keep your personal documents in a safe place, preferably in a lockable drawer or cabinet at home. Consider storing valuable financial documents such as share certificates with your bank.

Don't throw away entire bills, receipts, credit-or debit-card slips, bank statements or even unwanted post in your name. Destroy unwanted documents, preferably by using a shredder.

## **Passwords and PINs**

Never give personal or account details to anyone who contacts you unexpectedly. Be suspicious even if they claim to be from your bank or the police.

Don't use the same password for more than one account and never use banking passwords for any other websites. Using different passwords increases security and makes it less likely that someone could access any other accounts.



## Action Fraud

Action Fraud is the UK's (England, Wales and Northern Ireland) national reporting centre for fraud and cybercrime. Members of the public, the police, businesses and charities can report to Action Fraud online 24 hours a day or on the telephone. The Action Fraud call centre is staffed by advisors who receive specialist training in fraud and cybercrime. Action Fraud provides protect advice and takes crime reports on behalf of the police. Since its inception, it has taken millions of reports from victims, UK law enforcement and businesses.

The benefits to policing provided by Action Fraud:-

- Reduction of demand on 999 and 101
- Saving forces time, resources and money
- Provision of expert help and support to victims of fraud and cyber crime
- A centralised way of reporting with a database that contains millions of high quality intelligence and

- crime reports relating to fraud and cybercrime.
- Provision of up to date information on all fraud types, new emerging scams and campaigns

The National Fraud and Cyber Crime Reporting Centre (NFRC) is comprised of Action Fraud and the National Fraud Intelligence Bureau (NFIB). The service is hosted by the City of London Police (national policing lead for Economic Crime). The NFIB analyses reports of fraud and cybercrime made to Action Fraud, identifying lines of enquiry and where there are lines of enquiry available, allocating cases to police forces for investigation. **NRFC does not have an investigative function.**

Action Fraud will only record fraud and Cybercrime. Where other notifiable offences are reported, the victim will be referred to the Police, for example; Blackmail, theft etc. Similarly, Action Fraud does not record Possession of articles for use in Fraud or Proceeds of Crime Act offences which will all be recorded on local police crime systems.

When a report is made to Action Fraud, a NFRC number is provided to the reporter; this is the crime number.

The Home Office use these NFIB recorded fraud and cybercrimes to analyse national figures, ascertain the

demand on Police by Force area and the result of that demand. i.e. outcomes.

Typically, there are no geographical boundaries for organised fraud. Offenders could be targeting fraud victims from overseas and are commonly outside of the jurisdiction of UK law enforcement and legislation. Even if there were greater judicial powers to bring overseas offenders to justice, the practicalities of investigating such offences would typically make them disproportionate to tackle.

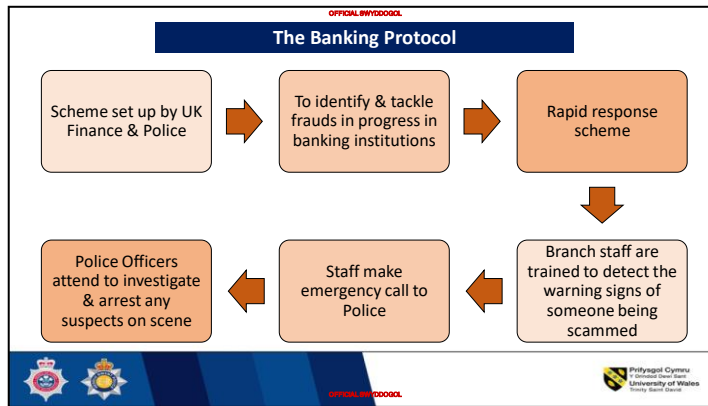
With these factors in mind, emphasis is placed on investigating the cases where offenders are based in the UK and can be effectively brought to justice. With overseas offending, the emphasis is on intelligence sharing with law enforcement agencies in their countries via the NFIB, disruption (for example taking down email headers and domains used by fraudsters), whilst also focussing on the prevention of fraud and protecting vulnerable people from repeat victimisation.

South Wales & Gwent Police receives reports of fraud from a number of different sources:-

1. Direct reports to police
2. NFIB Pursue disseminations

### 3. NFIB Protect disseminations

Reports made to Action Fraud



## The Banking Protocol

The Banking Protocol is a scheme set up by UK Finance and the Police to identify and tackle frauds in progress in banking institutions. Under this rapid response scheme, branch staff are trained to detect the warning signs that someone is being scammed and to make an emergency call to the Police. Police officers will then visit the branch to investigate the suspected fraud and arrest any suspects still on the scene.

The scheme has prevented £142 million of fraud since it was launched in 2016 (figures published 01/03/2021). This close collaborative work between the Police and branch staff led to the arrest of 200 suspected criminals during 2020, a total of 843 arrests since the scheme began. The criminals arrested included rogue traders that demanded cash for unnecessary work on people's property and individuals that persuaded their victims to take out large sums of cash to hand it over to someone posing as a courier. Others impersonated the Police, government or banks, or created fake dating profiles in an attempt to steal personal and financial information

from innocent victims to commit fraud.

## **NFIB Pursue disseminations**

The NFIB disseminates packages to Police forces with a verifiable rationale for further investigation.

This Pursue dissemination will be sent in accordance with the five principles detailed in the HOCR (Home Office Counting Rules)

The HOCR for fraud:-

- 1st - Police force covering the location of the fraudulent operation/suspect's address. For business related fraud, the offence address of the employee. If there is no office address, the head office of the company (\*\* this results in many investigations being sent to forces where the suspect resides, and not where the victim lives \*\*)
- 2nd - The police force area with the greatest number of individual usages or offences
- 3rd - The police force area where the first offence was committed
- 4th - the police force area where the victim resides or works.
- 5<sup>th</sup> - NFIB determined force area

Each NFIB dissemination is received via a 'vault' and will

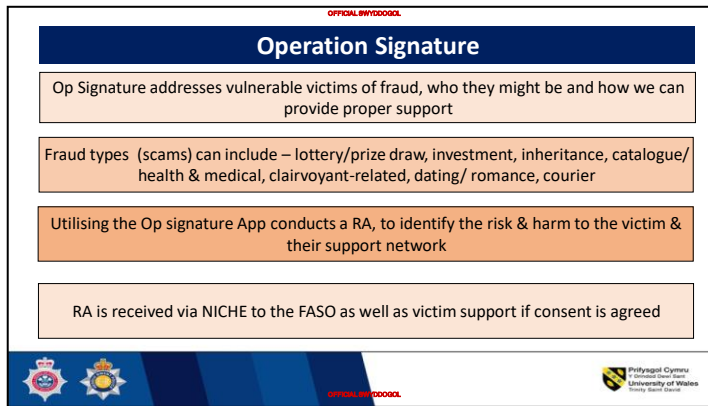
be assessed by the Action Fraud SPOC in the Economic Crime Unit. The Fraud SPOC will ensure that the report is logged on NICHE and adhere to force allocation policy when allocating for further investigation.



or works.

- 5<sup>th</sup> - NFIB determined force area

Each NFIB dissemination is received via a 'vault' and will be assessed by the Action Fraud SPOC in the Economic Crime Unit. The Fraud SPOC will ensure that the report is logged on NICHE and adhere to force allocation policy when allocating for further investigation.



**QTS** – has anyone ever heard of Operation Signature?

## Operation Signature

Operation Signature addresses vulnerable victims of fraud; thinking about which members of our community are likely to fall victim to a fraud; and thinking about how we provide them with proper support.

The types of fraud Operation Signature is concerned with can take many forms.

The Fraud types can include: -

- Lottery/prize draw scams
- Investment scams
- Inheritance scams
- Catalogue/health and medical scams
- Clairvoyant-related scams
- Dating/romance scams

- Courier scams

When reporting officers utilise the Operation Signature App, it asks the officer / PCSO to complete certain information about the scam or fraud that has been experienced by the vulnerable victim.

The aim of the questions conducted a risk assessment, to identify the risk and harm of the victim becoming a repeat victim and being targeted again.

The assessment looks at the support network the victim has in place highlighting whether additional support is required.

The risk assessment is received via Niche to the FASOs as well as victim support if consent is agreed to share the information. The FASO's will look further into the fraud and the vulnerability of the victim and visit the victim within their own home to assist with putting preventative measures in place.

For SWP - You can additionally create an Operation Signature report via BOB and the details are mostly similar to that of a PPN. If in addition to the report, the victim consents to the sharing of information to Social Services, then a PPN will also be required. Additionally, there are occasions when other agencies can also be contacted and should be done so, i.e. Trading Standards Age Concern, Victim Support to name a few. If required,

please liaise with the FASOs to obtain the relevant contact details.



## vulnerability

- Assist the victim in furthering any complaint to the Banks and Financial Ombudsman

In addition to the above, the following duties may be considered: -

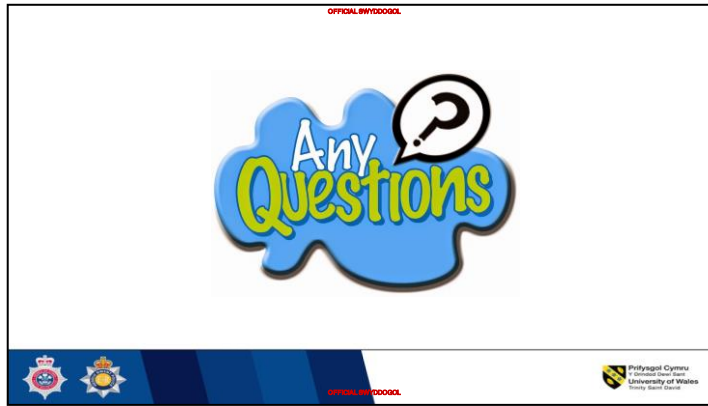
- To reduce the overall impact from offences related to Fraud.
- To prepare and convey presentations in front of live audiences to share experience or advice/guidance, as appropriate.
- To work with partners; for example Trading Standards, Age Concern and Local Government to prevent offending through training, advice and guidance.
- Provide support to colleagues by receiving and progressing safeguarding enquiries borne out of Fraud investigations.
- If required, to contribute/attend safeguarding meetings, representing ECCU and providing investigation updates and advice.

For most frontline staff and supervisors, the FASOs are the first port of call when dealing with vulnerable victims of Fraud. They should be contacted, or their

supervisor (DS 4998 Andrew Westlake) in order to discuss best options of quick time asset preservation (to stop money from being sent from MULE accounts) and support and advice for the investigation, particularly when the suspect resides out of the force area and would need to be “Transcrimed”, which is the name of the process of sending a Fraud to another Police force.

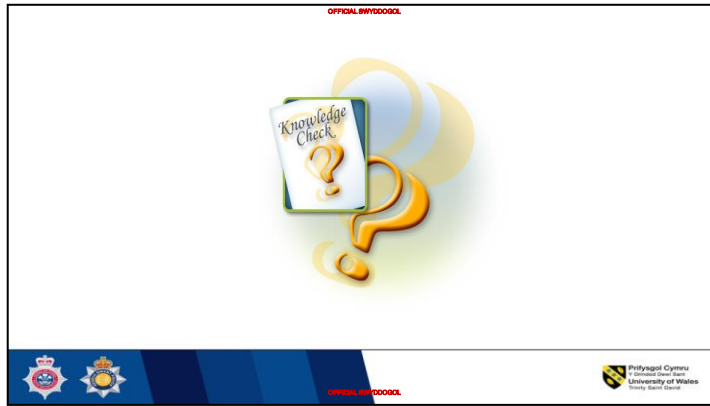
\*\*\*\*FAO Gwent Trainers\*\*\*\*

Anyone seeking Fraud/safeguarding support from GWP contacts the Fraud Triage team online or via [fraudtriage@gwent.police.uk](mailto:fraudtriage@gwent.police.uk)



Trainer to re-visit objectives.

Any questions?



Trainer to put students in pairs and hand out Knowledge Check.

Students have 10 minutes to complete the questions.

After 10 minutes, trainer to de-brief.