Fraud

Historic Fraud Offences

In January 2007 the Fraud Act 2006 became law and repealed much of the previous fraud legislation. Whilst it is not possible to prosecute offenders under the new legislation for offences committed before the new act became law, the Home Office require the National Fraud Intelligence Bureau via Report Fraud to record fraud for statistical purposes, under the new legislation.

Report Fraud

Report Fraud is the name of the contact centre that records NFIB fraud and some cyber-enabled and cyber-dependent crimes such as Computer Misuse Act offences like hacking (Cyber Crime). Report Fraud does this through its' contact centre and on-line reporting tool. The NFIB codes used in this section are used by Report Fraud to enable them to record specific fraud/cyber crime types reported to them that are then passed to the NFIB. These codes are also used to count fraud/cyber types passed to the NFIB in bulk data transfers from other data providers working in partnership with the NFIB, such as those in the banking and credit industry. All confirmed fraud/cyber crimes held within the NFIB database will use the NFIB codes.

Report Fraud can only record NFIB fraud and cyber crimes. Where other notifiable offences are apparent the victim will be referred to the police. Likewise, non-NFIB recorded frauds and cyber enabled offences remain the responsibility of the police to record (i.e Other Fraud and Forgery or blackmail offences committed through social media/chatrooms etc).

The National Fraud Intelligence Bureau (NFIB)

The Home Office will obtain levels for NFIB Recorded Fraud and Cyber offences from the NFIB. This will consist of:

1 The national total level of NFIB recorded fraud/cyber crime. (i.e it will not broken down by Police Force area).
2 The demand on police by Force area, and
3 The result on that demand (i.e Outcomes).

The '**demand on police'** is

Offences that meet the call for service criteria (See Fraud page 1 of 7) and
Offences passed to the Force by the NFIB for law enforcement.

Fraud
(Page 1 of 7)

General Principles

With the exception of crimes meeting the 'call for service criteria' (see below) it is anticipated that the majority of NFIB crimes will be recorded at the NFIB directly by data providers and by victims using the 'Report Fraud' on-line reporting tool or the AF contact centre.

Where victims contact police to report a fraud, police may, unless a police CALL FOR SERVICE exists (**important see below**), advise the victim that they can report fraud to Report Fraud directly via the contact centre by telephone or on-line reporting tool. If this advice is taken, then there is no need for police to record a crime or record a CRI. Where victims decline this facility and ask police to record a fraud, then police should take full details of the fraud and pass the details to NFIB. This will usually be by inputting the report direct to AF via on-line reporting. It is recognised that some forces may continue to record allegations of fraud/cyber in their local crime recording systems. Regardless of local record being raised the force must also report the crime to AF using on-line reporting.

Police recording of NFIB Crime

Police must create local case management records for NFIB recorded fraud/cyber crime, for the following:

- Crimes which meet the call for service criteria,
- Crimes passed to them by the NFIB.

Calls for Service

Police will create a case management record for all the following fraud/cyber offences when:

- Offenders are arrested by police or
- There is a call for service to the police and the offender is committing or has recently committed at the time of the call for service or
- There is a local suspect (see page 2 of 7).

Fraud
(Page 2 of 7)

Local Suspect

'Local suspect' is where through viable investigative leads;

- Police can or could locate a suspect with the details provided, or
- have sufficient details to apprehend an offender.

The word "local" has its everyday meaning and has been used to ensure that like any other type of crime reported directly to police, where there are local viable investigative leads police should consider the crime for investigation. This is intended to provide the same policing response as with other crime types. For example: If following an assault a suspect can be apprehended, police could respond to that policing demand. It should be the same for fraud offences.

For every call for service where a confirmed fraud/cyber offence is apparent, police will also record an offence at AF via on-line reporting. The number of reports required will be in accordance with the victim count specified by each relevant NFIB offence code.

Example 1: A local business reports to the police that their accountant has been defrauding the company by falsifying their accounts.

The call for service criteria has been met. Police create a local case management record And create an AF report (via on-line reporting).

Example 2: A department store phones police informing them that a suspect is at the till presenting a cloned credit card for payment.

In all the following circumstances the call for service criteria has been met:

A suspect is arrested at the scene
A suspect who has decamped is identified on CCTV
After watching CCTV the suspect is seen but not identified
CCTV not available and the suspect has escaped before police arrival

Police create a local case management record and create a AF report (via on-line reporting).

Example 3: Police are informed by a mail order company that goods purchased using a stolen credit card are going to be delivered to an address on their policing area.

The call for service criteria has been met. Police create a local case management record and create an AF report (via on-line reporting).

Example 4: Police are called by a bank that a person seeking a mortgage is in the branch with a false application.

The call for service criteria has been met. Police create a local case management record and create an AF report (via on-line reporting).

Fraud
(Page 3 of 7)

Crime Location – Call for Service

The venue will be:

Offences where offenders are arrested by the police:

- The venue where the false representation was made.

Where there is a call for service to Police and the offender is committing or has recently committed at the time for the call for service for all fraud types:

- The venue where the false representation was made. This is regardless of any address for the suspect being established through reporting or investigation.

Where there is a local suspect:

- The police force area covering the location of the fraudulent operation/suspect's address, or
- for business related fraud the office/usual place of work of the suspect employee or if no office address or usual place of work, the Head Office of the company. (The term "business related" generally applies to corporate employee fraud, abuse of trust, boiler room addresses etc).

Goods ordered remotely:

- The delivery address to which the fraudulently ordered goods were delivered or are to be delivered.

Fraudulent applications:

- The venue from which the fraudulent application is sent shall be deemed to be the location. However if, as is commonly the case, the fraudster has arranged for a mail re-direction from the first address, then the latest known re-direct address shall be deemed to be the location.

Fraud
(Page 4 of 7)

Crime Location

Crimes passed to Police for enforcement by the NFIB.

Where NFIB recorded fraud crime or a linked series of crimes are passed to police by the NFIB as a case for investigation, the Force Area (except frauds relating to the railways) to record the case will be determined from the following set of principles. The principles are listed in order of priority and it is only when a principle cannot be achieved or is not known that the next principle will apply:

1st The police force area covering the location of the fraudulent operation/suspect's address or for business related fraud the office address/ usual place of work of the suspect employee or if no office address /usual place of work, the Head Office of the company. (The term "business related" generally applies to corporate employee fraud, abuse of position of trust, boiler room addresses etc).

2nd The police force area with the greatest number of individual usages (banking/credit industry) or offences.

3rd The police force area where the first offence (individual usage in banking/credit card fraud) was committed.

4th The police force area where the victim resides or works.

5th In the unlikely event that it is impossible to determine a Force Area using these principles the NFIB will determine a Force Area.

Where there is more than one suspect and the suspects reside in different Force Areas the NFIB will apply the second to fourth principles to try and establish primacy for the investigation. If this does not determine primacy, then the NFIB in discussion with the respective force crime registrars will determine primacy.

Crime Location – British Transport Police
Where the fraud is in relation to the railways (BTP jurisdiction), the NFIB will forward them to BTP Headquarters and not apply the above. Where there are a series of different linked frauds and one of those is in relation to the railways, the NFIB will only forward all linked crimes to BTP if the railway fraud is the most serious offence disclosed in their view.

Crime Location – Cyber Dependent Crime. (Computer Misuse Act etc).
The location of crime rules for fraud apply equally for Cyber dependent crime.

Reminder: The location of crime rules contained within this section overrule those within General Rules Section G - Location of Crime.

The above crime recording, location rules and examples will not cover each and every situation that police will encounter. Therefore nothing contained in these rules should prevent police acting in the best interests of justice, the preservation of property or providing the appropriate levels of service to victims of crime.

Fraud
(Page 5 of 7)

Outcomes

Forces should apply the Outcome rules contained within the General Rules - Section H.

When cases or crimes have been assigned outcomes Forces must contact the NFIB providing the case number, the crime numbers, the suspect details and the outcome details. The NFIB will then update the database and assign the relevant outcome for the Force. Where specimen charges or an all embracing conspiracy have been charged, provided that these charges are reflective of all the crimes within the case investigated, the NFIB will clear up all the crimes within the case.

Example1: The NFIB sends a case to Force A containing 100 crimes of boiler room fraud. The suspects are arrested and CPS authorise charges with 10 specimen counts of fraud by false representation in relation to the investigation.

The NFIB can assign outcomes to all 100 crimes in this situation.

Example 2: The NFIB sends a case relating to the same suspect, to Force A containing a number of mortgage frauds, on line shopping frauds and application fraud. Following a lengthy investigation, the police are only able to charge with one specific offence of application fraud.

The NFIB can only clear up the one specific offence of application fraud.

Where previously a recorded offence under the old legislation is assigned an outcome, Forces should return the outcome information as if recorded under the new legislation. For example a crime recorded in 2004 as a S15 Theft Act deception is assigned an outcome in 2014 the outcome would now be shown as the relevant false representation outcome.

PNC 'Registered item'

Report Fraud does not have access to the Police National Computer (PNC) and therefore will be unable to record crimes where a PNC 'registered item' (vehicle, plant, machinery etc) requires an entry on PNC. Police will be responsible for reporting these offences to the NFIB, and making the relevant PNC entry, i.e LOS, PNC, Interest etc.

Frauds abroad

There is an increasing trend for victims abroad or whilst abroad to try and report fraud in this country, (England and Wales). Where there is no connection with this country the victim is to be told to report it in their own country or to the country they were staying in, when the fraud was committed.

Where the only connection with this country is that the victim of a fraud committed whilst in another jurisdiction resides in this country or a bank or financial institution has only been used to facilitate the transfer of funds from one jurisdiction to another then the crime should not be recorded in this country.

Where it is apparent that the offender was resident in this jurisdiction or that a victim whilst resident in this country has been defrauded from abroad, then a crime should be recorded.

Fraud
(Page 6 of 7)

Frauds abroad

Example 1: A resident of this country travels to Spain and is defrauded in Spain by Spanish registered Time Share Company. He returns and reports it to police force area A.

No crimes need to be recorded under these circumstances.

Example 2: A Belgium National orders goods over the internet from an American Company. He pays for the goods using PayPal. The goods are never delivered. Enquiries at PayPal show that funds were transferred from Belgium to USA via PayPal account in London.

No crimes need to be recorded under these circumstances.

Example 3: A person in the United Arab Emirates receives information via SMS texts and mobile phone calls that they have won £100,000 in a lottery but need to send £450 to receive the winnings. The victim in the United Arab Emirates sends through £450 to the suspect at an address in England via a Western Union office.

One crime (class NFIB1B). The suspect is in England.

Example 4: Mrs 'A' receives a letter to her London address in the post with a Spanish stamp and post mark informing her that she has won the Spanish Lottery. She follows the instructions in the letter and transfers £1000 via Western Union to a Spanish account. When she fails to receive her million pounds she reports the fraud to Report Fraud using the web template.

One crime (class NFIB1B).

Principal Crime Rule and Fraud

By the very nature of the offence being committed for some fraud types there will also be an offence of 'perverting the course of justice' or the non notifiable offence of 'wasting police time'. The Fraud Rules aim to determine levels of fraud within this section. Therefore where such notifiable offences are prosecuted in addition to the fraud offence a crime should be recorded for this offence in addition to the fraud offence. The Principal Crime Rule will not apply in these cases.

Conspiracy to defraud: do not count in addition to substantive crime.

Fraud
(Page 7 of 7)

Financial Institutions

The Financial Institutions will encourage customers (both personal and business) to report cheque, plastic card (Credit card, Debit card, Prepayment card and Store card) or online bank account fraud directly to them and not the Police in the first instance. Online bank accounts include telephone bank accounts. The Financial Institutions will pass fraud reported to them directly to the NFIB.

Where Financial Institutions wish to report a crime to the police they will complete the online Report Fraud template. The NFIB will then pass these offences to the appropriate law enforcement agency when an agreed criteria has been met by applying the same principles as in 'Crimes passed to Police by the NFIB'.

Account holders reporting at Police Stations

Account holders attempting to report cheque, plastic card or online bank account fraud offences at police stations will be asked in the first instance if they have been specifically told to do so by their Financial Institution. If they have, they will be referred to the Report Fraud contact centre. If they have not, they will be told to contact their Financial Institution who will deal with the account holder. It is not necessary to record a crime related incident.

If the Financial Institution wishes an account holder to report the crime, the Financial Institution will give the account holder a reference number for Report Fraud – either in the form of a letter or verbally. In this case, the account holder will be asked to report it to the Report Fraud contact centre.
Where account holders with reference numbers attend the police station they should be referred to the Report Fraud contact centre.

Identity Theft

The use of another person's identification details (or the use of false identification details), often referred to as identity theft, is not in itself an offence in law. It is the action that is undertaken, using those identification details, that needs to be considered in respect of whether an offence has occurred.

Most instances of 'Identity Theft' come to light when victim's details are used to obtain goods, services or money using credit arrangements or loans. Instances of this should be considered under the relevant NFIB recorded crime. Where bank, credit card, or store card accounts are opened using identities to which the individuals are not entitled, and then used to commit fraud, then an offence of NFIB5A Fraud by False Representation Cheque, Plastic Card and Online Bank Accounts (NOT eBay or PayPal) should be recorded.
Note: The opening of a bank or other account using other peoples' identities without permission or false details is unlikely to be a crime of fraud per se, and should only be recorded if there is an offence of fraud committed on the account or evidence that fraud was the purpose for the creation of the account.

Any usage on the account will be dealt with under the reporting guidance General Principles detailed in NFIB5A Fraud by False Representation Cheque, Plastic Card and Online Bank Accounts (NOT eBay or Pay Pal) Classification (1 of 2).

Where people are found in possession of any identity document or items containing identity details, with intent to commit fraud then an offence under 33A Making, Supplying or Possessing Articles for Use in Fraud should be considered.

Remember that if there is no intent to commit fraud and there is evidence that an account has been created using a false, stolen or improperly obtained identity document contained within the Identity Documents Act 2010 then an offence under class 61A possession of False documents should be considered.

NFIB Fraud

NFIB Fraud (Continued)

NFIB3	Consumer and Retail Fraud
NFIB3A	Online Shopping and Auctions
NFIB3B	Consumer Phone Fraud
NFIB3C	Door to Door Sales and Bogus Tradesmen
NFIB3D	Other Consumer and Retail Fraud
NFIB3E	Computer Software Service Fraud
NFIB3F	Ticket Fraud
NFIB3G	Retail Fraud (not NFIB3A or NFIB5A)
NFIB4A	Charity Fraud
NFIB4B	Fraudulent Applications for Grants from Charities or Lottery Fund Organisations
NFIB5	Banking and Credit Industry Fraud
NFIB5A	Cheque, Plastic Card and Online Bank Accounts (not PSP)
NFIB5B	Application Fraud (excluding Mortgages)
NFIB5C	Mortgage Related Fraud
NFIB5D	Mandate Fraud
NFIB5E	Dishonestly retaining a wrongful credit

NFIB Fraud (Continued)

NFIB6A	Insurance Related Fraud
NFIB6B	Insurance Broker Fraud
NFIB7	Telecom Industry Fraud (Misuse of Contracts)
NFIB8A	Corporate Employee Fraud
NFIB8B	Corporate Procurement Fraud
NFIB9	Business Trading Fraud
NFIB10	False Accounting
NFIB11	Bankruptcy and Insolvency
NFIB12	Passport Application Fraud
NFIB13	Department of Works and Pensions (DWP) Fraud
NFIB14	Fraudulent Applications for Grants from Government Organisations
NFIB15	HM Revenue and Customs Fraud (HMRC)
NFIB16	Pension Fraud
NFIB16A	Pension Fraud by Pensioners (or their Estate)

NFIB Fraud (Continued)

NFIB16B	Pension Fraud committed on Pensioners
NFIB16C	Pension Liberation Fraud
NFIB17	Other Regulatory Fraud
NFIB18	Fraud by Failing to Disclose Information
NFIB19	Abuse of Position of Trust
NFIB20A	DVLA Driver Licence Application Fraud
NFIB90	Other Fraud (Not covered elsewhere)
NFIB50	Computer Misuse Crime
NFIB50A	Computer Viruses\Malware\Spyware
NFIB51A	Denial of Service Attack
NFIB51B	Denial of Service Attack Extortion
NFIB52A	Hacking-Server
NFIB52B	Hacking-Personal
NFIB52C	Hacking-Social Media and E-mail
NFIB52D	Computer Hacking – PBX/Dial Through
NFIB52E	Hacking (Extortion)

NFIB1A "419" Advance Fee Fraud Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - "419" Advance Fee Fraud

"A communication soliciting money from the victim for a variety of emotive reasons to assist the fraudster. "

The name has its origin to a reference to the violation of Section 419 of the Nigerian Criminal Code. The 419 scam combines the threat of impersonation fraud with a variation of an advance fee scheme in which a letter, e-mail, or fax is received by the potential victim. The communication from individuals representing themselves as foreign government officials offers the recipient the "opportunity" to share in a percentage of millions of dollars by helping the fraudster to place large sums of money in an overseas bank account.

Payment of taxes, bribes to government officials, and legal fees are often described in great detail with the promise that all expenses will be reimbursed as soon as the funds are out of the country. The recipient is sometimes encouraged to send information to the author, such as blank letterhead stationary, bank name and account numbers, and other identifying information using a facsimile number provided in the letter. The scheme relies on convincing a willing victim to send money to the author of the letter in several instalments of increasing amounts for a variety of reasons.

NFIB1A "419" Advance Fee Fraud Counting Rules (1 of 1)

General Rule: One crime for each specific, intended or identifiable victim.

Application of the Rule

The important aspect to consider is specific intended victim. Where people are cold called or receive global e mails or are part of a mail shot, they are not generally specific intended victims. Where Report Fraud receive reports under these circumstances, then an information report should be recorded.
People are specific intended victims if they take action following the contact.

Example 1: Mr ‘A’ receives a letter purporting to come from an African Government official. The letter effectively states that if Mr ‘A’ pays £1000 into an account to facilitate the transfer of five million pounds into his account he will be entitled to £10,000.

a) Mr A ignores the letter and contacts police.

There is no crime to record in these circumstances, record an information report.

b) Mr A contacts the author by e mail and receives further instructions of what he should do.

One crime (class NFIB1A). Mr A has become a specific intended victim.

Example 2: Mr ‘A’ receives a letter purporting to come from an African Government official. The letter effectively states that if Mr ‘A’ pays £1000 into an account to facilitate the transfer of five million pounds into his account he will be entitled to £10,000. He transfers the money. He then receives another letter asking for an additional £1000, which again he transfers. When a further letter arrives he contacts the police who discover the fraud.

One crime (class NFIB1A).

NFIB1B Lottery Scams Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Lottery Scams

"A fraud which involves the victim being informed they have won a non-existent lottery and required to send an advance to release their winnings."

The lottery scheme deals with persons randomly contacting e-mail addresses, postal addresses or faxes advising them they have been selected as the winner of an International lottery. The e-mail message usually reads similar to the following:

"This is to inform you of the release of money winnings to you. Your e- mail was randomly selected as the winner and therefore you have been approved for a lump sum payout of $500,000.00. To begin your lottery claim, please contact the processing company selected to process your winnings."

An agency name follows this body of text with a point of contact, phone number, fax number, and an e-mail address. An initial fee ranging from $100 to $5,000 is often requested to initiate the process and additional fee requests follow after the process has begun. These emails may also list a United Kingdom, point of contact and address while also indicating the point of contact at a foreign address.

NFIB1B Lottery Scams Counting Rules (1 of 1)

General Rule: One crime for each specific, intended or identifiable victim

Application of the Rule

The important aspect to consider is specific intended victim. Where people are cold called or receive global e mails or are part of a mail shot, they are not generally specific intended victims. Where Report Fraud receive reports under these circumstances, then an information report should be recorded. People are specific intended victims if they take action following the contact.

Example 1: Mrs 'A' receives a letter in the post informing her that she has won a European Lottery. There are details of what she has to do to claim the prize.
a) She puts the letter in the bin as she has never held a ticket in a European Lottery.

There is no crime to record in these circumstances, record an information report.

b) On opening the letter, she contacts the number given and is told to transfer money to an account to facilitate claiming the winnings. She puts the phone down and ignores the request.

One crime (class NFIB1B). Mrs A has become a specific intended victim.

c) On opening the letter, she contacts the number given and is told to transfer money to an account to facilitate claiming the winnings. She transfers money to the account and hears nothing further.

One crime (class NFIB1B).

NFIB1C Counterfeit Cashiers Cheques and Bankers Drafts Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Counterfeit Cashier's Cheques and Bankers Drafts

"Fraudulent cheques or Bankers Drafts are presented as payment for goods or services ordered over the Internet in excess of the actual value. The seller reimburses the purchaser with the excess prior to the cheque or draft being discovered as fraudulent."

This fraud targets individuals that use the Internet to sell merchandise or services. An interested party located in a foreign country contacts a seller. The seller is told that the buyer has an associate in the seller's country that owes him money and that the associate will send a cashiers cheque or bankers draft to pay the seller.

The amount of the cashier's cheque or bankers draft will be far greater than the price of the goods and the seller may be told the excess amount will be used to pay the shipping costs to the buyer. The seller is instructed to deposit the cheque/draft, wait for clearance and wire the excess funds to the buyer or an associate (normally in West Africa).

As a cashier's cheque or bankers draft is used, a bank will typically release the funds immediately, or after a one or two day hold. The seller falsely believes the cheque/draft has cleared and wires the money as instructed. Additionally the seller can be convinced to terminate the sale and refund all the money. Shortly after the seller is notified the cheque/draft was fraudulent and has therefore lost all their money.

A variation to the counterfeit cashier's cheques is:-

Definition - Employment/business opportunities

"A fraud which involves soliciting personal details of victims under the guise of potential employment"

- **Utilising employees to resell/reship goods abroad.**
- **Overpaying employees in the form of a fraudulent cheque/bankers draft accompanied with instructions to wire the overpayment to the fraudster."**

Employment/business opportunity schemes are where bogus foreign- based companies recruit citizens in other countries on several employment search websites for work-at-home employment opportunities.

Prospective employees are required to provide personal information and copies of their identification. Employees hired by these companies are informed their salary will be paid by cheque/draft from a company in the victim's country and reported to be a creditor of the employer.

The amount of the cheque/draft is significantly more than the employee is owed for salary and expenses, and the employee (victim) is instructed to deposit the cheque/draft into their own personal bank account, and then wire the overpayment back to the employer's bank, often located in Eastern Europe. The bank cheques are later found to be fraudulent, often after the wire transfer has taken place.

NFIB1C Counterfeit Cashiers Cheques Counting Rules (1 of 1)

General Rule: **One crime for each specific, intended or identifiable victim.**

Example 1: A person advertises a boat for sale on a website and receives an email from abroad offering the full purchase price. They are sent a cheque covering the purchase cost and an additional £5000 for shipping fees. They pay the cheque into their account and transfer the £5000 to the shipping agents account in Spain before a man collects the boat. The cheque then is returned unpaid as it is a forgery.

One crime (class NFIB1C).

Example 2: Alison is selling her car. Joe contacts her, views the car and a price is agreed. He then hands her a cheque which is made out for £500 more than agreed price. He tells her to pay it into her account and he will come round tomorrow to collect the car and £500 in cash. Alison declines and says that it is cash in hand or nothing.

One crime (class NFIB1C), Alison is an intended victim.

Example 3: A person advertises a horse for sale on a website and receives an email from abroad offering the full purchase price - £2000. They are sent a cheque for £5000 with a request to return the difference of £3000. The seller takes the £5000 cheque to the bank but is advised not to bank it. No monies (or the horse) are sent to the buyer. The seller reports the incident to the police.

One crime (class NFIB1C). They are a specific intended victim.

Example 4: Mrs ‘A’ is contacted by a company from abroad and asked to work at home for them. After a weeks work she receives a bankers draft in payment that is double her wages. She is asked to pay the draft into her account and wire the overpayment to the employer’s bank. This she does. Three days later she is notified by her bank that the bankers draft is fraudulent and the payment has been rejected.

One crime (class NFIB1C)

Example 5: Mrs ‘A’ is contacted by a company from abroad and asked to work at home for them. After a weeks work she receives a cheque in payment that is double her wages. She is asked to pay the cheque into her account and wire the overpayment to the employer’s bank. Being suspicious, she contacts the police who inform her of the fraud.

One crime (class NFIB1C). Mrs A is an intended victim and has worked for nothing.

NFIB1D Dating Scam Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Dating Scam

"The intended victim is befriended on the Internet and eventually convinced to assist their new love financially by sending them money for a variety of emotive reasons."

The intended victim is approached in a chat room or via a social networking site. The fraudster creates a relationship with the victim over the Internet often posting pictures of an attractive person – which is not usually them and may target those of a certain income, if disclosed. The background may suggest that their partner is deceased and they are bringing up a child/children alone. The fraudster will resist any suggestion to meet, often stating that they are moving to work abroad temporarily. Once the fraudster gains the trust of the victim, they then ask for money. This is normally via claims that they have been trapped abroad, have unforeseen medical bills, mobile/internet access problems etc. Once the request for money is declined, they cease contact.

NFIB1D Dating Scam
Counting Rules (1 of 1)

General Rule: One crime for each victim

Example 1: Janet has been chatting to John over the internet for a couple of weeks, having joined a dating chat room. John is very plausible and gains Janet's trust. He purports to be UK based, but moving abroad on short-term contract. He says contact may be difficult as his laptop is malfunctioning and asks for a 'loan' to fix it to be repaid upon his return, which she forwards on. Following payment Janet becomes suspicious and she discovers on investigation that the details she had been provided were false and John is no longer contactable.

One crime (class NFIB1D).

Example 2: Janet has been chatting to John over the internet for a couple of weeks, having joined a dating chat room. John says that he is in the American military fighting abroad. John asks for some money to be sent out via money transfer so he can pay for an airfare to go home to visit his sick mother. It is a large sum of money and Janet makes some checks. She discovers that there is no one with Johns name or rank serving with the US military. She contacts Report Fraud.

One crime (class NFIB1D). On balance of probability this is a fraud.

Example 3: Janet has been chatting to John over the internet for a couple of months. She was contacted after joining a dating chat room. Having spoken more and more John then asks for some money as he has to make an unforeseen trip home as his child is ill. Janet is suspicious and refuses to transfer money. John then refuses to talk with Janet in the chat room and Janet contacts Report Fraud.

There is no crime to record in these circumstances, record an information report.

NFIB1E Fraud Recovery Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Fraud Recovery

"A fraud targeting fraud victims to gain personal details and additional money, by means of posing as recovery agents."

These frauds target former victims of frauds. The victim is contacted by the fraudster who poses as a legitimate organisation. The organisation claims that they can apprehend the offender and recover any monies lost by the victim, for a cost. Another tactic used is the fraudster stating a fund has been set up by the Nigerian government to compensate victims of 419 fraud. This is used to gain personal details of the victim and additional money as a fee to release the amount of the claim.

NFIB1E Fraud Recovery Counting Rules (1 of 1)

General Rule: **One crime for each specific, intended or identifiable victim.**

Example 1: Mr A has been the victim of a boiler room fraud. He is contacted by a suspect who states that they work for a company who specialise in helping victims of boiler rooms and they have traced some of the money that he invested. For a fee of £1000 they can recover £20,000. Mr A pays the fee into an account and then discovers that he is the victim of another fraud.

One crime of fraud (class NFIB1E) and one crime of boiler room fraud (class NFIB2A) if not already recorded.

Example 2: Mr A has been the victim of a boiler room fraud. He is contacted by a suspect who states that they work for a company who specialise in helping victims of boiler rooms and they have traced some of the money that he invested. For a fee of £1000 they can recover £20,000. Mr A is not taken in and reports the matter to police.

One crime of fraud (class NFIB1E) and one crime of boiler room fraud (class NFIB2A) if not already recorded. Mr A is a specific intended victim.

NFIB1F Inheritance Fraud Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

“…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. “

Definition - Inheritance Fraud

Another name for these "estate locators" is "research specialists". Contact is made with victims as part of a mass mailing to people who share the same surname. Each one is told there is cash from inheritances that have been located in their names. The research specialists make money by asserting they've put together an estate report that includes information on where the inheritances are located and how they can be claimed. For a relatively small fee, the report can be provided. They may also propose to administer any inheritance claim for an additional fee. The fraudsters perpetrating this type of inheritance scam purposefully choose smaller inheritances on the off chance that someone receiving their correspondence turns out to be an actual heir with rights to claim the inheritance assets. Once the funds are claimed, they will probably be less than the fee that was paid to the people promoting this scam.

NFIB1F Inheritance Fraud Counting Rules (1 of 1)

General Rule: One crime for each specific, intended or identifiable victim.

Application of the Rule

The important aspect to consider is specific intended victim. Where people with the same surnames are cold called or receive global e mails or are part of a mail shot, they are not generally specific intended victims. Where Report Fraud receive reports under these circumstances, then an information report should be recorded.
People are specific intended victims if they take action following the contact.

Example 1: Mrs Jones receives a global e mail to Jones's informing her that she has inherited some money from the estate of Mr Jones in California. There are details of what she has to do to claim the inheritance.
a) She ignores the e mail because she has no relatives in America.

There is no crime to record in these circumstances, record an information report.

b) On opening the e mail, she replies with an e mail and is given instructions to transfer money to an account to facilitate claiming the inheritance. She ignores the request.

One crime (class NFIB1F). Mrs Jones has become a specific intended victim.

c) On opening the e mail, she contacts the number given and is told to transfer money to an account to facilitate claiming the inheritance. She transfers money to the account and hears nothing further.

One crime (class NFIB1F).

Example 2: Mrs Jones receives a letter through the post informing her that she has inherited some money from a distant relative's estate. The letter contains her full name, date of birth and her maiden name. Mrs Jones is sceptical and makes enquires and discovers that the company sending the mail is bogus, she informs the police.

One crime (class NFIB1F). Mrs Jones is a specific intended victim.

NFIB1G Rental Fraud Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Rental Fraud

Prospective tenants are tricked into paying advanced fees/rent for the rental of premises which, either don't exist, are not for rent, are already rented or are rented to a multiple of victims at the same time. The consequence is that the accommodation is not available to the victim and they have lost the advance fees paid. This particular fraud is often perpetrated against students looking for university accommodation.

NFIB1G Rental Fraud Counting Rules (1 of 1)

General Rule: **One crime for each victim**

Example 1: A student books rental accommodation over the internet for his first year at University. On his arrival he discovers that the apartment he has rented and paid the first three months rent for does not exist. The email address that he replied to is no longer available.

One crime (class NFIB1G).

Example 2: Five students have turned up to a one bedroom apartment to discover that it is not for rent. All of them have paid a deposit and three months rent in advance having answered an advert in a local newspaper. The address that they sent the money to is found to be an accommodation address and there is no trace of the suspect.

Five crimes (class NFIB1G).

NFIB1H Other Advance Fee Frauds Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

NFIB1H Other Advance Fee Frauds Counting Rules (1 of 1)

General Rule: **One crime for each specific, intended or identifiable victim.**

Example 1: Mr ‘A’ has advertised his car for sale in a local newspaper. He is telephoned at home by someone saying that they have a buyer for his car. If he pays them £100 he will put them in touch with him. Mr ‘A’ transfers £100 to an account that was provided but hears nothing further. The person who made contact never had any details of any buyer for the car.

One crime (class NFIB1H).

NFIB1J Lender Loan Fraud Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition – Lender Loan Fraud

"A fraud which involves the victim being contacted and told that they can have a loan for a fee. The fee is paid and no loan is forthcoming."

Victims are cold called, usually over a mobile phone and told that for a fee, a loan has been agreed for them. They are then asked to transfer a fee electronically or via a money service bureau and the loan money will be transferred to their account within hours of the fee being received. The loan is never transferred.
On occasions they may receive an additional request for a transfer fee or additional fees. This is again paid and no loan ever materialises.
Lender loan fraud is entirely different from application fraud (NFIB 5B). In application fraud, it is the suspect falsely applying for a genuine loan. This fraud deals with suspects obtaining fees for non existent loans.

NFIB1J Lender Loan Fraud Counting Rules (1 of 1)

General Rule: One crime for each specific, intended or dentifiable victim.

Example 1: Mr A receives a call on his mobile phone from a suspect stating that for a fee of £50 he can have a loan of £1000 transferred to his current account now, with no credit checks. Mr A agrees and transfers the sum of £50 to the account provided and provides details of his current account. No loan is then transferred to his account.

One crime (class NFIB1J)

Application of the Rule

The important aspect to consider is specific intended victim. Where people are cold called and break of the contact, they are not specific intended victims. Where people who are cold called provide contact details or act on the information, then they become specific intended victims, even if subsequently no money is lost.

Example 1: Mrs A receives a call on her mobile saying that for a small fee she can have a guaranteed loan of £500.

a) She hangs up immediately.

There is no crime to record in these circumstances, record an information report.

b) The same suspect phones her back asking her to please listen to the offer of the loan. She again hangs up.

One crime (class NFIB 1J). Mrs A has become a specific intended victim.

Example 2: Mr ‘B’ receives a call on his mobile phone from a suspect stating that for a fee of £50 he can have a loan of £1000 transferred to his current account now, with no credit checks. Mr ‘B’ agrees and receives details of an account to transfer the fee to. Mr ‘B’ then decides that he does not want the loan and takes no further action.

One crime (class NFIB1J).

NFIB2A Share/Bond sales or Boiler Room Fraud Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Share/bond Sales or Boiler Room Fraud

"Boiler room fraud is a fraud where victims are cold-called by fake stockbrokers and encouraged or persuaded to buy shares or bonds in worthless, non-existent or near bankrupt companies."

Boiler room is the term used for the illegal offshore dealing rooms that are often located abroad in Spain, Switzerland or the USA. The sales person cold calls potential victims and oppressively sells shares or bonds that are non-existent or worthless enticing victims with the promise of quick, high returns on the investment.

In a bid to appear legitimate, a Boiler room may have a web-site and produce glossy literature and use a telephone number with a London prefix that diverts overseas.

NFIB2A Share/Bond sales or Boiler Room Fraud Counting Rules (1 of 1)

General Rule: One crime for each specific, intended or identifiable victim.

Application of the Rule

The important aspect to consider is specific intended victim. Where people are cold called or receive global e mails or are part of a mail shot, they are not generally specific intended victims. Where Report Fraud receive reports under these circumstances, then an information report should be recorded.
People are specific intended victims if they take action following the contact or are re-contacted.

Example 1: Mr ‘A’ is cold called at home by a boiler room and asked if they wish to invest with them.

a) Mr ‘A’ has heard a report about boiler rooms and hangs up before phoning Report Fraud.

There is no crime to record in these circumstances, record an information report.

b) He shows some interest and his contact details are obtained. The next day he is personally contacted by the boiler room using the details provided and offered shares in a non existent company. Following some discussion Mr ‘A’ declines to invest.

One crime (class NFIB2A). Mr A has become a specific intended victim.

Example 2: Police receive information that five people have invested in a boiler room. They contact all five who confirm that they have invested in the scheme. The shares purchased are in a non existent company.

Five crimes (class NFIB2A).

NFIB2B Pyramid or Ponzi Schemes Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Pyramid or Ponzi Schemes

"A pyramid scheme is a non sustainable business model using cross-selling. It involves the exchange of money for enrolling other persons into the scheme and PONZI is named after the fraudster Charles Ponzi the 1920's financier who defrauded people with a get rich scheme"

Pyramid schemes are investment scams in which investors are promised abnormally high profits on their investments. The individual makes a payment for a high return and then attempts to recruit more investors to increase their payments, however no investment is made on their behalf.

Early investors are paid returns with the investment money received from the later investors. Unfortunately, the system usually collapses and later investors do not receive dividends and lose their initial investment. This can be facilitated by email, letter, fax or phone solicitation often involving fake referrals and information.

NFIB2B Pyramid or Ponzi Schemes Counting Rules (1 of 1)

General Rule: **One crime for each investor or group of investors.**

Example 1: Following the collapse of an investment fund police discover a ponzi fraud. They find 30 individual investors and three syndicate group investments. Each syndicate has 10 individual investors.

Thirty three crimes (class NFIB2B). Each syndicate is a group of investors.

NFIB2C Prime Bank Guarantees Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

“…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. “

Definition - Prime Bank Guarantees

International fraudsters have invented an investment scheme that offers extremely high yields in a relatively short period of time. In this scheme, they purport to have access to "bank guarantees" which they can buy at a discount and sell at a premium. By reselling the "bank guarantees" several times, they claim to be able to produce exceptional returns on investment. For example, if $10 million worth of "bank guarantees" can be sold at a two percent profit on ten separate occasions, or "tranches," the seller would receive a 20 percent profit. Such a scheme is often referred to as a "roll program." To make their schemes more enticing, fraudsters often refer to the "guarantees" as being issued by the world's "Prime Banks," hence the term "Prime Bank Guarantees." Other official sounding terms are also used such as "Prime Bank Notes" and "Prime Bank Debentures." Legal documents associated with such schemes often require the victim to enter into nondisclosure and non-circumvention agreements, offer returns on investment in "a year and a day", and claim to use forms required by the International Chamber of Commerce (ICC). In fact, the ICC has issued a warning to all potential investors that no such investments exist.

The purpose of these frauds is generally to encourage the victim to send money to a foreign bank where it is eventually transferred to an off-shore account that is in the control of the fraudster. From there, the victim's money is used for the perpetrator's personal expenses or is laundered in an effort to make it disappear.

NFIB2C Prime Bank Guarantees Counting Rules (1 of 1)

General Rule: One crime for each specific, intended or identifiable victim.

Application of the rule

The important aspect to consider is specific intended victim. Where people are cold called or receive global e mails or are part of a mail shot, they are not generally specific intended victims. Where Report Fraud receive reports under these circumstances, then an information report should be recorded.
People are specific intended victims if they take action following the contact or are re-contacted.

Example 1: Mr ‘A’ is cold called at home by a person selling Prime Bank Guarantees and asked if he wishes to invest with them.

a) Mr ‘A’ has heard a report about Prime Bank Guarantees and hangs up before phoning Report Fraud.

There is no crime to record in these circumstances, record an information report.

b) He shows some interest and his contact details are obtained. The next day he is personally contacted again using the details provided. Following some discussion Mr ‘A’ checks the web site of the International Chambers of Commerce and declines to invest.

One crime (class NFIB2C). Mr A has become a specific intended victim.

Example 2: Mr A has purchased three different Prime Bank Guarantees over the last year from the same individual. After a year and a day when he tries to cash in the investment, he discovers the fraud and reports the matter to Report Fraud.

One crime (class NFIB2C).

NFIB2D Time Shares and Holiday Club Fraud Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Time Shares & Holiday Clubs

In Timeshare and Holiday Club frauds the Fraudsters will contact you at home, often by phone and tell you that you have won a 'free' holiday. Or whilst you are on holiday they approach you on the street and give you a scratch card which reveals that you have won a 'free' holiday. All you need to do is go to a presentation to collect your prize and learn more about a new holiday venture. You will be told that this is not about timeshare.

You will later find out that the 'free' holiday isn't free, as you must pay for extras, such as flights and other add-ons and go somewhere you don't want to go at a time that doesn't suit you. If you go to the presentation it will more often than not be held in a plush hotel. The brochures will look glossy and convincing. You will be made to feel as if you are joining an exclusive holiday club which will offer exciting and great value holidays all over the world in top class accommodation.

Unlike the law covering timeshare arrangements, you are not necessarily given a chance to cancel if you have second thoughts. Don't believe everything you hear. What the bogus holiday club tells you in the sales pitch and what is in the contract you sign could be two very different things. Where it states 'You will have holidays in fabulous places at times of year that fit in with your needs.' There are in reality no guarantee of dates or destinations and holidays are often not available when and where you want them. You might end up going nowhere.

NFIB2D Time Shares and Holiday Club Fraud Counting Rules (1 of 1)

General Rule: One crime for each victim

Example

Mr ‘a’ attends a luxury hotel as his prize in a free draw. he is then given a presentation by a Holiday Club, promising him wonderful holidays all over the world at any time of the year in five star accommodation. He invests in two one week slots. He later then discovers that the only holiday he can have under this club is in resorts and at times he does not want to go. The hotels are also way below the advertised standard.

One crime (class NFIB2D).

Application of the Rule

It is important to establish that there is a fraud in Law in these cases before a crime is recorded and not just matters for the Office of Fair Trading and Trading Standards. Each case should be taken on its own merits.

Example 1: Mr ‘A’ attends a luxury hotel as his prize in a free draw. He pays for his own travel and receives discounted hotel accommodation. He attends a presentation to collect his prize and is surprised to find that far from being free he has to pay a yearly fee to a holiday club.

On the information available at the present time, there is no crime to record.

Despite this Mr ‘A’ thinks that it is a good deal, with good resorts and hotels. He signs up. When he tries to book his holiday he discovers that none of the hotels and resorts advertised in the brochure are ever available and the alternatives are at lesser resorts/locations and in three star hotels and not five star hotels. He also discovers that he could have purchased a holiday in the offered hotels at 50% less than his club subscriptions.

One crime (class NFIB2D).

NFIB2E Other Financial Investment Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

“…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. “

Definition - Investment Seminar

The word "investment" is used in connection with a wide range of schemes offering income, interest or profit in return for a financial investment. “Investment” is often used loosely, and sometimes misleadingly, in order to disguise the true nature of a fraud; eg pyramid schemes, chain letters or other types of scheme where a return depends on persuading others to join.

The term "investment" is commonly used in connection with the purchase of something - such as high value or rare goods, stocks and shares, property - in the expectation that what is purchased will increase in value, and even provide an exceptional return compared to other forms of investment.

It is not always understood by potential investors that there is a wide range of so-called investments which are unregulated. This means that they are not traded by authorised investment brokers, who might be expected to operate to professional standards. Nor are they traded on a regulated exchange, which means that their current value and prospects for appreciation are difficult or impossible to assess through any of the normal channels. There is no guarantee that the market will still be functioning when you come to realise your investment and almost no chance of any compensation if the investments have been mis-sold. This all creates opportunities for the unscrupulous to mislead and trap the unwary.

An investment seminar will hook individuals by offering a return which is more attractive than a conventional investment, and so the return on the outlay is always likely to be exaggerated or unrealistic. It follows that the essential message which applies to other scams applies equally to investments. If it looks too good to be true, it probably is!

NFIB2E Other Financial Investment Counting Rules (1 of 1)

General Rule: **One crime for each investor or group of investors**

Example 1: Twelve people are invited to an investment seminar and asked to invest in fine quality wine. Three of the people invest in the scheme. A year later they discover that the wine was not premier cru wine but cheap table wine that was not worth the purchase price and of no value now.

Three crimes (class NFIB2E).

Example 2: A person receives an email asking them to join an investment company which will double their money in 6 months. They send £500 by BACS transfer to an email account. Nothing is received back and the victim reports the matter to police. The method of this incident are recognised to be part of a scam.

One crime (class NFIB2E).

Example 3: Four people separately invest in ostriches at an ostrich farm. They purchase ten chicks each and are told that once fully grown and slaughtered they will see a 50% growth in their investment. A year later they discover that there were only ever 50 ostriches on the farm whereas there should be 5000 for the number of investors. No other victims have come forward.

Four crimes (class NFIB2E).

NFIB3A Online shopping and Auctions Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Shopping and Auction Fraud

"Shopping and Auction fraud involves fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site."

The seller often requests funds to be transferred directly to him/her via Western Union, Money-Gram, or bank-to-bank money transfer. This ensures the money is virtually unrecoverable with no recourse for the victim.

Equally buyers from a legitimate auction site can commit fraud by requesting a certain method of shipping for tax avoidance or they use fraudulent cards or payment methods to purchase goods.

NFIB3A Online shopping and Auctions Counting Rules (1 of 3)

General Rule: One crime for each victim

Example 1: Three people purchase a camera from the same seller on an online site. Payment is made electronically over the internet. The goods do not arrive, and the site is later found to be bogus and untraceable.

Three crimes (class NFIB3A).

Application of the Rule

Note: This is not cheque and credit card fraud (class NFIB5A), as the account holder is responsible for making the transaction.

Great care must be taken in determining that there is a crime in law and not just undelivered goods or a dispute over the goods purchased. Crimes should not be recorded simply because goods have not arrived or are not what was expected. Additional details are necessary, for example email address no longer available, address unknown or found to be a mail drop, more than one complainant, or payment service provider (PSP) payment stopped.

Example 1: Mrs A reports that she is the victim of fraud because goods that she purchased on an on line auction site using her credit card had not arrived.

There is no crime to record in these circumstances.

Mrs A then sends an e mail to the seller and is informed by the Internet Service Provider (ISP) that the e mail address is no longer valid.

Additional details are available to show that on the balance of probabilities this is a fraud. One crime (class NFIB3A)

Example 2: Mr A reports that he has sold goods to a suspect following placing the goods on an on line auction site to Suspect B. He has not received payment.

There is no crime to record in these circumstances

Following further enquiries Mr A has established that payment was made using a PSP into his PSP account but the following day the payment was reclaimed by the PSP as a stolen credit card was used to make the payment.

One crime (class NFIB3A) and one crime of cheque and credit card fraud (class NFIB5A) if not already recorded.

Example 3: Mr A has sent goods to a purchaser following an advertisement on an on line auction site. He has received no payment and on making enquiries discovered that the address that the goods were sent to is a mail drop used by many different people.

One crime (class NFIB3A)

Example 4: Mr A purchased goods from an on line auction site. On receipt of the goods, the quality was far inferior to what he expected. He complained and reported the matter to police.

There is no crime to record in these circumstances.

NFIB3A Online shopping and Auctions Counting Rules (2 of 3)

Application of the Rule (continued)

(i) Mr A's details were passed to Trading Standards who linked his case to five other victims. With these additional details, Trading Standards consider that the action of the seller are fraudulent and report the matter to Report Fraud.

Six crimes (class NFIB3A)

Example 5: Mrs A purchased goods from the internet and transferred money using Western Union to a European Western Union Office. The goods do not arrive and she discovers that the address she has been given does not exist.

One crime (class NFIB3A).

For a crime to be recorded the victim must be an actual victim or potential victim. Where a thief for example, has disposed of stolen property using an on line auction site and goods have been purchased and received by innocent purchasers, although the purchasers can never receive good title to those goods, they are not treated as victims unless the goods are recovered and they then become victims.

Example 1: A thief steals a delivery of 1000 Birthday cards and sells them to a 1000 different people using an on line auction site at a slightly discounted price. The thief is arrested and the details of all the purchasers are obtained from the on line site. Ten purchasers are contacted and state that they purchased a card.

There are no additional crimes to record beyond the original theft crime.

Example 2: A thief burgles a fishing shop and steals 10 fishing rods. The rods are then disposed of on an on line auction site. The innocent purchasers are traced and police recover the 10 fishing rods from ten separate purchasers.

Ten crimes (class NFIB3A) in addition to the original burglary. The innocent purchasers are now victims.

Example 3: A thief burgles a fishing shop and steals two very expensive fishing rods. He sells the rods on an online auction site at a tenth of the value. The two purchasers are traced and admit that they thought the rods were stolen because of the price.

One crime of Burglary (class 30C) and two crimes of handling stolen goods (class 54).

Principal Crime: see also General Rules Section F and Annex C.

Where goods are purchased over the internet and payment is made using a stolen or cloned plastic card the crime should be recorded under class NFIB5A (cheque and credit card fraud) and not NFIB3A.

Example 1: Suspect purchases a train ticket over the internet using a cloned card. She then obtains the rail ticket at the station by inserting the cloned card into a ticket machine.

One crime (class NFIB5A).

NFIB3A Online shopping and Auctions Counting Rules (3 of 3)

Use of Payment Service Providers (PSP's)

Where fraud is perpetrated using PSP's (eg Paypal, Moneygram) offences should be recorded under this section and not under Cheque and credit card Fraud. Where PSP accounts have been topped up using stolen credit cards or debit cards then a crime should also be recorded for the credit card fraud (if not already recorded).

Example 1: Goods are purchased from an online site and paid for using pay pal. The goods are dispatched and the next day the retailer is informed that the pay pal payment has not gone through because the account was funded by a stolen credit card.

One crime (class NFIB3A) and one crime of cheque and credit card fraud (class NFIB5A) if not already recorded.

NFIB3B Consumer Phone Fraud Classification (1 of 2)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Phone Frauds

a) Missed calls & Text messages

Missed call frauds start by ringing your phone and hanging up so quickly that you can't answer the call in time. Your phone registers a missed call and you probably won't recognise the number. People will often then call the number back to find out who it is. Apart from being a nuisance, the missed call can lead to a fraud in two ways:

- the number you call back may be redirected to a premium rate service without your knowledge, which means you will be charged a lot of money per minute, often costing up to £15 per call;
- The number may tell you that you have won a prize of some sort, and give you another number to call to 'claim' your prize, but they may not tell you how much the call will cost. This second number may be a premium rate number, again charging you a lot of money to get your 'prize'. Your prize may be nothing more than a ring tone subscription which can also be a fraud!

Text message frauds work by sending you a text message from a number you may not recognise, but the content of the message could sound like it's from a friend, for instance 'Hi, it's John. I'm back! When do you want to catch up?' or 'Hey big fella, happy birthday!'

Another common tactic is for a text message to sound like someone flirting with you. Many people reply asking who it is, and end up engaging in a lengthy SMS exchange with the fraudster. Only later do they find out that they have been charged a high rate both for messages they sent (sometimes, there are also charges for messages received as well).

b) Ring Tone Scams

A reverse text scam is where the victim can end up paying to receive texts, such as ring tones and wallpapers, typically from 25p to £1.50 per message.

These scams might attract you with an offer for a 'free' or low cost ring tone. What you may not realise is that by accepting the offer, you are actually subscribing to a service that will keep sending you ring tones—and charging you a premium rate for them. There are many legitimate companies selling ring tones, but there are also fraudsters who will try to hide the true cost of taking up the offer.

The fraudsters don't tell you that your request for the first ring tone is actually a subscription to an expensive service. A fraudster will also make it difficult for you to stop the service. You actually have to 'opt out' of the service to stop the ring tones and high charges. Some people have been charged over £100 for what they thought was one ring tone.

NFIB3B Consumer Phone Fraud Classification (2 of 2)

Definition - Phone Frauds (continued)

c) SMS competition & Trivia scams

An SMS competition or SMS trivia scam usually arrives as a text message and may encourage you to enter a competition for a great prize (like an mp3 player). The message (or sometimes, an advertisement) could also invite you to take part in a trivia competition, with a great prize on offer if you answer a certain number of questions correctly.

The fraudsters make money by charging extremely high rates for the messages you send, and any further messages they send to you. These charges could be as high as £2 for each message sent and/or received.

With trivia scams, the first lot of questions will be very easy. This is meant to encourage you to keep playing. However, the last one or two questions that you need to answer to claim your 'prize' could be very difficult or impossible to answer correctly (and may even require you to guess a random number). A winner, to claim a cash prize, may have to dial a number that begins with say 0906, to collect the prize. This is a premium rate number that lasts several minutes with no prize materialising.

Definition - Phone Insurance Scams (not to be confused with false insurance claims by account holders)

The fraudsters target people with new phones and make them believe they are getting a call from the shop or the mobile phone network. After the consumer gives their payment details they end up with poor quality phone insurance or none at all. Those involved in the scam often buy phones and call numbers similar to their own number until they find someone with a new phone.

NFIB3B Consumer Phone Fraud Counting Rules (1 of 2)

General Rule: One crime for each specific, intended or identifiable victim.

Example 1: Mrs A receives a missed call on her mobile phone. She dials the number and is told by the person answering the call that he is on the other line and will be with her in a minute and is placed on hold. After being on hold for a few minutes she hangs up. When she receives her bill she notices that this call was to a premium rate phone line and had cost her £20.

One crime (class NFIB3B)

Example 2: Mr A receives a voice message informing him that he has won a prize. He dials a new number to claim his prize which is a premium rate number. After keying in a number of options he is eventually told that the prize is a one month free ring tone subscription. The call has cost him £20.

One crime (class NFIB3B)

Application of the Rule

The important aspect to consider is specific intended victim. Where people are cold called or receive global texts, they are not generally specific intended victims. Where Report Fraud receive reports under these circumstances, then an information report should be recorded. People are specific intended victims if they take action following the contact.

Example 1: Mrs ‘A’ receives a missed call on her mobile phone. She dials the number and is told by the person answering the call that he is on the other line and will be with her in a minute and is placed on hold. After being on hold for a few minutes she hangs up. Three colleagues in her office also receive missed calls from the same number. Knowing what has just occurred they ignore the missed call.

One crime (class NFIB3B). The three other people are not specific intended victims.

Example 2: Mr ‘A’ has just purchased a new mobile phone contract with a new number. About half an hour later he receives a call selling him insurance for the phone. He hangs up.

There is no crime to record in these circumstances

Mr ‘A’ likes the offer and takes out the insurance, paying on his credit card. No policy comes through the post as promised and on making enquiries he discovers that the Insurance company do not exist.

One crime (class NFIB3B).

Finished Incident: see also General Rules Section E.

Frequently victims of mobile phone frauds become the victim of a number of different types of fraud in relation to a phone fraud. Only one crime should be recorded in these instances.

NFIB3B Consumer Phone Fraud Counting Rules (2 of 2)

Finished Incident: see also General Rules Section E (continued)

Example 1: Mr A receives a voice message informing him that he has won a prize. He dials a new number to claim his prize which is a premium rate number. After keying in a number of options he is eventually told that the prize is a one month free ring tone. The call has cost him £20. On accepting the free ring tone he has in fact subscribed to a very expensive opt out ring tone service. By the time he has managed to opt out he has been charged £100 for a number of ring tones he does not want.

One crime (class NFIB3B)

NFIB3C Door to Door Sales and Bogus Tradespeople Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

NFIB3C Door to Door Sales and Bogus Tradespeople Counting Rules (1 of 2)

General Rule: **One crime for each victim**

Example 1: An elderly resident Mrs 'A' reports that following a knock on her door from a chimney sweep, she has been talked into having her chimney cleaned for £500. Her son has informed her that she does not have a chimney as all her services are electrically supplied.

One crime (class NFIB3C)

Application of the Rule

Crimes should be recorded where it is clear that the circumstances are fraudulent. Where it is not clear that the circumstances are fraudulent then Trading Standards should be informed.

Example 1: Police attend a street where three houses have had their front gardens tarmacked. They have received a quote detailing full description of the work to be carried out that includes removing the turf, laying hardcore and substrate before two layers of tarmac are applied. They have paid £2000 for each drive. Two weeks later, when grass is growing through the tarmac it is clear that a thin layer of asphalt has been laid and rolled directly onto the lawn.

Three crimes (class NFIB3C)

Example 2: Police are called to an address where a gardener and owner are in dispute over the quality of work of gardening. The gardener's details are verified and police are not able to determine if there is an offence or not. Both are advised to consult solicitors and trading standards.

There is no crime to record in these circumstances

Finished Incident: see also General Rules Section E.

Example 1: An offender admits to deceiving five people over a period of two years by deceiving them as to the condition of their roofs, getting them to agree to his repairing the invented damage and then charging an exorbitant price.

On confirmation of the victim, five crimes (class NFIB3C).

Class NFIB3C and Distraction Burglary Class 28K and 28L.

Class NFIB3C should only be recorded where a false representation is used to carry out work or sell goods or services, or a clear attempt to sell goods or services or carry out work.
This is entirely different from Distraction Burglary the definition of which can be found under Class 28K.

If there is any doubt about which crime to record an offence under class 28K should be recorded.

NFIB3C Door to Door Sales and Bogus Tradespeople Counting Rules (2 of 2)

Class NFIB3C and Distraction Burglary Class 28K and 28L (continued).

Example 1: A man knocks at the door purporting to be a double glazing salesman. He is invited into the lounge where it is apparent that he has little knowledge about double glazing, no leaflets and can not provide any identity or details of his company. He is challenged and runs from the property.

One crime (class 28D).

Example 2: A man knocks at the door purporting to be a double glazing salesman. He is invited into the lounge where he provides great details of double glazing products and provides leaflets. A costing is made and the owner is asked to provide a £500 deposit to secure the one of deal. On examination of the leaflets it is noticed that they are of poor quality and when questioned about them, the salesman leaves.

One crime (class NFIB3C).

Example 3: A man knocks at the door stating that he is selling off cuts of carpet and if he can measure the lounge carpet he will be able to lay it today. He is invited into the front lounge and offered a cup of tea. The householder then disturbs him in a separate room searching through a chest of draws. The suspect decamps without any explanation.

One crime (class 28D).

NFIB3D Other Retail and Consumer Fraud Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

NFIB3D Other Retail and Consumer Fraud Counting Rules (1 of 1)

General Rule: **One crime for each victim**

Example 1: Mr ‘A’ agrees to purchase a laptop computer advertised in a local paper. He attends a car park and is shown the advertised goods working. He hands over the cash and is distracted by an accomplice. He is then handed the computer in its case and drives home. When he opens the case he discovers a telephone directory instead of the computer he had purchased.

One crime (class NFIB3D).

Example 2: Mrs ‘A’ purchases a car she sees for sale on a street corner after a test drive. She is promised that the paperwork will follow. When she does not receive any documents, she contacts the police who inform her that she has purchased a stolen vehicle.

One crime (class NFIB3D).

Example 3: The organiser of a school fete is approached by a man who states that he has 10 signed premiership football shirts with documentation of authenticity to auction. If he can do this at the fete he will donate a third of the proceeds to the school. The shirts sell for an average of £250 and are purchased by 10 separate people. When they get home and unpack the shirts they find that the certificate of authenticity is a forgery and the signatures are copies.

Ten crimes (class NFIB3D).

Example 4: John is trying to obtain a pedigree puppy for his wife’s Birthday. He answers an advertisement in a paper and is told that the latest litter has all been sold but to leave his contact details. About an hour later he receives a call and is told that one of the puppies has become available and if he transfers the money to a bank account provided he can secure the purchase and pick up the puppy later. John asks if he can see the puppy first, but is told that unless he pays for the puppy now it will not be saved for him and that it is a first come first served basis. He transfers the money and then discovers that the kennels he has attended do not exist.

One crime (class NFIB1H).

Example 5: Police are called to an Airport where five passengers have purchased holidays over the internet. On turning up at the airport they have discovered that the company does not exist and there is no holiday.

Five crimes (class NFIB1H).

NFIB3E Computer Software Service Fraud Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition – Computer Software Service Fraud

"A fraud which involves the victim being contacted and told that there is a problem with their computer and for a fee this can be fixed. No fix actually occurs"

Victims are cold called, usually by phone and told that there is a problem with their computer and for a nominal fee the suspect can fix it. Often the suspects claim that the computer has been infected with a virus or that they are from Microsoft and can offer an update or fix performance. Many reasons can be given, but the victim is persuaded to provide details so the fraudster can gain access to the computer. The victims then often witness the mouse moving and pages displayed. They then pay a small fee and are told that the problem has been fixed. This is not the case, nothing has been done. Sometimes programs are also installed that allow the fraudsters unlimited access to the computer without the victims knowledge. This allows further illegal activity to be carried out. Once the initial small payment has been processed, it is not uncommon for additional larger payments to be withdrawn without permission from the victims account.
This fraud should not be viewed as limited to desk or lap top computers. It can include any device using operating software accessible on line, for example games consoles and smart phones.

NFIB3E Computer Software Service Fraud Counting Rules (1 of 1)

General Rule: One crime for each specific, intended or identifiable victim.

Example 1: Mrs ‘A’ is cold called at home on her house phone. After a short conversation, she is persuaded that she has a virus on her computer. She provides details to the suspect who gains access to her computer. He then demonstrates to her the problem with her computer and tells her that for a fee of £19.99 he can fix it now. She pays the fee, and watches a number of things happen on her computer. She is then told that the problem has been fixed. When she receives her credit card bill, she finds that an additional payment of £99 has been taken. Examination of her computer discovers that she did not have the virus and no software was downloaded to her.

One crime (class NFIB3E)

Application of the Rule

The important aspect to consider is specific intended victim. Where people are cold called and break of the contact, they are not specific intended victims. Where people who are cold called provide details or carry out instructions on their computer, then they become specific intended victims, even if subsequently no money is lost.

Example 1: Mrs ‘A’ receives a call at home stating that her computer has a virus and that for a fee of £5 it can be sorted out now.

a) She hangs up immediately.

There is no crime to record in these circumstances, record an information report.

b) The suspect then asks her to turn on her computer and open up her internet home page. He then asks her to provide details that will allow him to access her computer. Mrs ‘A’ becomes suspicious and hangs up, without giving any details.

One crime (class NFIB 3E). Mrs A has become a specific intended victim.

NFIB3F Ticket Fraud Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition – Ticket Fraud

"Ticket fraud involves the victim purchasing tickets remotely e.g. over the phone or internet"
By victims purchasing any ticket in advance over the phone or internet. Tickets could be for concerts, events, or flights for example. The tickets are never supplied or turn out not to be valid or worthless.

NFIB3F Ticket Fraud Counting Rules (1 of 1)

General Rule: One crime for each victim

Example 1: Mrs A was unsuccessful in obtaining tickets to see her favourite band live at a stadium venue. She then found a web site that was offering tickets for this concert. She purchased a ticket and paid for it using a debit card. She was informed that the ticket would arrive two weeks before the concert. When it failed to arrive she discovered that the web site no longer existed, the phone number provided was disconnected and there was a lot of information on forums stating that this was a scam.

One crime (class NFIB3F).

Application of the Rule

Note: This is not cheque and credit card fraud (class NFIB5A), as the account holder is responsible for making the transaction.

Great care must be taken in determining that there is a crime in law and not just undelivered tickets or a dispute over the tickets purchased. Crimes should not be recorded simply because goods have not arrived or are not what was expected. Additional details are necessary, for example email address no longer available, address unknown or found to be a mail drop, more than one complainant, or payment service provider (PSP) payment stopped.

Example 1: Mrs A reports that she is the victim of fraud because tickets that she purchased on an on line web site using her credit card had not arrived.

There is no crime to record in these circumstances.

Mrs A then sends an e mail to the seller and is informed by the Internet Service Provider (ISP) that the e mail address is no longer valid.

Additional details are available to show that on the balance of probabilities this is a fraud. One crime (class NFIB3F).

Number of Crimes

The victim is the purchaser or the person attempting to make the purchase. It is not the number of people affected. Where tickets are all inclusive, for example a holiday package, then a crime should be counted for the overall package and not each element of that package.

Example 1: Mrs A has purchased 10 airline tickets for her family to travel for the ‘Hajj’. When they arrive at the airport they discover that the airline does not exist.

One crime (class NFIB3F).

Example 2: Police are called to an Airport where five passengers have independently purchased holidays over the internet. On turning up at the airport with their tickets, they have discovered that the company does not exist and there are no flights and no holiday.

Five crimes (class NFIB3F).

NFIB3G Retail Fraud (not NFIB3A or NFIB5A) Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

053/46(pt) Obtaining services dishonestly
(V) Fraud Act 2006 Sec 11

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Legal: Obtaining Services Dishonestly

Fraud Act 2006 Sec 11

"… if he obtains services for himself or another by a dishonest act and the services were made on the basis that payment has been, is being or will be made for or in respect of them or he obtains them without payment having been made for or in respect of them or without payment having been made in full, and when he obtains them he knows they are being made available on the basis that payment will be made for them….".
Definition – Retail Fraud

"**Retail fraud** is fraud committed against retailers that does not involve on line sales or cheque, or plastic card sales"

Refund Fraud: This is where the suspect attempts or obtains a refund by false representation. For example, refunding goods that have been stolen and not purchased, or goods purchased during a sale and the non-sale price being claimed.

Label Fraud: This is where the label on an expensive product is switched with a cheaper label and an attempt is made to purchase at the cheaper price.

Obtaining Goods or services with no intent to pay: This is where you order food or enjoy entertainment where you have no intention of paying.

NFIB3G Retail Fraud (not NFIB3A or NFIB5A) Counting Rules (1 of 1)

General Rule: One crime for each victim

Example 1: Mrs 'X' approaches the customer service desk of a department store with a dress that she knows has been stolen. She asks for a refund, as it is an unwanted Birthday present.

One crime (class NFIB3G)

Example 2: Mrs 'X' selects two dresses in a department store. One is twice the price of the other. She goes to the fitting room to try them on. In the fitting room she swaps the pricing labels over, leaves the cheap dress behind and approaches the till and attempts to pay the cheap price for the expensive dress. The sales staff realise what she has done and Police are called.

One crime (class NFIB3G)

Example 3: A person approaches a shop and request change of a £20 note. They then keep changing their mind and ask for different denominations of change until the staff member becomes confused and hands over too much money.

One crime (class NFIB3G)

Principle Crime: see also General Rules Section F and Annex C.

Example 1: A garage reports that a man drove up and filled his car with petrol. He then had a cup of coffee in the shop and went up to the cashier to pay for the coffee. The cashier asked him if he wished to pay for the petrol now as well. He replied that he had not filled up with petrol. The cashier indicated his car at the pump and again was told that no petrol had been taken for the car. He paid for the coffee and drove off. When the assistant looked at the CCTV it was clear that £35 of petrol had been placed in the vehicle.

One crime (class NFIB3G). This should be recorded as a false representation and not making off without payment.

NFIB4A Charity Fraud Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Charity Fraud

"Fraudulently soliciting donations to a non-existing charity or the organised fraudulent collection of funds from genuine charities."

The fraudster poses as a representative of a charitable organisation soliciting donations to help a number of worthy emotive causes such as a natural disaster, epidemic or conflict. The fraudster requests donations with links to news stories or fraudulent websites to strengthen their cases. The victims are charitable persons willing to help a good cause and expect nothing in return. Once sent the money is irretrievable and the fraudster disappears.

NFIB4A Charity Fraud Counting Rules (1 of 2)

General Rule: One crime for each victim

Example 1: Following a major earthquake that kills many people ten people contact Report Fraud to state that they made donations to a charity web site to support the victims. The Charity and web site are found to be bogus.

Ten crimes (class NFIB4A).

Example 2: Five households contact police to report that they were visited by a man purporting to be from a charity. They completed Direct Debit mandates and have had two payments taken from their accounts before becoming suspicious and discovering that the charity does not exist.

Five crimes (class NFIB4A).

Application of the Rule

For crimes to be recorded in this class it is essential that actions are more than merely preparatory. Calling door to door and speaking to the person who answers the door or approaching passers by and holding conversations with them is preparatory for crime recording purposes.

Example 1: Following an enquiry into a bogus Charity Police find five households that were visited by a man purporting to be from the charity. They were spoken to and encouraged to donate to the charity, but politely declined to donate to the Charity.

Five crimes (class NFIB4A).

Example 2: Following an enquiry into a bogus Charity an offender admits that he visited twenty households purporting to be from the charity. There was no reply at fifteen addresses. Three households were spoken to but politely declined to donate to the Charity. The other two households completed direct debit mandates which they cancelled before any money was transferred from their accounts.

Five crimes (class NFIB4A).

Non existing or Organised

For crimes to be recorded in this class the charity must be a non existing charity or there is an organised attack by the offender(s) on a registered charity.

Example 1: A registered Charities web page is hacked into and the account details are changed to make donations to the offenders account. Police trace five people who donated money through the hacked web page.

Five crimes (class NFIB4A).

NFIB4A Charity Fraud Counting Rules (2 of 2)

'Non existing or Organised' (continued)

Example 2: A youth steals a charity box from a station. He then stands on the corner of a street and obtains money from a number of passing commuters. Police arrest him and trace two victims who made donations.

One crime of theft (class 49) and two crimes of other fraud (NFIB90). This is not organised

Where no donators can be traced or the organised operation has been stopped before any donations are made then count one crime class NFIB4A for each charity, provided that an attempt in Law is made out. If the acts are not more than merely preparatory then record an offence under class 33A Making, Supplying or Possessing Articles for use in Fraud should be recorded.

Example 1: A thief steals a box containing twenty charity collection boxes from a Post Office van. He then passes them to twenty mates who make collections using the boxes. Police become suspicious and arrest all twenty collectors. There are no details of any people who have made donations into the boxes.

One crime (class NFIB4A). One crime Theft of Mail (class 42) if not already recorded.

Example 2: A thief steals a box containing twenty charity collection boxes from a Post Office van. He then passes them to twenty mates who make collections using the boxes. Police become suspicious and arrest all twenty collectors. There are details of twenty people who have made donations into the boxes.

Twenty crimes (class NFIB4A). One crime Theft of Mail (class 42) if not already recorded.

Example 3: A police operation arrests a number of offenders who had created false web pages in relation to five registered charities to obtain money. The offenders were arrested before using the false pages and were charged with a conspiracy to defraud the five Registered Charities.

Five crimes (class NFIB4A).

Charity Fraud or Theft

Example 1: A registered charity has provided households with collection bags to put clothing in. These bags are filled and placed outside front doors for collection by the charity. They are taken by someone who has nothing to do with the charity.

One crime of theft (class 49) for each household.

Example 2: Bags are delivered to householders purporting to be from a registered charity. They are not. They look like the registered charity bags but have nothing to do with them. Householders fill the bags and place them on their doorsteps. They are then collected.

One crime (class NFIB4A) for each household.

NFIB4B Fraudulent Applications for Grants from Charities or Lottery Fund Organisations Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

This is where Charities have provided grants, based on false representations or where they have received grant applications that contain false representations and so no grant was paid.

Lottery Fund Organisations

NFIB4B includes grants from organisations that distribute money from the National Lottery for example Sport England.

NFIB4B Fraudulent Applications for Grants from Charities or Lottery Fund Organisations Counting Rules (1 of 1)

General Rule: **One crime for each grant application.**

Example 1: A registered charity has provided funding for a project as a result of a grant application. The applicant receives the money, pays it into his account and then leaves the country.

One crime (class NFIB4B).

Example 2: A Charity has received an application for a grant of £10,000 for a project. In checking the application the Charity finds that the applicant has used false details and the company who were to undertake the work does not exist.

One crime (class NFIB4B).

Example 3: Sport England has provided funding for a project as a result of a grant application. The applicant receives the money, pays it into his account and spends the money on himself. No money is used on the project.

One crime (class NFIB4B).

NFIB5A Fraud by False Representation Cheque, Plastic Card and Online Bank Accounts (not PSP) Classification (1 of 1)

053/40(pt)	Fraud by false representation	053/04(pt)	Conspiracy to commit cheque or credit card fraud.
(V)	Fraud Act 2006 Sec 2.	(V)	Common Law. Criminal Justice Act 1987 Sec 12(pt).

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - PSP
PSP is a payment service provider for example Paypal and World Pay that are not banks, dealing in electronic money transfers.

Definition - Plastic Card

Plastic card means: Credit card, Debit card, Prepayment card and Store card.

Recording Practice: Cheque and Plastic Card Fraud

Report Fraud will not record the original theft of items used to commit this fraud. Customers of the Financial Institutions will be asked to report the theft of items separately to Police where appropriate. In these instances Police should record the original theft of the card etc under the appropriate class. It is not necessary to record another crime if the theft is already recorded or included in another principle crime e.g. burglary or robbery.

Recording Practice: Conspiracy to Defraud

If, following receipt of information, there is evidence that suggests that plastic cards are being compromised at a particular location on a regular basis, and no crimes have been confirmed for this location with individual financial institutions, this should be recorded as one offence of Conspiracy to Defraud (class NFIB5A), by the Police. Details should also be passed to the NFIB.

NFIB5A Fraud by False Representation Cheque, Plastic Card and Online Bank Accounts (not PSP) Counting Rules (1 of 6)

General Rule: **One crime for each identifiable financial loser, for each account defrauded, using stolen, forged or cloned cheques or cards.**

Application of the Rule

Generally this will equate to one crime per credit card or cloned card or cheque book or online account. The Bank is the aggrieved unless otherwise stated.

Example 1: A stolen credit card is used to obtain goods from five separate shops.

One crime of cheque and credit card fraud (class NFIB5A) plus original theft of card (class 49).

Example 2: Personal and security details obtained legitimately of a victim's bank account are subsequently used fraudulently to purchase goods from five on line suppliers. The money is exchanged electronically.

One crime cheque and credit card fraud (class NFIB5A) only one account defrauded.

Example 3: A person is apprehended for manufacturing four forged credit cards and using them to obtain goods from three separate shops.

Four crimes of cheque and credit card fraud (class NFIB5A). One crime for each account defrauded.

Example 4: Five cheques from a previously reported stolen cheque book are used to obtain goods from the same store. They are reported to the police at different times.

One crime cheque and credit card fraud (class NFIB5A). They are all from the same account.

Example 5: A lost store card is used to obtain goods from three different branches of the same store-chain.

One crime of cheque and credit card fraud (class NFIB5A) plus theft by finding of card (class 49).

Example 6: A stolen benefit cheque issued by DSS is cashed at the Post Office.

One crime of theft (class 49) plus one crime of cheque and credit card fraud (class NFIB5A).

Example 7: A stolen cash card is used to obtain money from four cash machines; one inside a supermarket and three outside separate branches of a bank.

One crime cheque and credit card fraud (class NFIB5A) plus original theft of card (class 49). All theft from the same account.

NFIB5A Fraud by False Representation Cheque, Plastic Card and Online Bank Accounts (not PSP) Counting Rules (2 of 6)

Application of the Rule (continued)

Example 8: Credit card deception occurs at a supermarket store and filling station situated within the same venue.

One crime of cheque and credit card fraud (class NFIB5A). All from same account.

Example 9: An offender has kept credit card details of 50 people. The offender has used each number once to transfer money from these 50 accounts into his/her own online account using a computer. All reported to Force A by the NFIB.

The number of crimes is the number of accounts defrauded (class NFIB5A).

Example 10: Police arrest a person for credit card fraud in a shop following the owner reporting to police that the suspect had used a cloned card in the shop two weeks ago.

One crime of cheque and credit card fraud (class NFIB5A). Arrested by police deal as though reported by the financial Institution concerned or NFIB.

Count each account defrauded, whether the Financial Institution or NFIB reported the fraud to the police or it was subsequently discovered in the investigation.

Example 1: A stolen credit card or cheque book has been used to obtain goods from two shops which reported the incidents separately. During police enquiries 57 other crimes, involving identifiable and different victims, are discovered using the same credit card or cheque book account.

One crime (class NFIB5A). They are all from the same account plus original theft of card or cheque book (class 49).

Example 2: Twelve stolen credit cards or stolen cheque books have been used to obtain goods from two shops which reported the incidents separately. During police enquiries 57 other crimes, involving identifiable and different victims, are discovered using the same credit cards or cheque books.

Twelve crimes (class NFIB5A). One for each account defrauded plus original theft of card or cheque book (class 49).

Example 3: A ladies purse is stolen containing a Nationwide Flex account card, a Nationwide Credit Card and a Nationwide Cashbuilder account card all in her name. All of them have been used fraudulently.

Three crimes (class NFIB5A). One for each separate account defrauded plus original theft of the purse.

Example 4: A ladies purse is stolen containing a Nationwide debit card and a Nationwide cheque book for the same account. Cheques are fraudulently cashed and goods purchased using the debit card.

One crime (class NFIB5A). There is one account defrauded plus original theft of the purse.

NFIB5A Fraud by False Representation Cheque, Plastic Card and Online Bank Accounts (not PSP) Counting Rules (3 of 6)

Application of the Rule (continued)

Example 5: An offender in police force area A obtains a friend's credit card details without their knowledge. The offender orders goods by mail from three companies in police force areas B, C and D to be delivered to an address in police force area A. Mail order companies report crimes to the NFIB. The NFIB establish that the suspect is located in police force area A and pass the case to them.

One crime (class NFIB5A) to be recorded by police force area A. There is one account defrauded.

Exceptions to the Application of the Rule

Exceptions will only occur where the financial institution has refused to honour the transaction, and are therefore not the financial loser. Where victims contact police or Report Fraud to report an offence of fraud where the financial institution are not honouring the transaction, a crime should be recorded and the victim should not be referred to the financial institution.

Example 1: Goods are purchased from five different stores using stolen cheques from the same account. The bank refuses to honour two of them because the cheque guarantee limit has been exceeded.

Three offences of fraud (class NFIB5A) plus original theft of the cheques (class 49). There are three financial losers in this case, the bank for three cheques and the two different stores, each for one cheque.

Example 2: A cloned credit card is used to obtain goods from a number of different sources one of them being a mail order catalogue company who have had the credit protection removed from them so they are liable for any fraud.

Two offences of fraud (class NFIB5A). There are two financial losers in this case, the credit card company and the catalogue company.

Example 3: A local trader has attended the police station to report that the bank has notified him that an on line sale (card holder not present), has involved a cloned credit card and has not been honoured by them. He has been defrauded of £450.

One offence of fraud (class NFIB5A) should be passed to the NFIB by the Police. The local trader is the victim and should not be referred to the financial institution. The NFIB will count an additional crime (class NFIB5A) if there are any other fraudulent transactions on the account.

NFIB5A Fraud by False Representation Cheque, Plastic Card and Online Bank Accounts (not PSP) Counting Rules (4 of 6)

Exceptions to the Application of the Rule (continued)

Prepayment Cards

The same rules apply to prepayment cards as to any other plastic card. Crimes should only be recorded from cardholders if the Financial Institution is not honouring the payment (Exception to the application of the rules).

Example 1: A cloned prepayment card is used to purchase goods from a number of different stores.

One crime (class NFIB5A), one account reported direct to the NFIB by the financial institution.

Example 2: A prepayment card is stolen and then used on a number of occasions. The card issuer refuses to reimburse the account holder for two of the transactions.

Two offences of fraud (class NFIB5A) plus the original theft of the card (class 49). There are two financial losers in this case.

Conspiracy to Defraud: Do Not Count in Addition to Substantive Crime.

Principal Crime: see also General Rules Section F and Annex C.

If on the schedule of usage there is evidence of fraud by false representation and usage from ATM machines then count one offence of fraud by false representation only.

Example 1: A schedule of usage reported by the bank shows a number of ATM withdrawals and fraud by false representation offences committed on this account throughout many different force areas.

One crime fraud by false representation (class NFIB5A)

Withdrawing money from ATM's should be recorded under this class and not under theft from machines or meters (class 47)

Example 1: A stolen cash card is used to obtain money from four cash machines, one inside a supermarket and three outside separate branches of a bank.

One crime of other theft (class 49) covering theft of the card, plus one crime of fraud by false representation (class NFIB5A). There is one account defrauded.

NFIB5A Fraud by False Representation Cheque, Plastic Card and Online Bank Accounts (not PSP) Counting Rules (5 of 6)

Principal Crime: see also General Rules Section F and Annex C (continued).

Example 2: A stolen cash card is used in several different telephone boxes in the same area.

One crime of other theft (class 49) for the theft of the card plus one crime of fraud by false representation (class NFIB5A). There is one account defrauded.

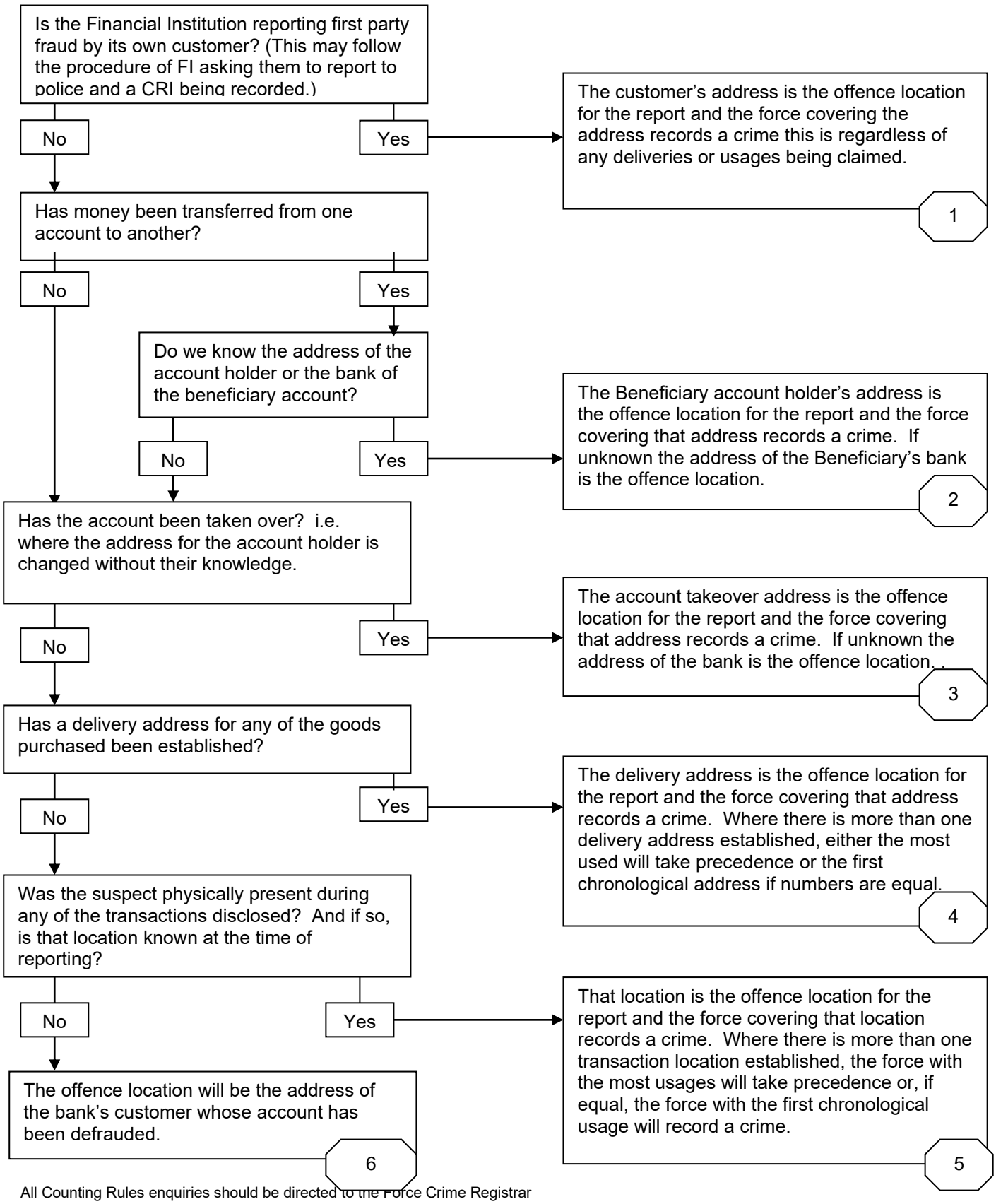
If an employee uses a company credit card beyond the permissions given to obtain goods or services, then the principal crime is Corporate employee Fraud and the venue is where they are employed.

Example 1: An employee uses their company credit card at a number of hotels he is staying at around the country on company business. The card is used as permitted by the company as well as in a non permitted manner to purchase gifts for his family. The unauthorised usage was reported to police at the same time.

One crime (class NFIB8A).

NFIB5A Fraud by False Representation Cheque, Plastic Card and Online Bank Accounts (not PSP) Counting Rules (6 of 6)

Fraud by False Representation – Cheque, Plastic Card and Remote Banking "Offence Location" Flowchart



NFIB5B Application Fraud (excluding Mortgages) Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Application Fraud

"Application fraud occurs when fraudsters open an account utilising fake or stolen documents in someone else's name."

The account is usually in respect to Hire Purchase or Loans.

Stolen documents may originate from a variety of sources such as theft of utility bills, they contribute along with counterfeit documents to creating a verifiable identity.

NFIB5B Application Fraud (excluding Mortgages) Counting Rules (1 of 2)

General Rule: **One crime for each account defrauded or attempted to be defrauded.**

Example 1: A person obtains a television from a store on interest free credit using details of another person he had obtained from a dustbin. No payments are made.

One crime (class NFIB5B)

Later on the same offender returns to the same store and obtains a DVD player on interest free credit. A new account is created for this from the same finance company. No payments are made.

Record an additional crime (class NFIB5B). One crime counted for each separate account.

Example 2: A person obtains documents from a dustbin and uses them to obtain goods at five different stores by setting up Hire Purchase Agreements. When the first payments are due it is discovered that the agreements were created using another person's identity.

Five crimes (class NFIB5B). One crime for each separate account.

Example 3: A person obtains documents from a dustbin and uses them to obtain goods at five different stores by setting up Hire Purchase Agreements. The Finance is all obtained from the same provider. Each agreement has a unique account number. When the first payments are due it is discovered that the agreements were created using another person's identity.

Five crimes (class NFIB5B). One crime for each separate account.

Example 4: A person obtains documents from a dustbin and uses them to obtain goods at two different stores of the same chain by setting up Hire Purchase Agreements. The Finance is all obtained from the same provider. The Finance provider in processing the two agreements is able to amalgamate them into one account. When the first payments are due it is discovered that the agreements were created using another person's identity.

One crime (class NFIB5B). One crime for each separate account.

NFIB5B Application Fraud (excluding Mortgages) Counting Rules (2 of 2)

Application of the Rule

Where a deposit is paid using a stolen cheque or plastic card then count an additional crime under class NFIB5A.

Example 1: A person obtains finance on a new car using false details. A deposit is paid on the vehicle using a stolen credit card.

One crime (class NFIB5B) and one crime (class NFIB5A).

NFIB5C Mortgage Related Fraud Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Mortgage Fraud

"Where an individual(s) generally involves one or more associates to fraudulently obtain one or more mortgages for profit and/or to assist in money laundering"

Mortgage fraud spans a wide spectrum of deceit from simple overstatement of income, through to systemic abuses by Organised Crime Groups. It can involve the work of fraudulent brokers/intermediaries, lawyers and accountants.

A surveyor or valuer can take a variety of actions in order to manipulate or falsely confirm these key areas to perpetrate a mortgage fraud either independently or in conjunction with other professionals and/or parties involved in the mortgage process.

NFIB5C Mortgage Related Fraud Counting Rules (1 of 1)

General Rule: One crime for each account defrauded or attempted to be defrauded, or each fraudulent application for a new mortgage account.

Example 1: An offender obtains three mortgages from different providers on three separate properties. He fails to disclose he has other mortgages and provides false details of employment.

Three crimes (class NFIB5C). Three separate accounts.

Example 2: A mortgagee obtains an additional mortgage loan on their property by providing false employment details.

One crime (class NFIB5C).

Example 3: A mortgagee applies for an additional mortgage loan on their property by exaggerating the value of their property and overstating their income. The Bank discovers this and the application fails.

One crime (class NFIB5C).

Application of the Rule

Mortgage fraud can be committed using professionals who are in collusion with the mortgagee. These professionals should be treated as aiding and abetting the fraudulent mortgage and no additional crime should be recorded in these circumstances.

Example 1: Mr A obtains an additional mortgage on his property by asking his brother in law who is a Chartered Surveyor to over value the property.

One crime (class NFIB5C)

Example 2: An offender purchases five properties to rent out. He uses false details and states that they are all for his own use to prevent paying the higher commercial mortgage rates. He then rents out the properties. His best friend is a solicitor who completes the conveyancing on all the properties for him.

Five crimes (class NFIB5C). There are five accounts.

NFIB5D Mandate Fraud Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Mandate Fraud

"Mandate fraud is where fraudsters obtain details of direct debits, standing orders or account transfer details and amend them to transfer monies to other accounts"

NFIB5D Mandate Fraud Counting Rules (1 of 1)

General Rule: One crime for each account defrauded or attempted to be defrauded.

Example 1: A company is contacted by someone purporting to be from their suppliers and is told that they have changed their bank and could they change their standing order to reflect this. As a result the standing order is amended to the account that was provided. The next month they are contacted by the genuine supplier asking what has happened with the monthly payment? The fraud is thus uncovered.

One crime (class NFIB5D)

Example 2: Sam receives a letter in the post that appears to come from a company supplying a monthly magazine to him. It provides details of a new bank account and asks him to change his payment details to reflect this. He goes on line and amends the account details as instructed. The following month when his magazine does not arrive he contacts the publisher and is told that because his payment was cancelled he no longer has a subscription for the magazine. His standing order was paid to the new account.

One crime (class NFIB5D)

Principal Crime: see also General Rules Section F and Annex C.

If there is evidence of unlawful access to a computer (computer Hacking) in order to change the payment details, then count one offence of Mandate Fraud only.

Example 1: An online bank account is hacked into by a fraudster and all the monthly payment details are altered so that the payments are transferred to the fraudsters account. Twelve separate payments to different payees are affected.

One crime (class NFIB5D). There is one account defrauded.

NFIB5E Dishonestly retaining a wrongful credit Classification (1 of 1)

053/32 (V)	Dishonestly retaining a wrongful credit. Theft Act 1968 Sec 24A (as added by Theft (Amendment) Act 1996 Sec 2 Fraud Act 2006).	053/32 Dishonestly retaining a wrongful credit (v) Theft Act 1968 Sec 1

Definition – Legal: Dishonestly Retaining a Wrongful Credit

Theft Act 1968 Sec 24a

(1)A person is guilty of an offence if—
(a) a wrongful credit has been made to an account kept by him or in respect of which he has any right or interest;
(b) he knows or believes that the credit is wrongful; and
(c)he dishonestly fails to take such steps as are reasonable in the circumstances to secure that the credit is cancelled.

(2A) A credit to an account is wrongful to the extent that it derives from –

(a) theft
(b) blackmail
(c) fraud (contrary to section 1 of the Fraud Act 2006); or
(d) stolen goods

(2) References to a credit are to a credit of an amount of money.

Definition – Legal: Theft

Theft Act 1968 Sec 1 (1)

“A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it”. The terms in this basic definition are amplified in Sections 2-6 of the Theft Act.

NFIB5E Dishonestly retaining a wrongful credit Counting Rules (1 of 1)

General Rule: **One crime for each victim.**

Example 1: A' pays stolen money into his account and transfers the funds from that account to an account owned by 'B', a wrongful credit has been made to 'B's account, and B may commit this offence if he dishonestly retains it, knowing or believing it to be derived from one or other of those offences.

One crime (class NFIB5E).

NFIB6A Insurance Related Fraud Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Insurance Fraud

"Insurance fraud is where policy holders obtain money or replacement goods through false insurance claims or obtain policies by furnishing incorrect details"

Reported to the NFIB by the insurance company. Involves any insurance policy, e.g. car, household, or travel.

NFIB6A Insurance Related Fraud Counting Rules (1 of 1)

General Rule: **One crime for each policy defrauded or attempted to be defrauded.**

Example 1: A householder claims on her home contents insurance that a number of items of property have been stolen during a burglary offence that was reported to the police. Following an investigation by an insurance assessor the householder admits that it is a false claim, there was no burglary and that the window was smashed by them when they were locked out.

One crime (class NFIB6A). The original recorded burglary can be cancelled under General Rules section C.

Example 2: A householder claims on her home contents insurance that a number of items of property have been stolen during a burglary offence that was reported to the police. Following an investigation by an insurance assessor the householder admits that two of the items claimed for had never been stolen and in fact they had never owned.

One crime (class NFIB6A).

Example 3: A motorist with only third party car insurance, crashes his vehicle. Realising that he is liable for the damage caused, he reports to police that the car has been stolen and leaves the scene of the accident. He later claims on the insurance. Following investigation he admits that the car was not stolen and he had crashed it.

One crime (class NFIB6A). The original recorded theft of motor vehicle can be no crimed under General rules section C.

Example 4: A father, realising that his 17year old son will not obtain car insurance, takes out a policy of insurance by falsely stating that he owns his son’s vehicle and is the main driver of the vehicle with his son as a named driver.

One crime (class NFIB6A).

Example 5: A householder claims on her household, travel and motor insurance policies for the theft of a camera and lenses valued at £2000. She has never owned a camera.

Three crimes (class NFIB6A). There are three separate policies.

NFIB6B Insurance Broker Fraud Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Insurance Brooker Fraud

Insurance broker fraud is where victims obtain insurance cover from a broker or someone purporting to be a broker. When a claim is made or the policy checked, they discover that they are not insured, or the cover that they have paid for and thought they had is not what they have.

NFIB6B Insurance Broker Fraud Counting Rules (1 of 1)

General Rule: **One crime for each victim**

Example 1: Mrs ‘A’ attends a brokers office and obtains insurance for her vehicle which she pays for in cash. Three weeks later following a car accident she claims on her car insurance and discovers that she does not have insurance the premium was never paid by the broker.

One crime (class NFIB6B).

Example 2: Following a burglary Mr ‘A’ claims on his house insurance that he had obtained and paid for via an online broker. He discovers that the insurance certificate is false and the on line site has been shut.

One crime (class NFIB6B).

Application of the rule

Count one crime for each victim on victim confirmation.

Example 1: Following a police investigation into an Insurance Brokers practice. Police trace twelve people who all confirm that they had obtained insurance policies and paid cash at the brokers for them. The insurance certificates they were given relate to a bogus insurance company.

Twelve crimes (class NFIB6B).

Principal crime: see also General Rules Section F and Annex C.

Insurance Broker fraud will be the principal crime over Corporate Employee Fraud (class NFIB8A).

Example 1: Following a police investigation into a member of staff at an Insurance Brokers practice. Police trace twelve people who have all obtained insurance policies and paid cash at the brokers for them. The monies paid have never been passed to the insurers but have been kept by one of the staff.

Twelve crimes (class NFIB6B).

NFIB7 Telecom Industry Fraud (Misuse of Contracts) Classification (1 of 1)

053/40(pt) (V)	Fraud by false representation Fraud Act 2006 Sec 2.	053/46 (V)	Obtaining services dishonestly Fraud Act 2006 Sec 11

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Legal: Obtaining Services Dishonestly

Fraud Act 2006 Sec 11

"… if he obtains services for himself or another by a dishonest act and the services were made on the basis that payment has been, is being or will be made for or in respect of them or he obtains them without payment having been made for or in respect of them or without payment having been made in full, and when he obtains them he knows they are being made available on the basis that payment will be made for them…."

Definition - Telecom Industry Fraud (Misuse of Contracts)

"This is where contracts are obtained by false representation from service providers either by using false details or stolen documents/credit cards or with no intention of paying the contract."

This also includes internet services.
Reported to the NFIB by the industry.

NFIB7 Telecom Industry Fraud (Misuse of Contracts) Counting Rules (1 of 1)

General Rule: **One crime for each contract defrauded or attempted to be defrauded.**

Example 1: A suspect obtains a mobile phone on a twelve month contract using a dormant bank account. The phone is then used for three months with no payments being made before the phone is cut off by the service provider. There were no funds in the account and never any intention to pay the monthly contract.

One crime (class NFIB7).

Example 2: A short stay tenant obtains an internet package from an ISP using false details knowing that he will no longer be there in a months time when the first bill arrives.

One crime (class NFIB7).

Application of the Rule

Where phone contracts are obtained using stolen credit cards count one crime under this class in addition to the crime recorded under the cheque and credit card fraud. If no contract is obtained then treat under cheque and credit card.

Example 1: A suspect obtains a mobile phone on a twelve month contract using a cloned credit card. The phone is then used for three months before the phone is cut off by the service provider.

One crime (class NFIB7) and one crime (class NFIB5A) if not already recorded.

Example 2: A suspect enters a phone shop and purchases a new handset for his sim card using a cloned credit card.

One crime (class NFIB5A).

NFIB8A Corporate Employee Fraud Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition – Corporate Employee Fraud

This is where employees or ex employees obtain property, or greater remuneration through fraud. It also covers the misuse of corporate cards and expense systems.

NFIB8A Corporate Employee Fraud Counting Rules (1 of 2)

General Rule: **One crime for each offender.**

Example 1: Employee, after leaving company, obtains petrol from a garage by signing the usual documents at the garage as if still employed by company thereby obtaining petrol on former employer's account.

One crime (class NFIB8A).

Example 2: An employee meets his girlfriend at a restaurant for lunch and then submits an expenses claim for lunch meeting a client to cover the cost of the meal with his girlfriend.

One crime (class NFIB8A).

Example 3: An employee in accounts creates a false employee within a large company and directs all the wage payments to one of his accounts.

One crime (class NFIB8A).

Example 4: Twelve employees claim overtime for working on a Sunday. The following Sunday the Company Director turns up on site and finds the site is closed. He calls police when he finds that the twelve employees have claimed overtime for working this Sunday. When questioned, the employees admit that they have never worked on a Sunday, but claim as though they have.

Twelve crimes (class NFIB8A).

Application of the Rule

Finished Incident: see also General Rules Section E.

Example 1: Employee, after leaving company, obtains petrol from a garage on five separate occasions by signing the usual documents at garage as if still employed by company thereby obtaining petrol on former employer's account. They are all reported at the same time.

One crime (class NFIB8A).

Example 2: Employee, after leaving company, obtains petrol from a garage by signing the usual documents at garage as if still employed by company thereby obtaining petrol on former employer's account. During the investigation Police discover that the employee had filled up the car on four previous occasions.

One crime (class NFIB8A).

NFIB8A Corporate Employee Fraud Counting Rules (2 of 2)

Application of the Rule (continued)

Example 3: Employee, after leaving company, obtains petrol from a garage by signing the usual documents at the garage as if still employed by company thereby obtaining petrol on former employer's account. Following the initial report the company discover that the employee had filled up the car on four previous occasions and report these offences.

One crime (class NFIB8A). No additional reports are required, the finished incident rule applies.

Example 4: Employee, after leaving company, obtains petrol from a garage by signing the usual documents at garage as if still employed by company thereby obtaining petrol on former employer's account. Before Police investigate the crime, the company report that since the original report the ex employee has filled the car up again using the company account.

One crime (class NFIB8A) in addition to the original recorded crime. Further offence committed after the recorded offence.

Theft Employee or Corporate Employee fraud

Corporate Employee Fraud (class NFIB8A) should only be recorded where there is a false representation. Where property is simply stolen then the crime should be recorded under Theft Employee (class 41).

Example 1: An employee steals a quantity of stationary from her employer and takes it home.

One crime (class 41).

Principal Crime: see also General Rules Section F and Annex C.

Where employees have stolen property (class 41) and also misappropriated assets by fraud then the principle crime is Corporate Employee Fraud (class NFIB8A).

Note: Please see Class NFIB6A if the offence relates to Insurance policies.

Example 1: An employee is caught stealing a laptop computer belonging to the company from an office at the company Headquarters. Whilst interviewed for this offence he admits that he has been submitting false mileage claims for the last six months.

One crime (class NFIB8A).

Example 2: Following a police investigation into a member of staff at an Insurance Brokers practice. Police trace twelve people who have all obtained insurance policies and paid cash at the brokers for them. The monies paid have never been passed to the insurers but have been kept by one of the staff.

Twelve crimes (class NFIB6A).

NFIB8B Corporate Procurement Fraud Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition – Corporate Procurement Fraud

This offence is where excess goods are ordered and then sold on by the offender or goods of an inferior quality are delivered to those paid for with the offenders pocketing the difference.

NFIB8B Corporate Procurement Fraud Counting Rules (1 of 1)

General Rule: One crime for each employee or group of employees.

Example 1: The site foreman orders kitchens for twelve properties when the company is only building ten houses. The two additional kitchens are then sold on by the foreman who keeps the money.

One crime (class NFIB8B).

Example 2: A large company is updating it's IT and an order is placed for 156 new desk top computers. 150 desk top machines are replaced with the new machines and the project team of six each take home a brand new computer. The company does not supply desk top computers for use at home.

One crime (class NFIB8B).

Application of the Rule

Where an employee is in collusion with people outside the company, treat people in collusion as aiding and abetting the employee.

Example 1: Jones phones his friends company Bill, for delivery of a quantity of high quality four foot shrubs for a development his company is undertaking. He tells him to invoice them for more expensive five foot shrubs as no one will know the difference. Bill and Jones then share the difference.

One crime (class NFIB8B).

NFIB9 Business Trading Fraud Classification (1 of 2)

051/01 (V)	False statements by company directors etc. Theft Act 1968 Sec 19	051/04 (V)	Give false information knowingly or recklessly when applying for a Confidentiality Order etc. Companies Act 1985
051/03 (V)	Fraudulent trading Companies Act 1985 Sec 458	051/05 (S)	Knowingly/recklessly make false misleading statement in S116 request to inspect/copy register. Companies Act 2006 Sec119.
053/45 (V)	Fraudulent Trading by Sole Trader Fraud Act 2006 Sec 9		
051/03 (V)	Other frauds by company directors etc. Companies Act 1985 Sec 70(1)	051/06 (S/V)	Carry on business of company with intent to defraud creditors or for other fraudulent purpose. Companies Act 2006 Sec 993.

Definition - Legal: False Statements by Company Directors etc

Theft Act 1968 Sec 19

"... an officer of a body corporate or unincorporated association (or person purporting to act as such), with intent to deceive members or creditors of the body corporate or association about its affairs, publishes or concurs in publishing a written statement or account which to his knowledge is or may be misleading, false or deceptive in a material particular ..."

The law also makes provision for organisations managed by its members.

Definition - Legal: Fraudulent Trading

Companies Act 1985 Sec 458

"... Any business of a company is carried on with intent to defraud creditors of the company or creditors of any other person, or for any fraudulent purpose ... "

This applies whether or not the company has been, or is in the course of being, wound up.

Definition - Legal: Fraudulent Trading by Sole Trader

Fraud Act 2006 Sec 9

“A person is guilty of an offence if he is knowingly a party to the carrying on of a business with intent to defraud creditors of any person or for any other fraudulent purpose…”

NFIB9 Business Trading Fraud Classification (2 of 2)

Definition - Long Firm Fraud

“Long Firm Fraud is normally where an apparently legitimate business is set up with the purpose to defraud its suppliers and customers after a relatively long period of time.”

The business develops a decent credit history to win the trust of suppliers; this is achieved by placing numerous small orders with wholesalers accompanied by prompt payment. The fraudsters then place several larger orders with the businesses with which they have established a good credit history. Once they receive the goods, the criminals will promptly disappear and sell the goods on from various trading places.

Definition - Short Firm Fraud

“Short Firm Fraud is normally where an apparently legitimate business is set up with the purpose to defraud its suppliers and customers after a relatively short period of time.”

This is similar in all aspects to long firm fraud, however over a shorter time span with no pattern to establish any form of credit history or creditability.

The companies involved have no day-to-day trading activity, not even a cash- generating front. Goods are obtained on credit and delivered to third party addresses, often located at multi occupancy trading estates. The goods are sold on for cash therefore creating no document trail.

NFIB9 Business Trading Fraud Counting Rules (1 of 2)

General Rule: One crime for each specific, intended or identifiable creditor defrauded.

Example 1: Three creditors have been intentionally defrauded by a company director's false statement.

Three crimes (class NFIB9).

Application of the Rule

Creditors can be purchasers and suppliers.

Example 1: A company is set up to supply diamond cluster rings. They advertise the ring at an amazing cost on the back of a Sunday supplement, and order an initial 100 rings from a supplier. They receive orders for 100 rings and dispatch these. The next week they run the advert more widely and receive orders and payment for 1000 rings from 900 customers. The director takes the money and disappears. No rings are ordered or dispatched and no attempt is ever made to pay the supplier for the original 100 rings.

There are 901 crimes (class NFIB9).

Example 2: The director of a long established photography shop is coming up to retirement. He also owns a separate photography e mail business. He orders significant new stock for his shop from well established suppliers and sells all of this stock through his web company. When the stock runs out he continues to take orders for cameras and accepts payments from 200 customers for high end cameras. After two weeks he moves abroad having taken all the payments from the 200 purchasers with him and failing to pay any of the suppliers for the stock he purchased. The loss to purchasers is £200,000 and the 15 separate suppliers are owed £500,000.

There are 215 crimes (class NFIB9).

If several directors' names have been used in defrauding a creditor, count separately only where a director is a separate person (rather than a mere alias) and has been acting independently of the others.

Example 1: Two directors of a company have been involved in defrauding a creditor.

One crime (class NFIB9).

Example 2: A director intentionally defrauds four building societies through fraudulent trading practices under several different names.

Four crimes (class NFIB9).

If no specific intended creditor, count one crime for each creditor identified as being defrauded. If none can be identified, count one crime for each director acting independently.

NFIB9 Business Trading Fraud Counting Rules (2 of 2)

Application of the Rule (continued)

Example 1: A company issues a prospectus containing false information with the intent of misleading investors and creditors generally, but no-one in particular.

(i) The police identify three creditors who have been defrauded.

Three crimes (class NFIB9).

(ii) The police cannot identify any creditors who have been defrauded.

One crime (class NFIB9).

For club officials defrauding members, count each identifiable member defrauded.

Example 1: A club treasurer persuades three other club officials and five members to donate money to the club, by making a false statement about the club's finances.

Eight crimes (class NFIB9).

Finished Incident: see also General Rules Section E.

Example 1: A company director intentionally defrauds a creditor on many occasions before he is discovered and reported to the police.

One crime (class NFIB9).

NFIB10 False Accounting Classification (1 of 1)

052/01 (V) False Accounting.
Theft Act 1968 Sec 17.
Protection of Depositors Act 1963 Sec 15.

052/02 (V) Failure to keep proper accounting records.
Companies Act 1985 Sec 221(5).

052/03 (V) Authorising the failure to keep proper accounting records.
Companies Act 1985 Sec 221(5)(6).

052/04 (V) Permitting the failure to keep proper accounts.
Companies Act 1985 Sec 221(5)(6).

052/05 (V) Failing to secure preservation of counting records.
Companies Act 1985 Sec 222(6).

052/06 (V) Failing to keep accounting records open to inspection.
Companies Act 1985 Sec 222 (4)

052/07 (S) Fail to comply with provision of S386 re keeping of accounting records
Companies Act 2006 Sec 387.

052/08 (S) Fail to comply with requirements of S388 re place of keeping of accounting records and accuracy.
Companies Act 2006 Sec 389.

052/09 (S) Fail to comply with S414 requirements re approval and signing of accounts.
Companies Act 2006 Sec 414.

052/10 (S) Fail to comply with requirements re approval and signing of abbreviated accounts.
Companies Act 2006 Sec 450.

052/11 (S) Fail to provide up-to-date information on on people with Significant Control Register (PSC).
Companies Act 2006 Sec 790D (1) (a) (b) (2) E (2) F(2)

052/12 (S) Offences in connection with request for disclosure of information from people with significant control. (PSC).
Companies Act 2006 Sec 790 R(1) (2) (3) (a) (b) (i)

Definition - Legal: False Accounting

Theft Act 1968 Sec 17(1)

"... A person dishonestly with a view to gain for himself or another or with intent to cause loss to another -

(a) destroys, defaces, conceals or falsifies any account or any record or document made or required for any accounting purpose;

or

(b) in furnishing information for any purpose produces or makes use of any account, or any such record or document as aforesaid, which to his knowledge is or may be misleading, false or deceptive in a material particular ..."

Section 17(2) states the circumstances whereby making an entry in an account or omission of an item in an account can be treated as falsification.

NFIB10 False Accounting Counting Rules (1 of 1)

General Rule: **One crime for each specific, intended or identifiable victim.**

Example 1: A person is reported to the police for falsifying accounting records, with intent to cause loss to two other employees.

Two crimes (class NFIB10).

Application of the Rule

If no specific intended creditor, count one crime for each creditor identified as being defrauded. If none can be identified, count one crime for each director acting independently.

Example 1: A person falsifies accounts to cause general loss, but with no-one particular in mind.

(i) Five shareholders report having suffered loss as a result of the false statement.

Five crimes (class NFIB10).

(ii) No-one is identified as having been defrauded.

One crime (class NFIB10).

Principal Crime: see also General Rules Section F and Annex C.

If a person undertakes false accounting in order to steal money or property, then the principal crime is corporate employee fraud.

Example 1: An employee is reported to the police for false accounting in order to steal money.

One crime of corporate employee fraud (class NFIB8A).

Example 2: As above, but there is no evidence that money or goods have actually been stolen.

One crime of false accounting (class NFIB8A).

NFIB11 Bankruptcy and Insolvency Classification (1 of 2)

055/01 (S) Fraud etc in anticipation of winding up.
Insolvency Act 1986 Sec 206(1).

055/01 (S) Privity to fraud in anticipation of winding up, fraud, or privity to fraud, after commencement of winding up.
Insolvency Act 1986 Sec 206(2).

055/01 (S) Knowingly taking in pawn or pledge, or otherwise receiving, company property.
Insolvency Act 1986 Sec 206(4).

055/01 (S) Transactions in fraud of creditors.
Insolvency Act 1986 Sec 207.

055/01 (S) Misconduct in course of winding up.
Insolvency Act 1986 Sec 208.

055/01 (S) Falsification etc of company's books.
Insolvency Act 1986 Sec 209.

055/01 (S) Material omissions from statement relating to company's affairs.
Insolvency Act 1986 Sec 210.

055/01 (S) False representations or fraud for purpose of obtaining creditors' consent to a agreement in connection with winding up.
Insolvency Act 1986 Sec 211.

055/01 (S) Contravening restrictions on re-use of name of company in insolvent liquidation. Insolvency Act 1986 Sec 216(4).

055/01 (S) Bankrupt failing to disclose property or disposals to official receiver or trustee.
Insolvency Act 1986 Sec 353(1).

055/01 (S) Bankrupt failing to deliver property to, or concealing property from, official receiver or trustee.
Insolvency Act 1986 Sec 354(1).

055/01 (S) Bankrupt removing property which he is required to deliver to official receiver or trustee.
Insolvency Act 1986 Sec 354(2).

055/01 (S) Bankrupt failing to account for loss of substantial part of property.
Insolvency Act 1986 Sec 354(3).

055/01 (S) Bankrupt failing to deliver books, papers or records to official receiver or trustee.
Insolvency Act 1986 Sec 355(1).

055/01 (S) Bankrupt concealing destroying etc books, papers or records, or making false entries in them.
Insolvency Act 1986 Sec 355(2).

055/01 Bankrupt disposing of, or altering, books, papers or records relating to his estate or affairs.
Insolvency Act 1986 Sec 355(3).

055/01 (S) Bankrupt making material omission in statement relating to his affairs.
Insolvency Act 1986 Sec 356(1).

055/01 (S) Bankrupt making false statement, or failing to inform trustee, where false debt proved.
Insolvency Act 1986 Sec 356(2).

055/01 (S) Bankrupt fraudulently disposing of property.
Insolvency Act 1986 Sec 357.

055/01 (S) Bankrupt absconding with property he is required to deliver to official receiver or trustee.
Insolvency Act 1986 Sec 358.

055/01 (S) Bankrupt disposing of property obtained on credit and not paid for.
Insolvency Act 1986 Sec 359(1).

055/01 (S) Obtaining property in respect of which money is owed by a bankrupt.
Insolvency Act 1986 Sec 359(2).

055/01 (S) Bankrupt obtaining credit or engaging in business without disclosing his status or name in which he was made bankrupt.
Insolvency Act 1986 Sec 360(1).

055/01 (S) Person made bankrupt in Scotland or Northern Ireland obtaining credit etc. in England and Wales.
Insolvency Act 1986 Sec 360(3).

055/01 (S) Bankrupt failing to keep proper accounting records.
Insolvency Act 1986 Sec 361(1).

055/01 (S) Bankrupt increasing extent of insolvency by gambling.
Insolvency Act 1986 Sec 362.

055/01 (S) Acting as insolvency practitioner when not qualified.
Insolvency Act 1986 Sec 389.

055/02 (S) Person contravening company directors disqualification order.
Company Directors Disqualification Act 1986 Sec 1 & 13.

055/03 (S) Disqualified person managing company.
Company Directors Disqualification Sec 8 & 13.

055/04 (S) Undischarged bankrupt acting as a director.
Company Directors Disqualification Sec 11(1).

055/05 (S) Undischarged bankrupt taking part in or being concerned in the promotion, formation or management of a company.
Company Directors Disqualification Sec 11(1).

NFIB11 Bankruptcy and Insolvency Classification (2 of 2)

055/06 (S) Make false representations/omissions in connection with (application for) debt relief order. Insolvency Act 1986 as inserted by Sch.1 Tribunals, Courts and Enforcement Act 2007 S.251O (1),(2),(4b).

055/07 (S) Fail to comply with duty in connection with (application for) debt relief order. Insolvency Act 1986 as inserted by Sch.1 Tribunals, Courts and Enforcement Act 2007 S.251O (2a) (4a)

055/08 (S) Fail to deliver records re debt relief order. Insolvency Act 1986 as inserted by Sch.1 Tribunals, Courts and Enforcement Act 2007 S.251P.

055/09 (S) Subject of debt relief order fraudulently dispose of property. Insolvency Act 1986 as inserted by Sch.1 Tribunals, Courts and Enforcement Act 2007 S.251Q.

055/10 (S) Subject of debt relief order dispose of property not paid for by them or obtain property in respect of which money is owed. Insolvency Act 1986 as inserted by Sch.1 Tribunals, Courts and Enforcement Act 2007 S.251R.

055/11 (S) Person in respect of whom a debt relief order is made obtain credit/engage in business without disclosing status/name. Insolvency Act 1986 as inserted by Sch.1 Tribunals, Courts and Enforcement Act 2007 S.251S.

055/12 (S) Make a false representation fraudulently do / omit to do a thing for the purpose of obtaining approval of creditors Insolvency Act 1986 Sec 262A

NFIB11 Bankruptcy and Insolvency Offences Counting Rules (1 of 1)

General Rule: One crime for each offender or group of offenders.

Application of the Rule

Crimes against specific creditors: One crime for each specific and intended creditor that can be identified. If there is no specific creditor, count one crime for each offending company official acting independently.

Example 1: A trustee under a deed of arrangement makes preferential payments to five creditors.

Five crimes (class NFIB11).

Example 2: Three members of a company collude in concealing key information to a liquidator when a company is being wound up.

One crime (class NFIB11).

Crimes by a Bankrupt: One crime for each bankrupt.

Example 1: A bankrupt is reported to the police committing a variety of Insolvency Act crimes.

One crime (class NFIB11).

Finished Incident: see also General Rules Section E.

Example 1: A bankrupt is bailed and subsequently reported for committing further Insolvency Act crimes.

Two crimes (class NFIB11). One for original series, plus one for those committed on bail.

Principal Crime: see also General Rules Section F and Annex C.

Example 1: A bankrupt illegally continues trading under different names and obtains money and goods from ten customers by deception.

Ten crimes of fraud by false representation (class NFIB9).

NFIB12 Passport Application Fraud Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Passport Fraud

"Passport fraud occurs where fraudsters obtain or try to obtain a United Kingdom Passport by false representation to the passport Agency."

This only applies to United Kingdom passports reported to the NFIB by the passport agency.

NFIB12 Passport Application Fraud Counting Rules (1 of 1)

General Rule: **One crime for each fraudulent application.**

Example 1: The passport office report that they have received a passport application using a forged birth certificate. No passport is issued.

One crime (class NFIB12).

Example 2: The passport office report that they have received three separate applications from the same offender for passports over the past year. They are all reported at the same time.

Three crimes (class NFIB12). Three separate applications.

Application of the Rule

This class only deals with fraudulent United Kingdom Passport Applications. It does not deal with other Nations passports or with Forged or counterfeit passports. The Passport Agency should be consulted to ensure that the application is false and to report the offence to the NFIB.
Forged/counterfeit passports should be dealt with under class 61 Other Forgery.

Crimes in this class should be counted in addition to any other notifiable offence disclosed.

Example 1: A suspect is arrested after using a United Kingdom passport obtained by a fraudulent application to obtain a fraudulent hire purchase agreement on a new car.

One crime (class NFIB12) and one crime (class 54).

Example 2: A suspect is stopped by police with a United Kingdom passport obtained by a fraudulent application and false utility bills. He admits that he was intending to use the documents to apply for a store card and obtain goods from the store.

One crime (class NFIB12) and one crime (class 33A). Having articles for use in fraud.

NFIB13 Department of Work and Pensions (DWP) Fraud Classification (1 of 1)

053/40(pt) (V) Fraud by false representation
Fraud Act 2006 Sec 2.

053/46 (V) Obtaining services dishonestly
Fraud Act 2006 Sec 11
(implementation 1/1/2000)

053/33 (V) Dishonest representation for obtaining benefit etc.
Social Security Administration Act 1992 Sec 111A.

053/36 (V) Fraudulent evasion of contributions.
Social Security Act 1998 Sec 61

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Legal: Obtaining Services Dishonestly

Fraud Act 2006 Sec 11

"… if he obtains services for himself or another by a dishonest act and the services were made on the basis that payment has been, is being or will be made for or in respect of them or he obtains them without payment having been made for or in respect of them or without payment having been made in full, and when he obtains them he knows they are being made available on the basis that payment will be made for them…."

DWP FRAUD

Reported to the NFIB by DWP.

NFIB13 Department of Work and Pensions (DWP) Fraud Counting Rules (1 of 1)

General Rule: **One crime for each fraudulent benefit application or tax credit**

Example 1: John claims benefits because he is out of work. In fact he is working as a labourer for cash in hand.

One crime (class NFIB13).

Example 2: Mary is claiming child tax credits for her three children. She has failed to declare that she has another job that takes her combined salary above the thresholds for claiming the benefits.

One crime (class NFIB13).

Application of the Rule

Count one crime for each separate application. It is not necessary for the application to be successful merely that it has been applied for. Where an offender has made claims in relation to different benefits count one crime for each separate benefit application. Where more than one person has claimed for the same benefit (couples or partners for example), treat as acting together and one application.

Example 1: John has claimed for three separate benefits. He has applied using false details. He in fact is already working as a cab driver in another name.

Three crimes (class NFIB13).

Example 2: Mary and John jointly claim for two different benefits. They fail to disclose their true financial position which would have made them ineligible for the benefits.

Two crimes (class NFIB13).

Finished Incident: see also General Rules Section E.

The general rule is one crime per application and not per payment. Where an offender has falsely claimed for a payment and then received regular payments in regard to the benefit count one crime only for the application and not one crime for each payment, unless subsequent applications have been fraudulently completed to continue the payments.

Example 1: Mary and John jointly claim for two different benefits. They fail to disclose their true financial position which would have made them ineligible for the benefits. They have received twelve payments.

Two crimes (class NFIB13).

Example 2: John has falsely claimed for a benefit he was not entitled to. He has received weekly payments for one year. After a year he has had to complete another application to continue the benefit. Whilst making checks on this further application, the fraud was discovered and no further payments made.

Two crimes (class NFIB13). There are two applications.

NFIB14 Fraudulent Applications for Grants from Government Funded Organisations Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition – Fraudulent Grants

This is where Government funded Organisations have provided grants, based on false representations or where they have received grant applications that contain false representations and so no grant was paid.

Definition - Government Funded Organisations

Government funded organisations are organisations set up to distribute funding on behalf of the government. They are not charities.

NFIB14 Fraudulent Applications for Grants from Government Funded Organisations Counting Rules (1 of 1)

General Rule: **One crime for each grant application.**

Example 1: Ofgem has provided funding for a householder to install solar heating as a result of a grant application. The applicant receives the money and pays it into his account when he submits receipts for the installation. It is then discovered that the receipts are false and no work was undertaken.

One crime (class NFIB14).

Example 2: Ofgem has received an application for a grant of £10,000 for a project. In checking the application the Ofgem finds that the applicant has used false details and the company who were to undertake the work does not exist. No grant was paid.

One crime (class NFIB14).

NFIB15 HM Revenue and Customs Fraud (HMRC) Classification (1 of 1)

053/40(pt) (V) Fraud by false representation
Fraud Act 2006 Sec 2.

053/46 (V) Obtaining services dishonestly
Fraud Act 2006 Sec 11

053/56 (S) Cheating the Public Revenue.
Common Law.

053/56 (S) Making false statements tending to prejudice Her Majesty the Queen and the Public Revenue with intend to defraud her.
Common Law.

053/56 (S) Acting with intent to defraud and to the prejudice of Her Majesty the Queen and the Public Revenue.
Common Law.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Legal: Obtaining Services Dishonestly

Fraud Act 2006 Sec 11

"… if he obtains services for himself or another by a dishonest act and the services were made on the basis that payment has been, is being or will be made for or in respect of them or he obtains them without payment having been made for or in respect of them or without payment having been made in full, and when he obtains them he knows they are being made available on the basis that payment will be made for them…."

HMRC fraud

Reported to the NFIB by HMRC.

NFIB15 HM Revenue and Customs Fraud (HMRC) Counting Rules (1 of 1)

General Rule: **One crime for each fraudulent return**

Example 1: John submits a Tax return to HMRC that he knows contains a number of false statements to lower his tax burden.

One crime (class NFIB15).

Application of the Rule

Count one crime for each separate tax return. It is not necessary for the return to be successfully processed merely that it has been submitted. Where an offender has made returns in relation to different taxes count one crime for each separate return.

Example 1: John has submitted three separate VAT returns that he knows contains false information to HMRC.

Three crimes (class NFIB15).

Example 2: Mary has submitted an Income Tax return and also a VAT return that she knows contains false information.

Two crimes (class NFIB15).

NFIB16A Pension Fraud by Pensioners (or their Estate) Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition – Pension Fraud by Pensioners (or their estate)

This is where the pension provider is defrauded by the pensioner or more usually by the pensioner's estate following their death.

NFIB16A Pension Fraud by Pensioners (or their Estate) Counting Rules (1 of 1)

General Rule: **One crime for each pension defrauded**

Example 1: John and his wife emigrated abroad on his retirement. On John's death his wife decides not to inform the pension provider of her husbands death so that she continues to receive full payments instead of the lesser widows pension. The pension provider only discovers this five years later.

One crime (class NFIB16A)

Example 2: John and his wife emigrated abroad on his retirement. On John's death his wife decides not to inform the pension providers of her husbands death so that she continues to receive full payments instead of the lesser widows pension. John has two separate pensions. The pension providers only discover this some time later.

Two crimes (class NFIB16A)

NFIB16B Pension Fraud committed on Pensioners Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition – Pension Fraud committed on Pensioners

This is where the pensioner is the victim of fraud on their pension. It is usually committed by Trustees or pension funds inappropriately using the pension fund.

NFIB16B Pension Fraud committed on Pensioners Counting Rules (1 of 1)

General Rule: **One crime for each offender or group of offenders.**

Example 1: A trustee of a pension fund moves funds from the trust fund into there own account by informing the fund that they have permission from the other trustees, who know nothing about the transaction.

One crime (class NFIB16B)

Example 2: The trustee's of a pension fund decide that they can transfer funds into their own accounts with little risk of being caught as the pension is not due to mature for another 25 years. They falsely complete documents to transfer the money.

One crime (class NFIB16B)

Example 3: Two trustee's acting independently at different times have transferred funds from a pension without the knowledge or agreement of the other trustee's by falsely representing that they had full agreement.

Two crimes (class NFIB 16B)

NFIB16C Pension Liberation Fraud Classification (1 of 1)

53/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition – Pension Liberation Fraud

This is where by fraud a pensioner is persuaded to 'liberate' their pension early for a large cash sum. The payment is considerably smaller than they expected because of fees and taxes.

NFIB16C Pension Liberation Fraud Counting Rules (1 of 1)

General Rule: **One crime for each pension liberated.**

Example 1: Joe is contacted by a company who states that they can obtain the value of his pension now for a small fee. He is going through a particularly hard time and agrees. His significant pension is liberated and he receives a cheque for only a quarter of it's value. The rest going on fee's and charges.

One crime (class NFIB16C)

Example 2: Joe is contacted by a company who states that they can obtain the value of his pensions now for a small fee. He is going through a particularly hard time and agrees. He has two significant pension that are liberated and he receives a cheque for only a third of there value. The rest going on fee's and charges.

Two crimes (class NFIB16C)

NFIB17 Other Regulatory Fraud Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

053/46 Obtaining services dishonestly
(V) Fraud Act 2006 Sec 11

053/06 Taking marks from public stores.
(V) Public Stores Act 1875 Sec 5.

053/11 Fraudulently printing, mutilating or
(V) re-issuing stamps.
Stamp Duties Management Act 189 Sec 13.

053/13 Frauds by farmers in connection with
(V) agricultural charges.
Agricultural Credits Act 1928 Sec 11.

053/15 Suppression etc of documents
(V) Theft Act 1968 Sec 20 (1).

053/21(pt) Frauds in connection with sale of land etc.
(V) Law of Property Act 1925 Sec 183(pt).

053/22 Frauds in connection with sale of land etc.
(V) Land Registration Act 1925 Secs 115-116

053/30 Insider dealing.
(V) Criminal Justice Act 1993 Sec 52.

053/37 Cartel offences.
(V) The Enterprise Act 2002 Secs 188, 190.

053/39 Obtaining an award or a sum by
(V) deliberately committing an act or making an omission.
Fire and Rescue Services Act 2004 Sec 34 (6)(7).

053/52 In the course of registration proceedings, (S) suppress information with intention of Concealing a person's right/claim or substantiating a false claim.
Land Registration Act 2002 Sec 123.

053/53 Induce another to change the register of
(S) title or cautions register, or to authorise the making of such a change.
Land Registration Act 2002 Sec 124.

053/99 Other frauds.
(V) Various

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Legal: Obtaining Services Dishonestly

Fraud Act 2006 Sec 11

"… if he obtains services for himself or another by a dishonest act and the services were made on the basis that payment has been, is being or will be made for or in respect of them or he obtains them without payment having been made for or in respect of them or without payment having been made in full, and when he obtains them he knows they are being made available on the basis that payment will be made for them…."

Definition – Other Regulatory

This crime type should be used to record regulators fraud not covered elsewhere. Examples would include Land Registry, Insider Dealing at the stock exchange, or the Gambling Commission, etc.

NFIB17 Other Regulatory Fraud Counting Rules (1 of 1)

General Rule: One crime for each victim

Example 1: The land registry receive a fraudulent application to change the ownership of a plot of land.

One crime (class NFIB17)

NFIB18 Fraud by Failing to Disclose Information Classification (1 of 1)

053/41 Fraud by failing to disclose information
(V) Fraud Act 2006 Sec 3

Definition - Legal: Fraud by Failing to Disclose Information

Fraud Act 2006 Sec 3

"…dishonestly fails to disclose to another person information which he is under a legal duty to disclose and intends by failing to disclose the information to make a gain for himself or another, or to cause loss to another or expose another to a risk of loss".

NFIB18 Fraud by Failing to Disclose Information Counting Rules (1 of 1)

General Rule: One crime for each specific, intended or identifiable victim.

Example 1: A solicitor fails to share vital information with a client within the context of their work relationship, in order to make a gain for another client.

One crime (class NFIB 18).

Example 2: A solicitor acting for a supermarket chain, fails to disclose that a planning consent application has been granted to a supermarket chain on land being purchased from four separate householders. The land is sold at a considerable discount.

Four crimes (class NFIB18).

NFIB19 Fraud by Abuse of Position Classification (1 of 1)

053/42 Fraud by abuse of position
(V) Fraud Act 2006 Sec 4

Definition - Legal: Fraud by Abuse of Position

Fraud Act 2006 Sec 4

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

A person may be regarded as having abused his position even though his conduct consisted of an omission rather than an act.

NFIB19 Fraud by Abuse of Position Counting Rules (1 of 1)

General Rule: One crime for each specific, intended or identifiable victim.

Example 1: A person employed to care for the elderly takes advantage of his position of access to an account of a victim in order to remove money from that account.

One crime (class NFIB19).

Example 2: A person employed to care for the elderly takes advantage of his position of access to an account in order to remove money from five residents' accounts.

Five crimes (class NFIB19).

Example 3: A person employed to care for the elderly takes advantage of his position of access to a number of accounts of one resident in order to remove money from all those accounts.

One crime (class NFIB19).

Principal Crime: see also General Rules Section F and Annex C.

Where other NFIB frauds are apparent in addition to an offence of abuse of position of trust, only one crime should be recorded under the specific NFIB crime type and not an offence of abuse of position of trust.

Where offenders have been arrested in relation to other NFIB frauds eg. Mortgage Fraud and are charged only with an offence of abuse of a position of trust, the recorded crime should be under this NFIB fraud classification only. The other NFIB crime still stands in relation to the other offenders. If the only charge relating to an investigation is in relation to abuse of position, then only the abuse of position offence can be assigned outcome type A. The alternative detection offence rule does not apply.

Application of the Rule

Example 1: A solicitor is arrested for assisting a client obtain five mortgages on a number of properties by false representation. He and his client are both jointly charged with Mortgage Fraud and the solicitor is also charged with an offence of abuse of a position.

Five crimes (class NFIB5C)

Example 2: Following an investigation into a number of mortgages from the same lender that have resulted in charges in relation to Mortgage Fraud, the conveyancing solicitor is arrested and charged with one offence of abuse of position of trust only.

One crime (class NFIB19)

Example 3: Following an investigation into three mortgages from different lenders that have resulted in charges in relation to Mortgage Fraud, the conveyancing solicitor is arrested and charged with one offence of abuse of position of trust only.

Three crimes (class NFIB19) There are three victims.

NFIB20A DVLA Driving Licence Application Fraud Classification (1 of 1)

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition – Driving Licence Fraud

"Driving Licence fraud occurs where fraudsters obtain or try to obtain a United Kingdom driving licence by false representation to the Driver and Vehicle Licensing Agency (DVLA)."

This only applies to United Kingdom driving licences reported to the NFIB by the DVLA.

NFIB20A DVLA Driving Licence Application Fraud Counting Rules (1 of 1)

General Rule: One crime for each fraudulent application.

Example 1: The DVLA report that they have received a driving licence application using a forged foreign driving licence. No driving licence is issued.

One crime (class NFIB20A).

Example 2: The DVLA report that they have received three separate applications from the same offender for driving licences over the past year. They are all reported at the same time.

Three crimes (class NFIB20A). Three separate applications.

Application of the Rule

This class only deals with fraudulent United Kingdom driving licence applications. It does not deal with other Nations driving licences or with forged or counterfeit driving licences. The DVLA should be consulted to ensure that the application is false and to report the offence to the NFIB.
Forged/counterfeit driving licences should be dealt with under class 814 Fraud, Forgery etc associated with Vehicle or Driver Records.

Crimes in this class should be counted in addition to any other notifiable offence disclosed.

Example 1: A suspect is arrested after using a United Kingdom driving licence obtained by a fraudulent application to obtain a fraudulent hire purchase agreement on a new car.

One crime (class NFIB20A) and one crime (class NFIB5B).

Example 2: A suspect is stopped by police with a United Kingdom driving licence obtained by a fraudulent application and false utility bills. He admits that he was intending to use the documents to apply for a store card and obtain goods from the store.

One crime (class NFIB20A) and one crime (class 33A). Having articles for use in fraud.

NFIB90 Other Fraud (Not covered elsewhere) Classification (1 of 1)

053/04(pt) Conspiracy to defraud (apart from cheque
(V) Common Law
Criminal Justice Act 1987 Sec 12

053/40(pt) Fraud by false representation
(V) Fraud Act 2006 Sec 2.

053/46(pt) Obtaining services dishonestly
V) Fraud Act 2006 Sec 11

053/57 Dishonestly sub-let / part with possession
(V) of dwelling house let under secure or an assured tenancy in breach of a term of the tenancy.
Prevention of Social Housing Fraud Act 2012
Sec 1 (2) & 2 (2)

Definition – Legal: Fraud by False Representation

Fraud Act 2006 Sec 2

"…. Dishonestly makes a false representation, and intends, by making the representation to make a gain for himself or another, or to cause loss to another or to expose another to risk of loss. "

Definition - Legal: Obtaining Services Dishonestly

Fraud Act 2006 Sec 11

"… if he obtains services for himself or another by a dishonest act and the services were made on the basis that payment has been, is being or will be made for or in respect of them or he obtains them without payment having been made for or in respect of them or without payment having been made in full, and when he obtains them he knows they are being made available on the basis that payment will be made for them….".

Other Fraud

This section should be used for all other fraud by false representation or obtaining services dishonestly, that are not covered elsewhere.

NFIB90 Other Fraud (Not covered elsewhere) Counting Rules (1 of 1)

General Rule: One crime for each specific, intended or identifiable victim.

Example 1: A youth steals a charity box from a station. He then stands on the corner of a street and obtains money from a number of passing commuters. Police arrest him and trace two victims who made donations.

One crime of theft (class 49) and two crimes of other fraud (class NFIB90). This is not organised.

Parking, congestion charging etc.

Where members of the public report to police that they believe that they are in dispute over a parking ticket or congestion charge because they believe their number plate has been copied, they should be referred to the issuing Authority. Where the issuing authority contact police and provide information to show that another vehicle has been displaying a false or copied number plate a crime should be recorded under this class.

Example 1: Mrs ‘A’ reports to police that she has received a parking ticket for parking in London and she lives in Devon and has never been to London.

Mrs ‘A’ should be referred to the London Authority, no crime is necessary.

Mrs ‘A’ contacts the London Authority concerned. Following enquiries the Local Authority report that they believe a car issued with this ticket was displaying a false number plate.

One crime (class NFIB90).

Where cars are displaying stolen, false or borrowed permits, blue badges, etc a crime should be recorded under class 814, Mishandling or faking parking documents.

Example 1: Mr ‘A’ loans his son his residents permit so that he can park his car in a resident’s bay whilst visiting.

One crime (class 814).

NFIB50 Computer Misuse Crime

Terminology

Within the Computer Misuse group of notifiable offences, the use of technical terms and jargon has been kept to a minimum. This enables the lay person to understand what the rules are determining and needs to be counted. It is also recognition that this is a very fast moving area of offending with new methods being discovered all the time. The focus of these rules is the end product, what is the criminal trying to achieve? It is not an attempt to describe or separate out every smurf, ping or syn flood attack.

It is also important to consider the main objective of the criminal. There will be considerable overlap between the offences, so for example a denial of service attack may well involve computer Hacking. The Hacking was a facilitator to commit the denial of service. The Principal crime will be the offender's goal.

Phishing E mails

Definition – Phishing

Phishing is a method employed by Fraudsters to try and obtain personnel details such as user names and passwords. Phishing is carried out by sending spoof e mails or instant messaging. Often the e mail will look like it is genuine and will contain links that take victims to a website that looks identical to the genuine web site. Victims will then attempt to log into the site and in so doing will disclose their username and password. The fraudster then uses the log in details to commit fraud.

Phishing is an enabler to commit fraud. Where the phishing e mail has been used to commit fraud or computer misuse offences, then the relevant fraud or computer misuse offence should be recorded. No separate crime should be recorded in relation to the phishing. Where no fraud offences have taken place as a result of the phising e mail, crimes should only be recorded where the victim has been specifically targeted. It is not sufficient just to have received a phising e mail for a crime to be recorded.

Where offenders are found to have created phishing e mails or fake websites an offence should be considered under class 33A making, supplying or possessing articles for use in fraud.

NFIB50A Computer Viruses\Malware Classification (1 of 1)

053/34 (V)	Unauthorised access to computer material with intent to commit or facilitate commission of further offences. Computer Misuse Act 1990 Sec 2.
053/35 (S/V)	Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer etc. Computer Misuse Act 1990 Sec 3, as amended by Police & Justice Act 2006.
053/54 (S/V)	Unauthorised access to computer material. Computer Misuse Act 1990 Sec 1 (3) as amended by Police & Justice Act 2006.

Definition – Legal: Computer Viruses or Malware

Computer Misuse Act 1990 Sec 3

"…he does any act which causes an unauthorised modification of the contents of any computer; and at the time when he does the act he has the requisite intent and the requisite knowledge."

Application

This fraud should not be viewed as limited to desk or lap top computers. It can include any device using operating software accessible on line, for example games consoles and smart phones.

Definition – Computer Virus

Computer virus is a computer program that can replicate itself and spread from one computer to another by using executable code. It is usually sent over a network or the internet or introduced to a computer on a disk drive or memory device.

Definition – Malware

Malware is short for malicious software. It consists of programming (code, scripts, or other software) designed to disrupt or deny the operation of a computer. The program can also gather information from the computer and pass this onto other computers. It can also use the computer as a resource for other computers, storing images or part of a botnet for example. It includes, worms, trojan horses, adware and spyware.

NFIB50A Computer Viruses\Malware Counting Rules (1 of 3)

General Rule: One crime for each specific intended victim.

Application of the Rule

The important aspect to consider is specific intended victim. Where viruses or malware, are launched onto the World Wide Web to infect any computer they come across, victim's computers that are infected are not generally specific intended victims. Where police receive reports under these circumstances, that computers have been infected by or received a virus or malware then a crime related incident should be recorded.

Example 1: John reports that a virus, known to have infected thousands of machines World Wide, has infected his computer. He has no idea when or how his machine was infected.

Record an information report.

Example 2: John has had his golf membership withdrawn by the Golf club committee. He goes home and sends an e mail with a virus attached to the home e mail address of the twelve members of the committee. The virus infects eight machines and four machines' antivirus programmes stop the attack.

Eight crimes of unauthorised modification of computer material (class NFIB50A) and four crimes of attempted unauthorised modification of computer material (class NFIB50A).

Example 3: Susan has been sacked from her high profile job at ABC Media. Before she leaves she sends an email with a virus attached to everyone @ABC Media. The next day all of ABC Media's employee's computers have been infected.

One crime of unauthorised modification of computer material (class NFIB50A). ABC Media are the intended victim.

Example 4: Susan has been sacked from her high profile job at ABC Media. Before she leaves she sends an e mail with a virus attached to the Chairman, Chief Executive and HR Director at ABC Media. The next day all of ABC Media employee's computers have been infected.

Three crimes of unauthorised modification of computer material (class NFIB50A). There are three specific intended victims.

If the victim has taken positive action following receipt of phishing e mails, or clicked on links on websites for their computer to become infected, then they will become a specific intended victim. For example by being directed to a specific website after receiving specific instructions to visit that site, e.g. by clicking a link in a phishing e mail, then they become a specific intended victim when the computer is infected, and a crime should be recorded.

Example 5: Lisa reports that she received an e mail into her account with a link to a website. She has clicked on the link. An internet page has opened and has downloaded a Malware program onto her computer.

One crime of unauthorised modification of computer material (class NFIB50A).Lisa has become a specific intended victim.

NFIB50A Computer Viruses\Malware Counting Rules (2 of 3)

Application of the Rule (continued)

Example 6: John receives a text message on his smart phone with a link attached. He taps the link and opens a web page that has downloaded Malware that locks his phone.

One crime of unauthorised modification of computer material (class NFIB50A).John has become a specific intended victim.

Principle Crime - Malware or Hacking? See also General Rules Section F & Annex C

Crimes should be recorded under this section up until the point where the offender then actually uses the malware. When the offender uses the malware it becomes a deliberate targeting of that computer. As soon as the offender directly uses the program then an offence of Hacking should be recorded as the principal crime.

Example 1: Mr A has clicked on a link on a web page that has downloaded a program onto his computer that enables his computer to be used in the storage of pornographic images.

At this stage there is one crime of unauthorised modification of computer material (class NFIB50A).

The program responds and starts to store the images into a hidden section of the hard drive.

This is now a crime of computer Hacking and one crime unauthorised modification of computer material (class NFIB52B) should be recorded.

Principle Crime and Finished Incident Rule: See also General Rules Section E & F & Annex C

Where malware is used to obtain details to commit fraud or other computer misuse offences then the fraud or computer misuse offences are the principle crime and should be recorded. The Malware has been used to enable another offence to be committed and no offence should be recorded under this section if reported at the same time.

Example 1: Mr A reports to Report Fraud that he has clicked on a link that has downloaded a program. He has run an anti spyware program and been told that the program is a key logger program and has been successfully removed.

One crime of unauthorised modification of computer material (class NFIB50A).

A week later, he contacts Report Fraud to report that today his online bank account has been

unlawfully accessed and £2000 has been stolen from it by changing a standing order to pay his mortgage.

One additional crime of Mandate fraud (NFIB5D) should be recorded.

Example 2: Mr A reports to Report Fraud that a week ago he has clicked on a link that has downloaded a program. He has run an anti spyware program and been told that the program is a key logger program and has been successfully removed. Today he has found that his online bank account has been unlawfully accessed and £2000 has been stolen from it by changing a standing order to pay his mortgage. This is why he has called today.

One crime of Mandate fraud (NFIB5D) should be recorded.

NFIB50A Computer Viruses\Malware Counting Rules (3 of 3)

Application of the Rule (continued)

Suspect releasing a virus or malware

Where a suspect is identified for releasing a virus or malware from a venue within England or Wales then a crime should be recorded for each distinct virus released from that venue, to be recorded where the suspect is based.

Example 1: An offender in Cardiff is identified for releasing a Virus onto the World Wide Web. This Virus infects hundreds of machines across the world.

One crime of unauthorised modification of computer material (class NFIB50A).

Example 2: A suspect in London is identified for releasing three different Viruses onto the World Wide Web. These Viruses infect hundreds of machines across the world.

Three crimes of unauthorised modification of computer material (class NFIB50A).

Example 3: Three victims have reported that after they had followed a link on a web page their computers had been infected with Malware. Following an investigation the suspect responsible for the Malware is arrested and charged.

Four crimes of unauthorised modification of computer material (class NFIB50A), one for each victim and one for the suspect responsible.

NFIB51A Denial of Service Attack Classification (1 of 1)

053/34 (V)	Unauthorised access to computer material with intent to commit or facilitate commission of further offences. Computer Misuse Act 1990 Sec 2.
053/35 (S/V)	Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer etc. Computer Misuse Act 1990 Sec 3, as amended by Police & Justice Act 2006.
053/54 (S/V)	Unauthorised access to computer material. Computer Misuse Act 1990 Sec 1 (3) as amended by Police & Justice Act 2006.

Definition – Legal: Denial of Service Attacks

Computer Misuse Act 1990 Sec 3

"…he does any act which causes an unauthorised modification of the contents of any computer; and at the time when he does the act he has the requisite intent and the requisite knowledge."

Definition – Denial of Service Attack

A 'denial of service attack' (DoS attack) or 'distributed denial of service attack' (DDoS attack) is an attempt to make a computer unavailable to its intended users. It consists of the concerted efforts of a person, or group of people to prevent an Internet site or service from operating. The Internet site or e mail address can be bombarded with thousands of hits or mail, frequently using 'Botnets' to perform these attacks. It can also be attacked by Malware that disrupts the operation, memory usage, or programs of the computer. These attacks lead to the server or bandwidth becoming overloaded and shutting down. DoS or DdoS attacks lead to the service being unable to operate and deal with genuine business.

Definition – Permanent denial of service attack

A 'permanent denial of service attack' (PdoS) is where the attack is aimed at, or has the result that the damage caused is so severe that computers or programs have to be replaced.

NFIB51A Denial of Service Attack Counting Rules (1 of 2)

General Rule: One crime for each victim.

Example 1: ABC ltd report that their website has been attacked by hundreds of thousands of users trying to access their site. Usually the site attracts 1000 visits a day. The concerted effort has resulted in the web server failing and they are unable to use the web site.

One crime denial of service attack (class NFIB51A).

Application of the Rule

Denial of service attacks are 'concerted efforts' to take down web sites and services. Care must be taken to establish the concerted effort and that the web site has not just been inundated with unexpected demand. Concerted effort will be apparent from viewing the traffic data and the source of the hits. This will usually be evidenced from the companies IT department. NOTE: It is not necessary for the service to fail to record an offence.

Example 1: Following a celebrity chef cooking on a live television cook show a supermarket online web site is inundated with orders for an unusual ingredient. The number of enquiries exceeds the bandwidth and the web site crashes.

There is no concerted effort and no crime to report in these circumstances.

Example 2: A company's IT department report that they have evidenced a concerted attack on their web server. This has caused a number of issues but no disruption to the service.

One crime denial of service attack (class NFIB51A).

Where malware is used to obtain details to commit fraud or other computer misuse offences then the other computer misuse offences are the principle crime and should be recorded. The Malware has been used to enable another offence to be committed.

Example 1: Malware has been used to disrupt the operating system and program files of a company's web site. This has caused the web site to be unusable and crash for a number of days

One crime denial of service attack (class NFIB51A).

Principle Crime : Permanent denial of service or Criminal Damage?: See also General Rules Section F & Annex C

Where the attack on the computer service is so severe that computers or programs have to be replaced to enable the system to operate again, the recorded crime should be under this section and not an offence of criminal damage.

Example1: A disgruntled ex employee decides that he will get his own back. He uploads malware onto the company's web site that replaces the server's firmware. This causes the web site to crash destroying the hard disk. The web site is restored some days later after a new hard disk is installed and the correct firmware reinstalled.

One crime denial of service attack (class NFIB51A).

NFIB51A Denial of Service Attack Counting Rules (2 of 2)

Finished Incident Rule

The finished incident rule should be applied to each allegation of a denial of service attack.

Example 1: ABC ltd report that there web site has crashed and their IT manager has established that they have been subjected to a denial of service attack.

One crime denial of service attack (class NFIB51A).

Two days later, they report that they are the victim of another similar attack.

One additional crime denial of service attack (class NFIB51A).

Two weeks later, they report that they have had another three attacks.

One crime denial of service attack (class NFIB51A). Finished Incident rule applies.

NFIB51B Denial of Service Attack (Extortion) Classification (1 of 1)

035/00 Blackmail.
(V) Theft Act 1968 Sec 21.

Definition - Legal: Blackmail

Theft Act 1968 Sec 21

(1) “A person is guilty of blackmail if, with a view to gain for himself or another or with intent to cause loss to another, he makes any unwarranted demand with menaces; and for this purpose a demand with menaces is unwarranted unless the person making it does so in the belief-
(a) that he has reasonable grounds for making the demand; and
(b) that the use of the menaces is a proper means of reinforcing the demand.

(2) The nature of the act or omission demanded is immaterial, and it is also immaterial whether the menaces relate to action to be taken by the person making the demand ...”

Definition – Denial of Service Attack

A ‘denial of service attack’ (DoS attack) or ‘distributed denial of service attack’ (DDoS attack) is an attempt to make a computer unavailable to its intended users. It consists of the concerted efforts of a person, or group of people to prevent an Internet site or service from operating. The Internet site or e mail address can be bombarded with thousands of hits or mail, frequently using ‘Botnets’ to perform these attacks. It can also be attacked by Malware that disrupts the operation, memory usage, or programs of the computer. These attacks lead to the server or bandwidth becoming overloaded and shutting down. DoS or DDoS attacks lead to the service being unable to operate and deal with genuine business.

Definition – Permanent denial of service attack

A ‘permanent denial of service attack’ (PdoS) is where the attack is aimed at, or has the result that the damage caused is so severe that computers or programs have to be replaced.

Definition – Denial of service attack (extortion)

This occurs where there is an unwarranted demand with menaces (Blackmail) attached to the Denial of Service attack, or the threat of a denial of service.

NFIB51B Denial of Service Attack (Extortion) Counting Rules (1 of 2)

General Rule: One crime for each victim.

Example 1: ABC ltd report that their website has been attacked by hundreds of thousands of users trying to access their site. Usually the site attracts 1000 visits a day. The concerted effort has resulted in the web server failing and they are unable to use the web site. They also report that they have received an e mail from someone who states that they are responsible for taking down the website today and that if they don't pay £10,000 to a given account by midnight then their website will be taken down again until the money is paid.

One crime Denial of Service attack (extortion) (class NFIB51B).

Example 2: Joe Soap ltd report that their website has been attacked by hundreds of thousands of users trying to access their site. The concerted effort has resulted in the web server failing and they are unable to use the web site. They also report that following receipt of an e mail they have paid £5,000 into the suspects account to prevent another attack. They have then decided to report the matter to Report Fraud.

One crime Denial of Service attack (extortion) (class NFIB51B).

Application of the Rule

It is not necessary for any denial of service attack to have taken place or to take place for a crime to Be recorded under this section. It is sufficient for an unwarranted demand to be made with the threat of a denial of service attack.

Example 1: ABC ltd report that they have received a telephone call stating that unless they pay £10,000 their web site will suffer a DDOS attack. There has been no attack on their website.

One crime Denial of Service attack (extortion) (class NFIB51B).

Principle Crime - Finished Incident Rule: See also General Rules Section F & Annex C.

Denial of Service attack (extortion), class NFIB51B is the principal crime over an offence of Blackmail class 35. Where an offence of NFIB51B is made out, no offence should be recorded under class 35.

The finished incident and principal crime rules should be applied to the circumstances of each case reported.

Example 1: ABC ltd report that their website has been attacked by hundreds of thousands of users trying to access their site. Usually the site attracts 1000 visits a day. The concerted effort has resulted in the web server failing and they are unable to use the web site.

One crime denial of service attack (class NFIB51A).

Two days later, ABC ltd reports a further attack that has caused the web server to fail and deny any access to their web site.

An additional crime of denial of service attack (class NFIB51A).

Two days later, ABC ltd reports a further attack that has caused the web server to fail and deny any access to their web site. They also report that they have received a telephone call demanding payment of £10,000 to stop any further attacks.

One crime Denial of Service attack (extortion) (class NFIB51B).

NFIB51B Denial of Service Attack (Extortion) Counting Rules (2 of 2)

Application of the Rule (continued)

Example 2: ABC ltd report that their web site has suffered a DDOS attack on two separate days last week. They have phoned up today because they have received an e mail stating that unless they pay £10,000 their site will be attacked again.

One crime Denial of Service attack (extortion) (class NFIB51B).

NFIB52 Computer Hacking
NFIB52A Hacking-Server Classification (1 of 1)

053/34 (V)	Unauthorised access to computer material with intent to commit or facilitate commission of further offences. Computer Misuse Act 1990 Sec 2.
053/35 (S/V)	Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer etc. Computer Misuse Act 1990 Sec 3, as amended by Police & Justice Act 2006.
053/54 (S/V)	Unauthorised access to computer material. Computer Misuse Act 1990 Sec 1 (3) as amended by Police & Justice Act 2006.

Definition – Legal: Computer Hacking

Computer Misuse Act 1990 Sec 3

"…he does any act which causes an unauthorised modification of the contents of any computer; and at the time when he does the act he has the requisite intent and the requisite knowledge."

Definition –Hacking

Computer Hacking is the unathorised modification of the contents of any computer. It is usually committed by persons unlawfully accessing the computer, but it can be committed by persons with lawful access to the computer as well. It is the deliberate targeting of a specific computer by the offender.

Definition – Server

A computer server is a physical computer dedicated to running services or hosting files for other computers on a network.

NFIB52A Hacking-Server Counting Rules (1 of 1)

General Rule: One crime for each server affected.

Example 1: A software company reports that there security software has detected an unauthorised access to their server. Following investigation they have established that there have been changes made to some of their programmes stored on the server.

One crime of Hacking-Server (class 52A).

Example 2: A software company reports that there security software has detected an unauthorised access to their server. Following investigation they have established that there have been changes made to some of their programmes stored on the server. They also establish that access has been gained to their separate mail server and files altered.

Two crime of Hacking-Server (class 52A).

Application of the Rule

For crimes to be recorded under this section the files or services modified must be on the server and not on a computers local hard drive.

Example 1: An employee leaves his desktop computer logged on when he leaves the office. A colleague then gains access to his employment records held on the server and amends some of the details recorded on his file by using the logged on computer.

One crime of Hacking-Server (class 52A).

Example 2: A colleague phones the office and asks her friend to show her out of office on. She provides her password. Once logged in, her colleague turns this on and then goes into the my documents section stored locally on her computer. There is a document in draft with performance pay recommendations. She alters this, thinking this will enhance her pay next year.

One crime of Hacking-Personal (class 52B).

Principle Crime Rule

With the exception of crimes under class NFIB52C Hacking-e mail and social media, where the Unauthorized access has directly enabled the commission of another Fraud Offence the principle crime will be the other fraud offence. No offence should be recorded under this section.

Example 1: A computer hacker has gained access to a number of on line bank accounts held on a banks server. He is able to transfer money from ten accounts into his own account.

Ten crimes of Cheque, plastic card and Online Bank Account Fraud (class NFIB5A). One crime for each account defrauded.

Where the actions of the hacker are only preparatory and no substantive offence has been committed under any other fraud offence, then an offence should be recorded under this section.

Example 1: A computer hacker has gained access to a banks server that holds details of online bank accounts. He has set up a money transfer to his own account from one of the accounts. However, before he can execute the command he is logged out.

One crime of Hacking-Server (class 52A).

NFIB52B Hacking- Personal Classification (1 of 1)

053/34 (V) Unauthorised access to computer material with intent to commit or facilitate commission of further offences.
Computer Misuse Act 1990 Sec 2.

053/35 (S/V) Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer etc.
Computer Misuse Act 1990 Sec 3, as amended by Police & Justice Act 2006.

053/54 (S/V) Unauthorised access to computer material.
Computer Misuse Act 1990 Sec 1 (3) as amended by Police & Justice Act 2006.

Definition – Legal: Computer Hacking

Computer Misuse Act 1990 Sec 3

"…he does any act which causes an unauthorised modification of the contents of any computer; and at the time when he does the act he has the requisite intent and the requisite knowledge."

Definition –Hacking

Computer Hacking is the unathorised modification of the contents of any computer. It is usually committed by persons unlawfully accessing the computer, but it can be committed by persons with lawful access to the computer as well. It is the deliberate targeting of a specific computer by the offender.

Definition – Personal Computer

A personal computer is any individual computer that is not a server. This fraud should not be viewed as limited to desk or lap top computers. It can include any device using operating software accessible on line, for example games consoles and smart phones.

NFIB52B Hacking- Personal Counting Rules (1 of 2)

General Rule: One crime for each computer affected.

Example 1: A computer hacker has gained access to a home computer connected to the internet. Having gained access he downloads and stores pornographic images onto the hard drive in a hidden directory he has created.

One crime of Hacking-Personal (class NFIB52B).

Application of the Rule

Principle Crime Rule

With the exception of crimes under class NFIB52C Hacking-e mail and social media, where the Unauthorized access has directly enabled the commission of another Fraud Offence the principle crime will be the other fraud offence. No offence should be recorded under this section.

Example 1: A computer hacker has gained access to the victims on line bank account through his home computer. He is able to transfer money from the account into his own account.

One crime of Cheque, plastic card and Online Bank Account Fraud (class NFIB5A).

Where the actions of the hacker are only preparatory and no substantive offence has been committed under any other fraud offence, then an offence should be recorded under this section.

Example 1: A computer hacker has obtained the password and log in details to the victims on line bank account stored on his home computer. He then tries to access the banks on line server to transfer money into his account using these details, but fails to do so.

One crime of Hacking-Personal (class 52B).

Number of Crimes

Where personal computers are hacked into to obtain details to obtain unauthorized access to a server then a crime should be recorded for each unauthorised access unless directly enabling the commission of another Fraud Offence. The principle crime will be the other fraud offence.

Example 1: A civil servants smart phone is hacked into whilst using the internet at a wifi hotspot. The hacker is able to obtain all the passwords and access codes to a governments secure server.

One crime of Hacking-Personal (class 52B).

Later, the hacker, using these details gains access to the secure server.

One additional crime of Hacking-Server (class 52A).

Example 2: A computer hacker has obtained the password and log in details to the victims on line bank account stored on his home computer. He then logs into the banks server with these details and transfers money into his own account from the victims on line account.

One crime of Cheque, plastic card and Online Bank Account Fraud (class NFIB5A).

NFIB52B Hacking- Personal Counting Rules (2 of 2)

Application of the Rule (continued)

Principle Crime - Malware or Hacking? See also General Rules Section F & Annex C.

Crimes should be recorded under class NFIB50A computer viruses and Malware up until the point **where the offender then actually uses the malware. When the offender uses the malware it becomes a deliberate targeting of that computer. As soon as the offender directly uses the program then an offence of Hacking should be recorded as the principal crime.**

Example 1: Mr A has clicked on a link on a web page that has downloaded a program onto his computer that enables his computer to be used in the storage of pornographic images.

At this stage there is one crime of unauthorised modification of computer material (class NFIB50A).

The program responds and starts to store the images into a hidden section of the hard drive.

This is now a crime of computer Hacking and one crime of Hacking-Personal (class NFIB52B) should be recorded.

NFIB52C Hacking- Social media and e mail Classification (1 of 1)

053/34 (V)	Unauthorised access to computer material with intent to commit or facilitate commission of further offences. Computer Misuse Act 1990 Sec 2.
053/35 (S/V)	Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer etc. Computer Misuse Act 1990 Sec 3, as amended by Police & Justice Act 2006.
053/54 (S/V)	Unauthorised access to computer material. Computer Misuse Act 1990 Sec 1 (3) as amended by Police & Justice Act 2006.

Definition – Legal: Computer Hacking

Computer Misuse Act 1990 Sec 3

"…he does any act which causes an unauthorised modification of the contents of any computer; and at the time when he does the act he has the requisite intent and the requisite knowledge."

Definition –Hacking

Computer Hacking is the unathorised modification of the contents of any computer. It is usually committed by persons unlawfully accessing the computer, but it can be committed by persons with lawful access to the computer as well. It is the deliberate targeting of a specific computer by the offender.

Definition-Social Media and Email

This offence should be applied to individual accounts. It includes all forms of individual e mail accounts and all forms of individual social media, for example twitter and Facebook. It includes personal as well as companies or organizations individual accounts.

This fraud should not be viewed as limited to desk or lap top computers. It can include any device using operating software accessible on line, for example games consoles and smart phones.

NFIB52C Hacking- Social media and e mail Counting Rules (1 of 1)

General Rule: One crime for each of the victims accounts affected.

Example 1: A suspect has gained unathorised access to the victims e mail account. They have then sent an e mail to all contacts in the contacts folder stating that they are stranded in an African country and urgently need £200 sent to a specific account to pay for an airfare home.

One crime of Hacking (class 52C).

Example 2: The victim logs into her Facebook account and to her horror discovers that someone has gained access to her account and posted a number of embarrassing photographs of her.

One crime of Hacking (class 52C).

Example 3: The victim logs into her Facebook account and to her horror discovers that someone has gained access to her account and posted a number of embarrassing photographs of her. She then finds that similar pictures have been posted on her Linkedin account.

Two crime of Hacking (class 52C).

Application of the Rule

Where accounts are hacked into and as a result of this action other people become victims of a fraud a crime under this section should be recorded in addition to the other victim based frauds.

Example 1: A suspect has gained unathorised access to the victims e mail account. They have then sent an e mail to all contacts in the contacts folder stating that they are stranded in an African country and urgently need £200 sent to a specific account to pay for an airfare home. Three of her friends send money to the account.

One crime of Hacking (class 52C) and three crimes of other advanced fee (class NFIB1H).

Harassment

The crime of Hacking requires unauthorised access to a users account. The offence does not involve people with access posting offensive or derogatory comments on a site or cyber bullying. These actions should be considered under Harassment provisions or under Public Order Act offences.

NFIB52D Computer Hacking-PBX/Dial Through Classification (1 of 1)

053/34 (V) Unauthorised access to computer material with intent to commit or facilitate commission of further offences. Computer Misuse Act 1990 Sec 2.

053/35 (S/V) Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer etc. Computer Misuse Act 1990 Sec 3, as amended by Police & Justice Act 2006.

053/54 (S/V) Unauthorised access to computer material. Computer Misuse Act 1990 Sec 1 (3) as amended by Police & Justice Act 2006.

Definition – Legal: Computer Hacking

Computer Misuse Act 1990 Sec 3

"…he does any act which causes an unauthorised modification of the contents of any computer; and at the time when he does the act he has the requisite intent and the requisite knowledge."

Definition-Private Branch Exchange (pbx)/dial through A PBX hack is a remote attack on telephone systems that contain features such as 'call forwarding', 'voicemail' and 'divert'. All of these systems have security features such as passwords to access the system remotely. Fraudsters usually gain access unlawfully and then use the system to divert calls to premium rate or overseas numbers that generate considerable revenue to the fraudster and loss to the victims.

It is possible for someone with lawful access to the system to commit this offence by acting beyond their permissions.

NFIB52D Computer Hacking-PBX/Dial Through Counting Rules (1 of 1)

General Rule: One crime for each victims exchange unlawfully accessed

Example 1: ABC ltd return from a bank holiday weekend to discover that there telephone system has been unlawfully accessed. On contacting their service provider, they discover that £56,000 of calls have been made to a premium rate number.

One crime class NFIB52D.

Example 2: Three small businesses working from the same address discover that all of their phone systems have been unlawfully accessed and each have received considerable bills for phone calls abroad.

Three crimes class NFIB52D.

NFIB52E Hacking (Extortion) Classification (1 of 1)

035/00 Blackmail.
(V) Theft Act 1968 Sec 21.

Definition - Legal: Blackmail

Theft Act 1968 Sec 21

(1) “A person is guilty of blackmail if, with a view to gain for himself or another or with intent to cause loss to another, he makes any unwarranted demand with menaces; and for this purpose a demand with menaces is unwarranted unless the person making it does so in the belief-
(a) that he has reasonable grounds for making the demand; and
(b) that the use of the menaces is a proper means of reinforcing the demand.

(2) The nature of the act or omission demanded is immaterial, and it is also immaterial whether the menaces relate to action to be taken by the person making the demand.

Definition –Hacking

Computer Hacking is the unauthorised modification of the contents of any computer. It is usually committed by persons unlawfully accessing the computer, but it can be committed by persons with lawful access to the computer as well.

Definition – Hacking (Extortion)
this occurs where there is an unwarranted demand with menaces (Blackmail) attached to any computer Hacking or threat of computer Hacking.

The extortion can be in relation to any NFIB class under NFIB52 Computer Hacking.

NFIB52E Computer Hacking (Extortion) Counting Rules (1 of 2)

General Rule: One crime for each victim.

Example1: An actor is sent an e mail with a number of explicit sexual photographs attached. The e mail states that there are a lot more photographs available that have been copied from his personal computer and that these will be released onto the World Wide Web if £50,000 is not paid immediately to the suspect's bank account. The attached photographs show the file directory of the actor's home computer from where they were copied.

One crime Computer Hacking (extortion) (class NFIB52E).

Example 2: An ex employee contacts his previous company Chairman and states that he has a copies of e mails that show that the company Chairman had made significant share trades by insider dealing. He includes a copy of an e mail from the Chairman's e mail account as proof of this. He demands £10,000 to keep quiet about the matter. The Chairman has paid the money but decides to report the matter to Report Fraud.

One crime Blackmail (class 35) recorded by the police.

Application of the Rule

It is not necessary for any computer Hacking to have taken place or to take place for a crime to be recorded under this section. It is sufficient for an unwarranted demand to be made with the threat of computer Hacking.

Example 1: A well known celebrity received a telephone call stating that unless she pays £10,000 nude photographs of her will be placed on her Facebook page. No photographs have been posted.

One crime Computer Hacking (extortion) (class NFIB52E).

Principle Crime

Where a threat or an unwarranted demand with menaces is connected to anything obtained as a result of hacking or involves an unwarranted demand made with the threat of computer hacking class NFIB52E is the principal crime over an offence of Blackmail class 35 unless the victim has complied with the demands made or suffered other direct loses.

The finished incident and principal crime rules should be applied to the circumstances of each case reported.

Example 1: ABC ltd report that they have received a memory stick in the post that contains part of their computer code for a new game that is about to be released. The code is secret software code and only available on the companies server.

One crime Computer Hacking Server (class NFIB52A).

Two days later, ABC ltd reports a further memory stick with additional code has been received for the same game.

An additional crime of Computer Hacking Server (class NFIB52A).

NFIB52E Computer Hacking (Extortion) Counting Rules (2 of 2)

Application of the Rule (continued)

Two days later, ABC ltd reports that they have received a telephone call demanding payment of £100,000 to stop the release of the games secret code on the World Wide Web.

One crime Computer Hacking (extortion) (class NFIB52E)

Example 2: ABC ltd report that they have received a demand for £100,000 to be paid unless a copy of the code for their new computer game will be posted on the World Wide Web. They are extremely concerned, because last week they received a memory stick with part of the code from their server copied on it.

One crime Computer Hacking (extortion) (class NFIB52E)

Example 3:

Where a threat or an unwarranted demand with menaces is connected to anything obtained as a result of hacking, or involves an unwarranted demand made with the threat of computer hacking Class NFIB52E is the principle crime over an offence of Blackmail class 35 unless the victim has complied with the demands made or suffered other direct losses.

A person reports receiving an email with several explicit sexual photographs attached. The email states that there are a lot more photographs available that have been copied from his personal computer and that these will be released onto the World Wide Web if £50,000 is not paid immediately to the suspect's bank account. The attached photographs show the file directory of the recipient's home computer from where they were copied. The victim makes no attempt to pay.

One crime Computer Hacking (extortion) (class NFIB52E). added April 2019

Maximum Sentence - Fraud							
Life	**14 years**	**10 years**	**7 years**	**5 years**	**3 years**	**2 years**	**Fine**
053/56	053/11	051/03, 06	051/01	053/02	053/13	051/04-05	052/09-10
	053/99	053/04	051/03	053/20		052/02-08, 11-12	061/28
		053/31,32,35	052/01	053/23-24		053/10	061/33
		060/21-22	053/06	053/34		053/14	
		061/21-27	053/08	053/37		053/21-22	
		061/31, 38-39	053/15	053/46		053/25	
		053/40-42	053/30	053/43		053/39, 52-55	
		053/44	053/33, 36, 38			055/00,02-05,07,09,11	
		053/45	055/01			061/29-30	
		061/34-35	055/06, 08,10, 12			061/32	
			061/41			061/36, 40	
						814/01-07,10	