Home Office

THE SCALE AND NATURE OF FRAUD:
A REVIEW OF THE EVIDENCE

Collated by Laura Blakeborough and Sara Giro Correia

1. METHODS AND DEFINING FRAUD

The **aim** of the review was to bring together what is known about the scale and nature of fraud affecting individuals and businesses in the UK. This was in order to establish the current state of the evidence base and identify areas for research.

Methodology

1. Review of Literature

Included published academic, government and industry sources (mainly from the UK).

The scope was limited as follows.

- Included fraud against individuals and businesses.
- Excluded fraud against the charity sector and the public sector.
- Excluded research regarding offenders.

2. Data Analysis

Data were analysed and synthesised according to a framework (see figure opposite) which assisted in presenting the evidence.

Sources included: Criminal justice system data, administrative data aggregated from membership organisations and victim surveys.

Overview of Fraud Types by Victim Group

The framework above combines **victim type** (individuals, financial services sector and other businesses) with **fraud type** (e.g. advanced fee fraud, fraud by customers) to help bring together academic, official and industry source data for the purposes of this review. See appendix for a more detailed breakdown.

1. **Fraud is, in many ways, a unique crime type.** It overlaps with many other crime types and there is no one body or organisation that can deal with fraud in its entirety.

Fraud is Unique

- It takes place in strikingly different contexts.
- It uses a plethora of methods.
- Methods can change and evolve during interactions.
- It takes place over short and long periods of time.
- It can be a single incident or multiple incidents and the fraud type can vary between these.
- It is a crime of deception so victims may be unaware of being defrauded.
- It can happen online or use more traditional methods and/or be facilitated by cyber crimes such as hacking or data breaches.

Fraud is not a new crime but it has evolved recently with the rise in technology and the internet.

Fraud Overlaps Considerably with Other Offences

NB. Money laundering is intrinsically linked with fraud and a variety of other crime types. Anecdotally it is thought that some fraud cases may be convicted as money laundering and vice versa.

It is not possible for any one body or organisation in the public, private or voluntary sector to tackle the entirety of fraud. It requires a multi-agency, multi-partnership response.

2. THE SCALE AND NATURE OF FRAUD AGAINST INDIVIDUALS

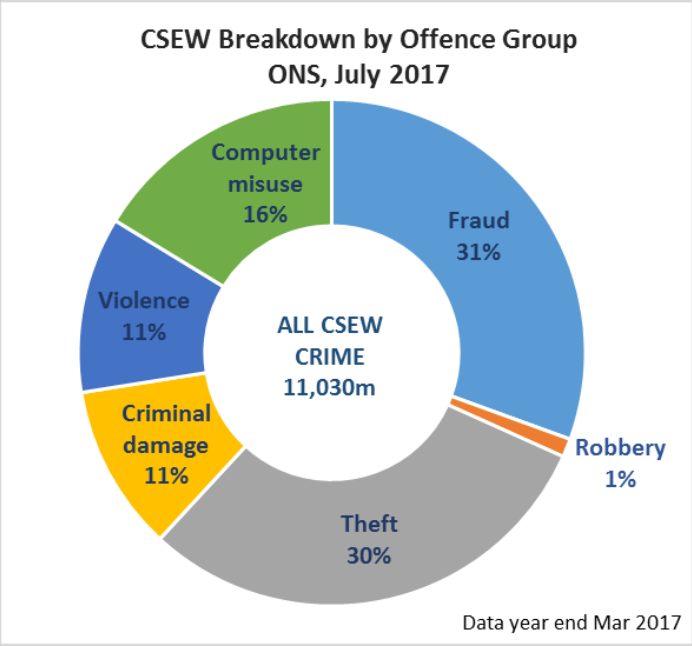
2. **The inclusion of fraud and cyber crime in the Crime Survey for England and Wales (CSEW) from October 2015 markedly altered the picture of crime**. Results show fraud and cyber crime are almost equivalent to the volume for *all* other crime (5.2m offences). Fraud alone represents 31% of CSEW crime. National Fraud Intelligence Bureau (NFIB) recorded fraud has been increasing steadily since 2011.

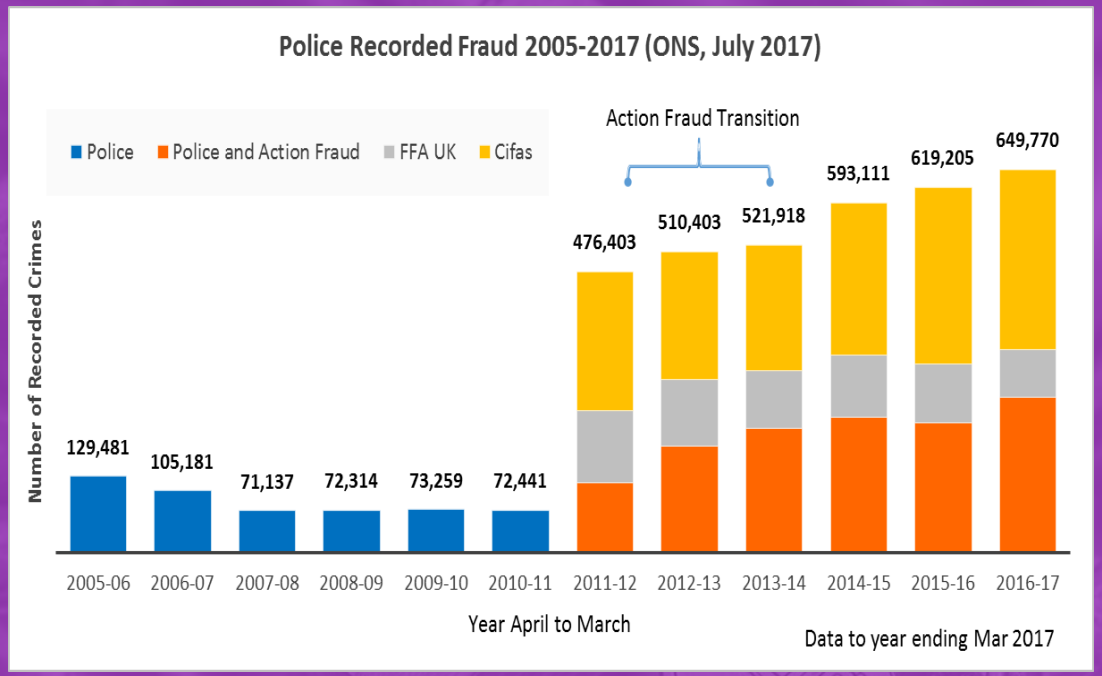
Crime Survey for England and Wales

Fraud is not a new crime, but for the first time the CSEW allows some measurement of its scale.

Total CSEW crime = 11m.

- Fraud and computer misuse = 5.2m
  - Fraud = 3.4m (31% of CSEW)



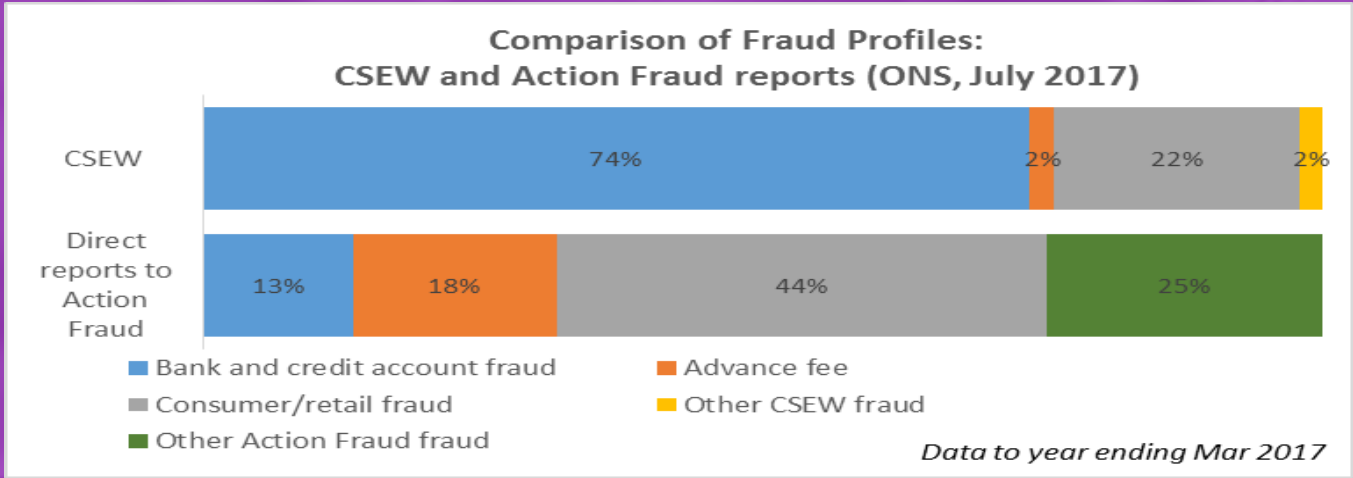


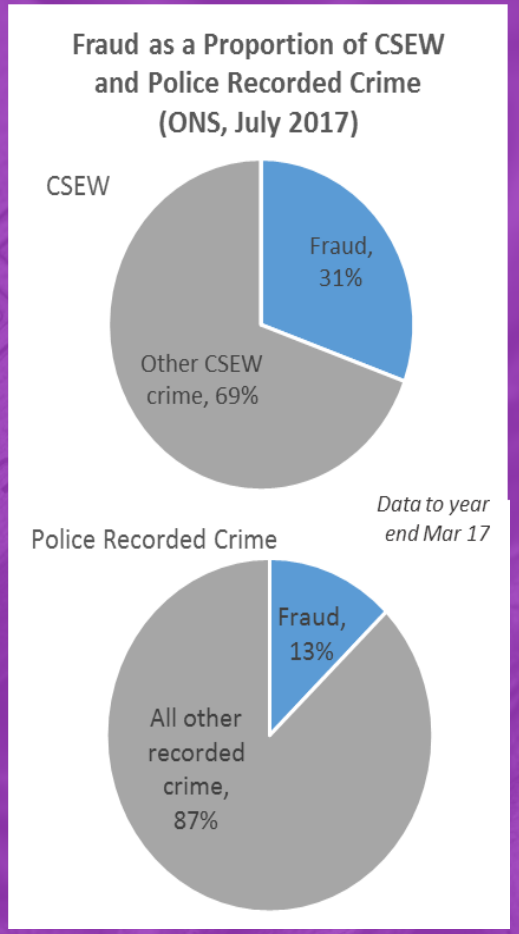
National Fraud Intelligence Bureau Recorded Fraud

NFIB recorded fraud is increasing, up 5% from Mar 2016 to 649,770 offences to March 2017. Some of this increase is likely to be due to improvements made to recording via Action Fraud and increased industry reporting via Cifas and Financial Fraud Action (FFA) UK (now UK Finance).

Office for National Statistics (ONS), July 2017. Data to year end Mar 2017

3. **The profile of fraud types differs considerably between the CSEW and fraud reported directly to Action Fraud.** The CSEW is dominated by banking and credit account fraud, arguably justifying the focus on this type of fraud. However, direct reports to Action Fraud have more consumer/retail and advance fee fraud which may suggest more focus is needed on these for law enforcement.





Fraud Profile Comparisons

Fraud accounts for 31% of CSEW crime but only 13% of recorded crime.

Comparing direct reports to Action Fraud* with the CSEW profile.

- Banking and credit account fraud is the most common type within the CSEW (74%), yet only accounts for 13% of direct reports to Action Fraud.
- Consumer/retail fraud is most common in direct reports to Action Fraud (44%), but makes up 22% of CSEW fraud.

** Direct reports to Action Fraud are used in the comparison of profiles as the closest match to CSEW fraud against individuals. These figures do not include industry reports which appear in NFIB recorded fraud, but they do include some direct reporting by businesses to Action Fraud which cannot be separated out.*

4. **Fraud is significantly under-reported with only 17% of CSEW fraud reported to Action Fraud.** Lack of awareness of Action Fraud and understanding of reporting mechanisms more generally are the main reasons cited for under-reporting. This differs somewhat from the drivers of reporting for other crime types.

Reporting Rate

- Only **17%** of CSEW fraud was reported to the police or Action Fraud.
- This is the third lowest rate within the CSEW, only attempted snatch theft and computer misuse crimes are lower.
- Reporting rates only vary slightly by fraud type.

ONS, July 2017. Data year ending Mar 2017.

Reasons for Not Reporting

The most commonly cited reasons for not reporting suggest problems with the reporting system:

- "never heard of Action Fraud", 66%;
- "thought it would be reported by another authority", 15% (ONS, Ad Hoc Feb 2017).

Academic theories about reporting behaviour for crime in general go some way to explaining other results, e.g.:

- "too trivial/not worth reporting" (5%) or "no loss" (2%) – akin to perceived seriousness;
- "inconvenient/too much trouble" (2%) – cost benefit calculations about value of reporting;
- "Action Fraud could do nothing" (2%) - limitations of reporting system.

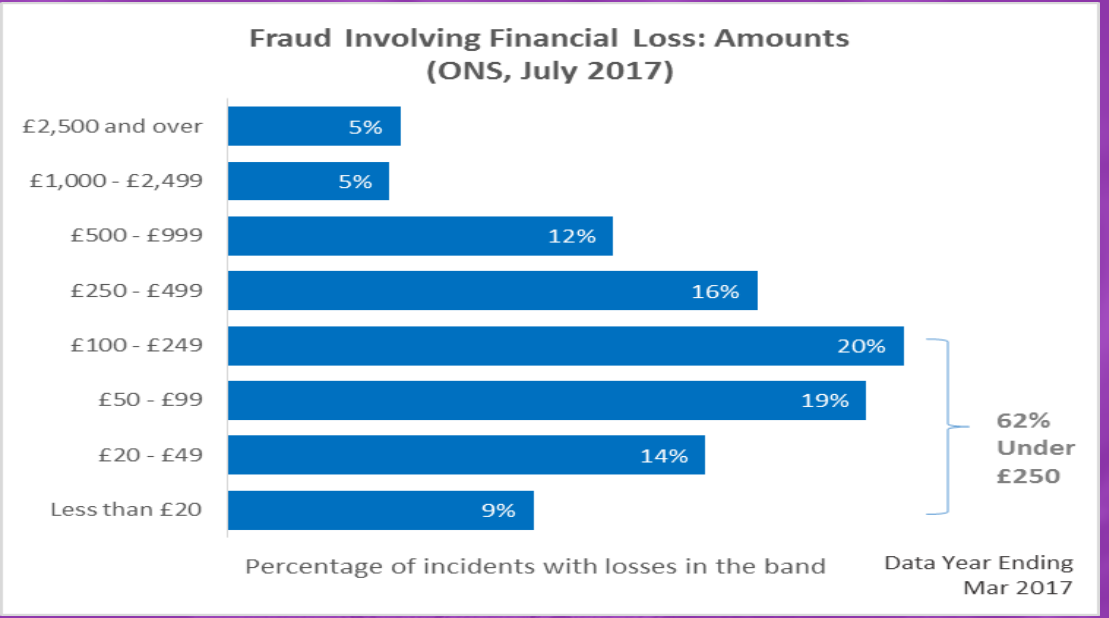
More personal reasons such as feelings of shame/embarrassment, not being believed, feeling at fault may be obscured somewhat in the survey by the way the question is asked.

5. **The majority of losses captured by the CSEW are under £250 (62%). Contrary to popular belief all fraud is not reimbursed.** Almost a quarter get no reimbursement and reimbursement appears largely driven by the fraud type rather than the amount lost.

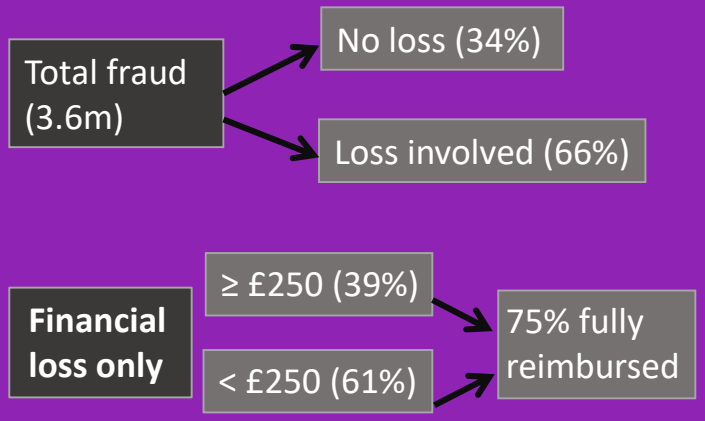
Fraud Loss

- The majority of fraud incidents result in small financial losses under £250 (62%).
- A small proportion (5%) incur losses of £2,500 and over.
- Thus the CSEW does not appear to capture many high-end losses i.e. in the tens of thousands of pounds.

ONS, July 2017.



Loss and Reimbursement (ONS, Jan 2017)



Data to year ending Sept 2016

Reimbursement

Three-quarters of CSEW incidents involving a financial loss are refunded in full (ONS, Jan 2017). But reimbursement varies considerably by fraud type (ONS, Ad Hoc Release June 2016).

- 86% of bank and credit account fraud was fully reimbursed. This seems intuitive given banks have a legal obligation to refund customers for non-authorised transactions.
- But, only 42% of consumer/retail fraud was fully refunded (and 3% partially refunded).

6. **The range of non-financial impacts that a victim can suffer are vast and can have profound effects on individuals** e.g. their relationships, physical and mental health, and reputation. Impacts are not necessarily linked to the scale of the financial loss.

Victim Impacts from Academic Literature

A wide range of impacts on individual victims as a result of fraud have been identified (Button, Lewis and Tapley 2009 and 2014; Kerr *et al*. 2013; Button *et al*. 2015). Impacts are not related to the scale of loss i.e. a small financial loss may still result in a high impact and vice versa.

CSEW Reported Impacts

- Loss of time and inconvenience most frequently reported (22%).
- Reported impacts were similar for fraud with and without loss.
- But there were differences between those reimbursed or not.

For those with no/partial reimbursement:

- more "felt ashamed/ embarrassed/self-blame or similar" (25%, this was 9% if reimbursed);
- more "stopped using specific internet sites" (15% compared to 9%).

ONS, Jan 2017. Data year ending Sept 2016.

7. **There is less variation in the profile of fraud victims than for other crime types**. Victims were more likely to be in higher income households, in managerial/professional occupations and aged 25-54, challenging the common belief that fraud is solely a problem amongst the elderly. Most were victims only once but this may hide true levels of repeat victimisation.

Victim Profile

One in 17 adults in England and Wales (6%) were a victim of fraud in the last year according to the CSEW up to year ending March 2017. But the majority (86%) were victims only once (ONS, Mar 2017).

Adults aged 25–54 more likely to be a victim of fraud (>=7.5%) than 16–24 year olds (4.8%) or those aged 75+ (3.3%).

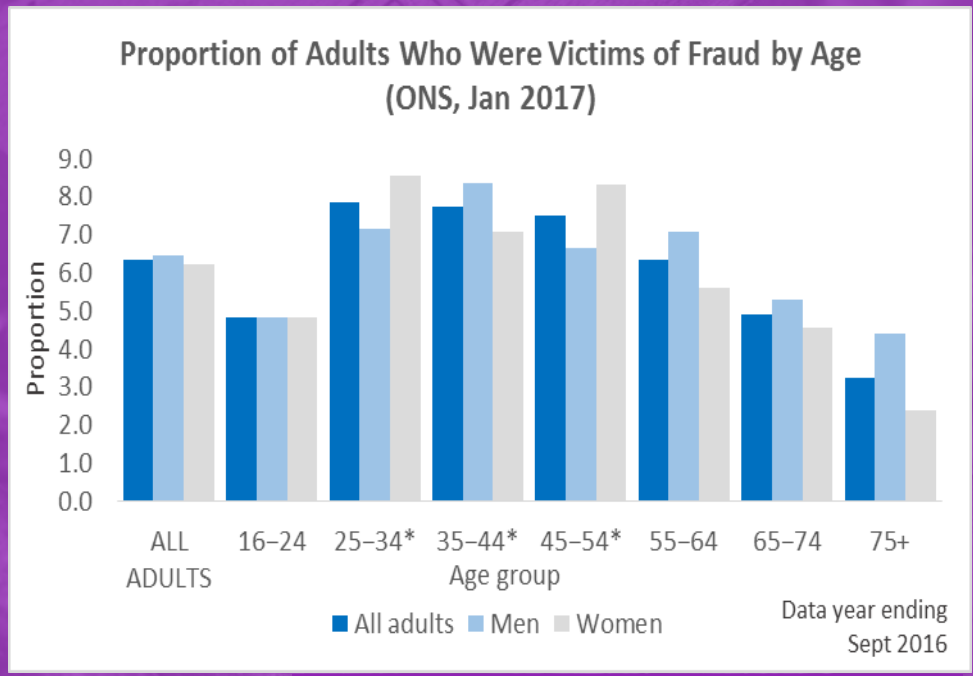
Victimisation is greater in higher income households (8.5%) compared with all other income bands e.g. (<£10k, 5.3%; £10k to <£20k, 5.0%).

Managerial/professional occupations have higher victimisation (8%) than all other occupation types.

Widows are significantly less likely to be a victim than all other marital types (3.3% compared with between 6.5–6.8%).

Victimisation by gender is roughly equal (6.5% for male, 6.2% for females)

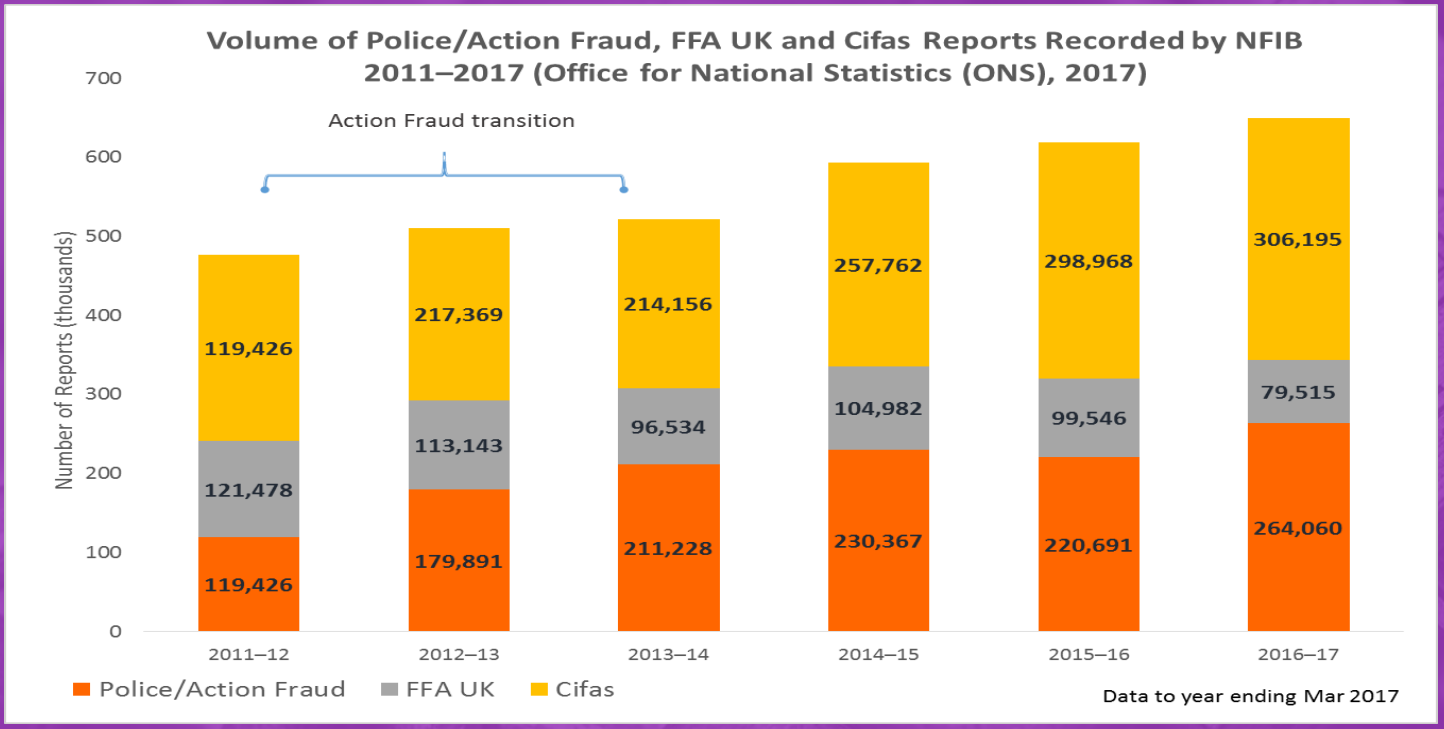
ONS, Jan 2017. Data to year ending Sept 2016.



** Statistically significant compared with those aged 16–24, 65–74 and 75+.*

3. FRAUD AGAINST BUSINESSES

8. **Understanding of the scale and losses from fraud experienced by businesses overall is limited with only a few available data sources.** A large volume of fraud reported to Action Fraud comes via the industry bodies Cifas and Financial Fraud Action (FFA) UK. This accounts for just under two-thirds of National Fraud Intelligence Bureau (NFIB) recorded fraud, but is heavily weighted to fraud in the financial sector.



Business Reporting

More than half (59%) of NFIB recorded fraud is from industry body reports to Action Fraud via FFA UK and Cifas.

Businesses can also report directly into Action Fraud but this cannot be disaggregated in the Action Fraud category.

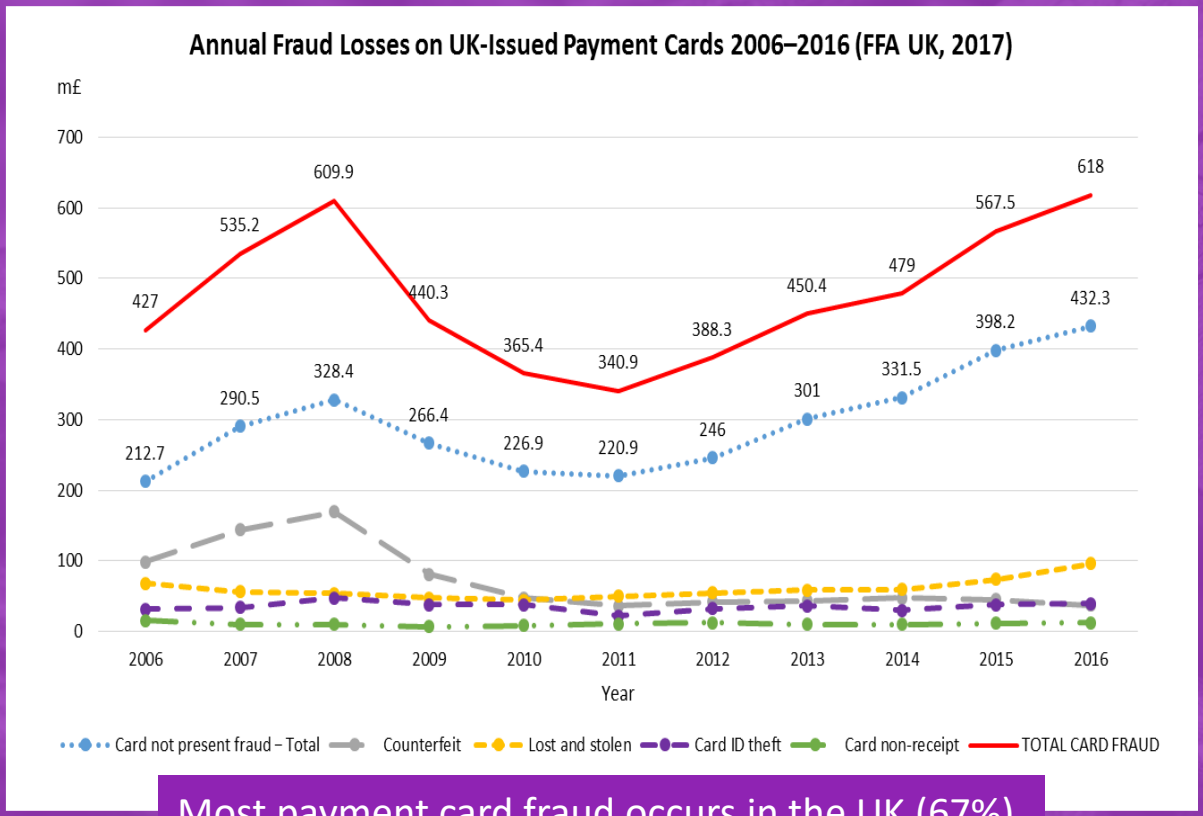
Cifas and FFA UK

- Cifas and FFA UK are membership organisations that collect and refer reports to NFIB. Membership is heavily weighted to the financial sector. Data therefore represents a good proxy for financial sector fraud but not fraud against other businesses, particularly small and medium enterprises (SMEs).
- FFA UK also collects data for UK-issued card, cheque and remote banking fraud (1.9m cases 2016/17). Only a subset of which are referred to NFIB where there is sufficient intelligence value for the police.

9. **The volume and losses from fraud affecting the financial sector tend to be driven by payment/plastic card fraud (FFA UK)**. Card not present fraud in particular represents a high proportion of both the losses (70%) and volume (79%) from payment card fraud and this has been increasing year-on-year since 2010/11.

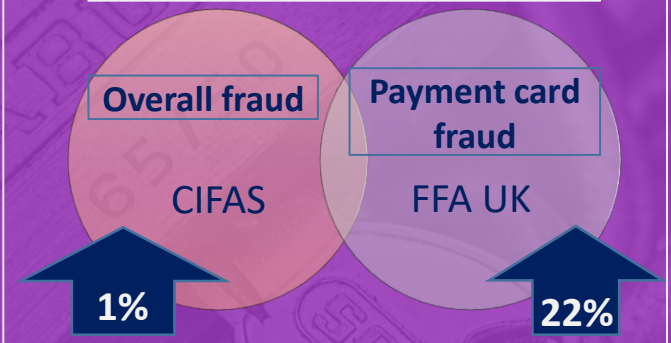
Fraud Losses (FFA UK, 2017)

- Reported losses for all fraud in 2016 totalled around **£769m**, an increase of **2%** from 2015.
  - Payment card fraud accounts for the vast majority of this total loss (£618m, 80%) with card not present fraud alone totalling £432m (70% of payment card fraud).
  - Remote banking (online and telephone banking) makes up 18% of the total loss and cheque fraud 2%.



Most payment card fraud occurs in the UK (67%).

Volume of Fraud



- Both Cifas and FFA UK reported increases in fraud for 2016 compared with 2015 (Cifas, 2017; FFA UK, 2017)
- Card not present fraud represents 79% (1.4m) of the volume of payment card fraud (1.8m) (FFA UK, 2017).

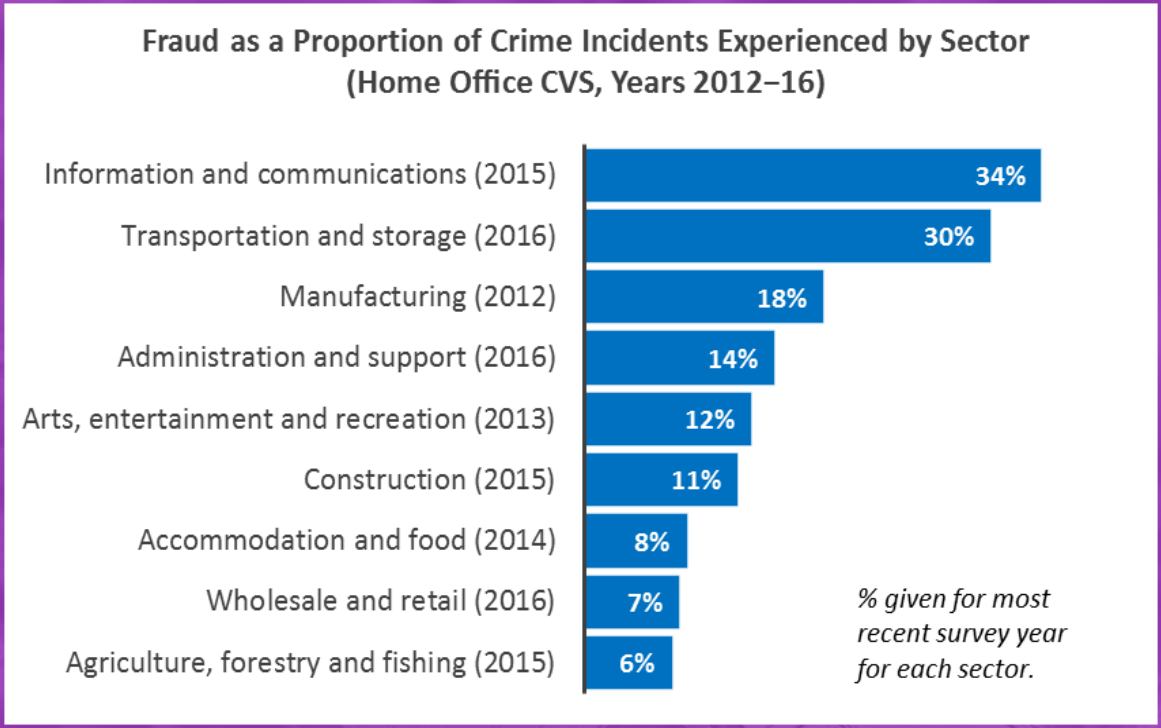
10. **Knowledge of the scale and impact of fraud on non-financial businesses is limited.** Data available suggest it disproportionately impacts on certain sectors but for many retailers theft is still the most common crime reported.

Commercial Victimisation Survey

The Commercial Victimisation Survey (CVS) shows some sectors are disproportionately affected by fraud:

- for the information and communications sector, 34% of incidents were fraud;
- in the transportation and storage sector, 30% were fraud; and,
- the remaining sectors ranged from 6–18% of incidents being fraud.

Home Office CVS. Survey Years 2012-16

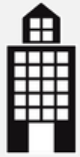


NB. The CVS does not cover the financial sector.

Fraud Across Business Sectors

- The 2016 Retail Crime Survey (2017) reported that customer theft accounted for 75% of incidents in 2015-16, with fraud at 18% (down from 28% in 2014-15). However, fraud was estimated to account for 28% of the direct cost of crime to UK retailers (£183m).
- In the CVS theft was the most common crime reported against the wholesale and retail sector (81% of crimes) and 58% of the administration and support sector. Fraud represented just 7% and 14% respectively (Home Office CVS, 2017).

11. Reasons for under-reporting among businesses will have many parallels with those for individuals, i.e. awareness of where to report and the perceived seriousness of the incident. However, studies highlight **concerns over damage to reputation, a culture of not reporting insider-fraud and confidence in the police to act, as important reasons for businesses.**

Trust in the Police 	The Retail Consortium Survey (BRC, 2016) pointed to a lack of capacity across law enforcement to respond effectively to fraud facing businesses: 89% of respondents reported no improvement in the service from the police once a fraud had been reported.
Seriousness of Incident 	Cyber-enabled fraud tends to be low impact but high volume. Its impact is mostly felt in the aggregate and long term through high indirect costs associated with prevention, incident response and reputational damage (Anderson *et al*. 2012). Thus any one incident may not appear serious enough to be 'worth' reporting.
Response / Focus on Short-Term Need 	The majority of fraud against business appears to be cyber-enabled. Yet the Cyber Security Breaches Survey (DCMS, 2017) suggests only 7% of those experiencing a disruptive breach (which also includes cyber-dependent crimes) reported it to Action Fraud. Around four in ten reported to an outsourced cyber security provider. This may be linked to a need to resolve issues quickly and/or who is regarded as most appropriate to respond. But lack of reporting will not address longer-term issues.
Insider-Fraud and Organisational Culture 	A significant proportion of fraud against business is believed to be insider-enabled. In many cases companies chose not to report this to the police (Boony, Goode and Lacey, 2015). Evidence from Swiss companies found that the size of business and corporate culture predict reporting of insider-enabled corporate crime, including theft and fraud (Isenring *et al.* 2016). Micro-businesses and those with 'family' corporate cultures are also less likely to report employee crime.

12. **Developments in fraud prevention measures (e.g. chip and PIN) and changes to fraudsters' methods may drive changes in trends over time.** However, the effectiveness of fraud prevention techniques is hard to demonstrate empirically, with only limited independent and reliable evidence available.

Displacement Hypothesis (Anderson *et al*, 2012)

Decline in counterfeit card and other card losses post 2008 – believed to mark the point at which chip and PIN and other initiatives were rolled out

Criminals moved to using rogue points of sale devices and ATM skimmers to steal card and PIN data for use in fall back magnetic stripe transactions

Fewer ATMs accept magnetic stripes so criminals respond by cashing out overseas.

This hypothesis would suggest changing developments in crime prevention techniques are affecting fraudsters' behaviour.

FFA UK Profile

FFA UK (2017) also suggests **methods used by fraudsters have adapted over time** and are driving trends.

- Increases in payment card fraud since 2011 are propelled by online attacks and data breaches (including malware and hacking), and impersonation/ deception scams to obtain card details.
- There has been an increase in distraction techniques and scams to acquire PIN & card details.

However, empirical evidence to support theories around changing patterns of fraud and the potential benefit of fraud prevention techniques such as these is limited and would warrant further research/analysis.

4. FRAUD AND THE CRIMINAL JUSTICE SYSTEM

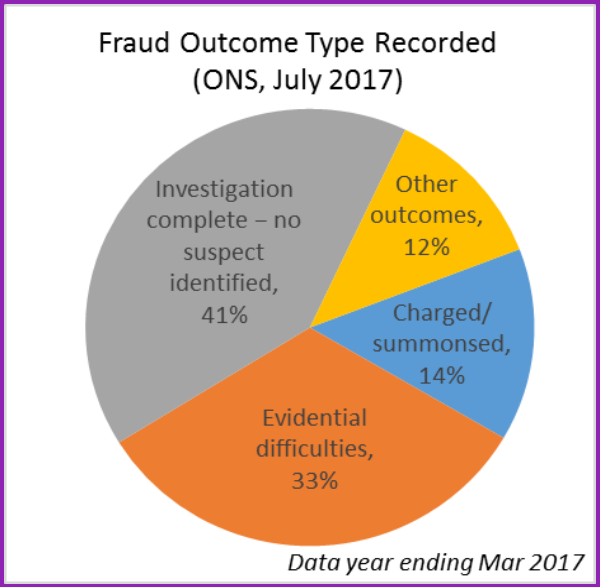
13. **Reported frauds will not always contain viable leads for a successful investigation and criminal conviction. Attrition of fraud cases occurs across all parts of the criminal justice process.** Policing outcome rates increased by 14% in the year ending March 2017, but this was driven by a number of cases where investigations were completed with no suspect identified.

Police Outcomes

The number of police outcomes recorded increased by 14% to 44,887. Largely driven by an increase in the outcome "Investigation complete – no suspect identified".

Overall, 14% of fraud outcomes resulted in a charge/summons.

ONS, July 2017. Experimental statistics.



Disseminations to Police Forces

Disseminations to forces decreased by 4% for year ending March 2017.

Office for National Statistics (ONS), July 2017. Experimental statistics.

NB. Outcomes and disseminations should not be directly compared for a given year as disseminations may not happen straightaway and investigations can be lengthy.

Disruptions

As well as helping to secure arrests/charges, intelligence from Action fraud reports can inform other disruption activity.

- In 2017, National Fraud Intelligence Bureau (NFIB) and Action Fraud's Prevention and Disruption team disrupted 807 websites, three quarters of which (74%) were based on information from Action Fraud reports (NFIB, ad hoc data request, Apr 2018).

Attrition

Home Office research conducted into the level of attrition and policing outcomes for frauds reported in 2013 led to a range of recommendations for tackling attrition.

Actions are being taken via the new Action Fraud and NFIB IT systems to help address attrition and improve recording processes for outcomes, including recording where fraud reports were used for disruption and intelligence purposes (Scholes, 2018).

14. **The number of defendants prosecuted for fraud declined in 2016 compared with 2015. However, once proceeded against the conviction ratio for fraud is high (87%).** Fraud cases take a disproportionate amount of time to reach a conclusion compared with other crimes.

Court Proceedings and Outcomes

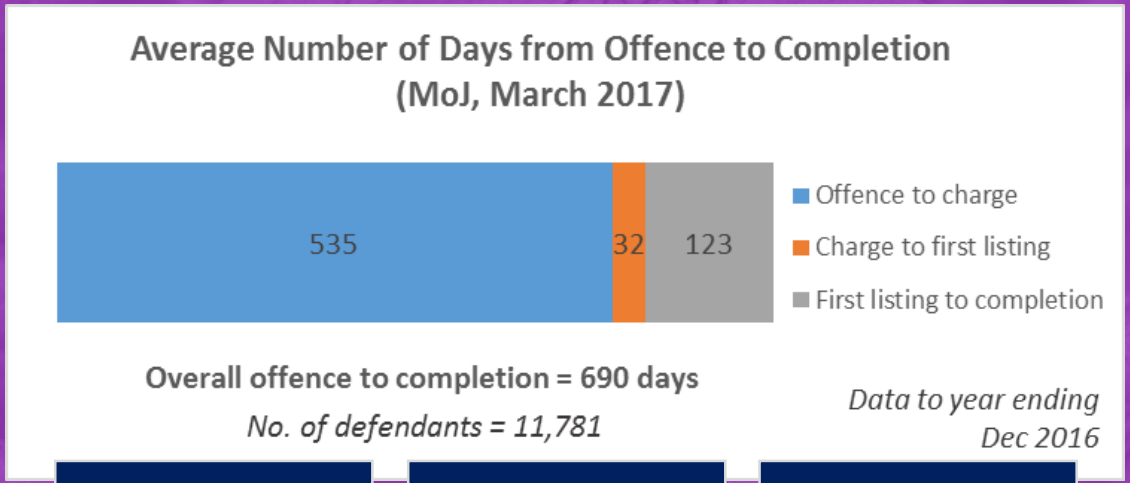
- The number of defendants proceeded against at magistrates' court was down 20% (2015 to 2016).
- The conviction ratio for fraud in 2016 was 87%, higher than for all offences (84%) and an increase from 2015 (83%).
- Nearly half of convictions in 2016 (48%) were for cheque, plastic and online account fraud.

Ministry of Justice (MoJ), May 2017. Data year ending Dec 2016.

Timeliness

Fraud offences take a disproportionate amount of time to reach a conclusion.

- The mean time to completion was 690 days, though this is skewed by a small number of lengthy cases.
- The median time was 451 days.
- Most of the time is from offence to charge with a mean of 535 days, over 4.5 times more than the mean for *all* offences.



Mean time to completion 6 x that of theft

Mean time second only to sexual offences

Median time to completion 8 x that of theft

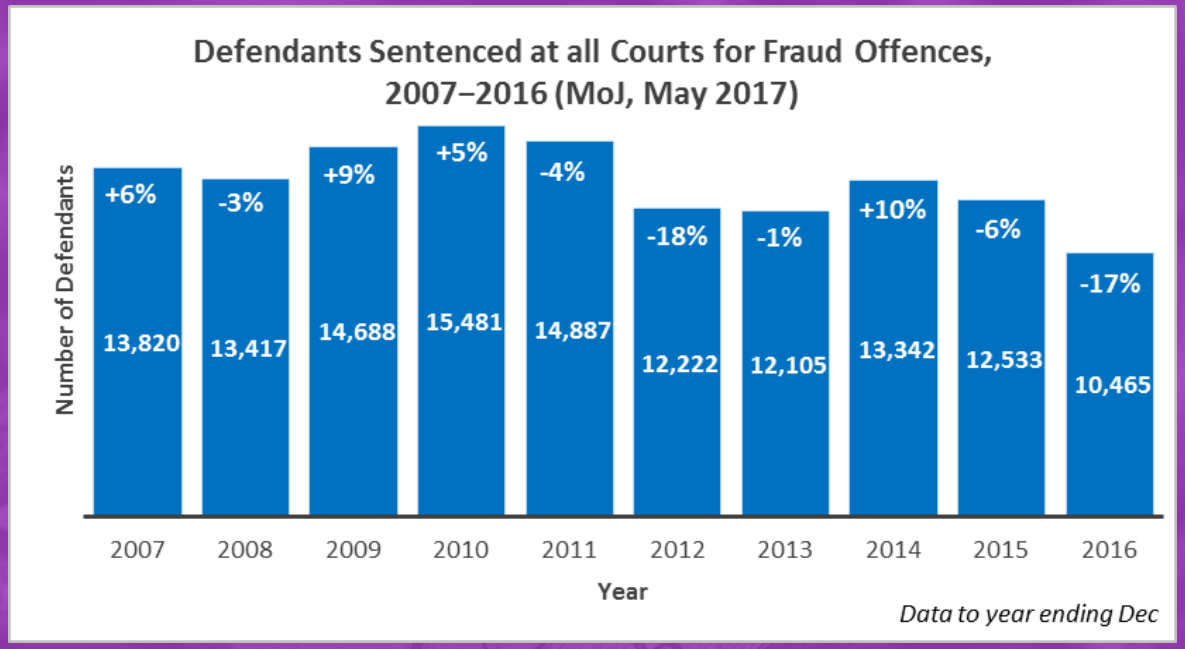
NB. MoJ data only have limited comparability with National Fraud Intelligence Bureau (NFIB) recorded fraud. MoJ data encompasses a wider range of prosecutions from agencies outside of the police and these data are difficult to disaggregate. Furthermore, timescales for cases reaching court can be lengthy, making comparison over time difficult.

15. **The number of individuals sentenced for fraud has declined since 2010.** When sentenced, most receive either community or suspended sentences; a fifth receive immediate custody.

Sentencing

- The number **sentenced for fraud** declined by 17% in 2016, continuing a general downward trend from 2010 (similar to *all* crime).
- 58% of those sentenced in 2016 received either a **community sentence** or a **suspended sentence,** with 21% sentenced to **immediate custody**.
- The number sentenced to immediate custody declined by 5% in 2016 from 2015 (to 2,206).
- However, the proportion sentenced (the custody rate) increased by 2.6 percentage points from 2015.
- The **average custodial sentence length** was 19.2 months. Theft by comparison was 9 months.

MOJ, May 2017.
Data year ending Dec 2016.



Views on Sentencing

There is little evidence of victims views of court outcomes but qualitative research on victim perceptions of sentencing of fraudsters suggests sentencing should take into account:

- the wider impact on the victim beyond monetary loss;
- the value of the fraud; and,
- the degree of planning and organisation by the fraudster.

Participants believed r**estorative justice** to be a particularly good sentencing option. Custody was felt to be important if there were sufficient aggravating factors. (Button *et al*. 2015).

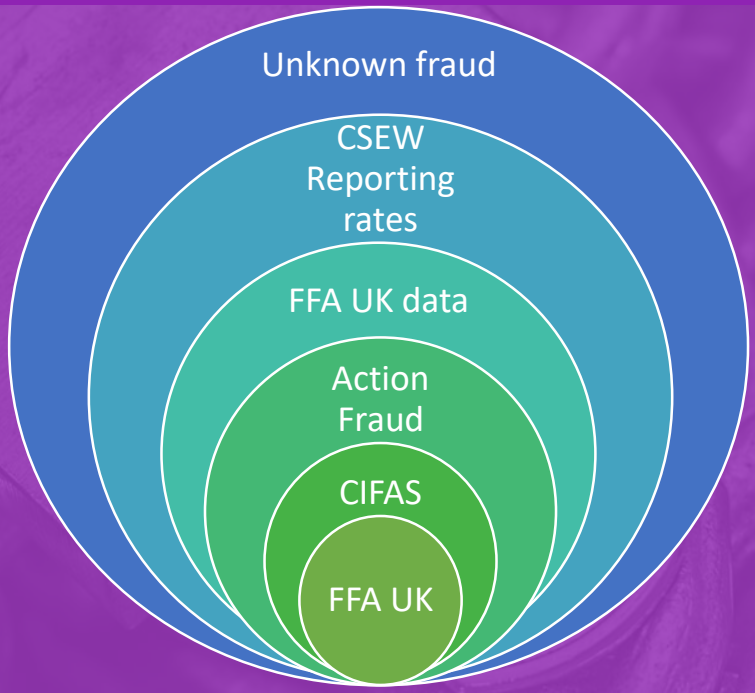
16. Despite considerable recent improvements in the reporting and recording of fraud, it is likely that what is known about fraud is just the tip of the iceberg. **The unique nature of fraud means it is very difficult to assess and measure accurately to understand the true scale and nature of fraud.**

True Scale of Fraud

Considerable improvements have been made to the reporting and recording of fraud, e.g. central reporting via Action Fraud; Cifas and Financial Fraud Action (FFA) UK data included in recorded crime; and fraud added to the Crime Survey for England and Wales (CSEW).

However, the scale of fraud will remain difficult to assess accurately for a variety of reasons, including but not limited to the following.

- Under reporting, e.g. due to feelings of shame/ embarrassment or concerns over business reputation.
- Individuals not believing they are a victim.
- Businesses not willing, or able, to look internally at fraud risk.
- Lack of awareness or trust in reporting systems.
- Unaware of victimisation.



As a result there is some confidence around known fraud (reports to Action Fraud and other bodies) and some insight into under-reporting e.g. CSEW reporting rates for individuals. However, there is little or no ability to unpick the scale and nature of 'unknown' fraud e.g. the extent of under-reporting in businesses, or fraud not recognised by victims. Thus it is difficult to understand the true scale and nature of fraud.

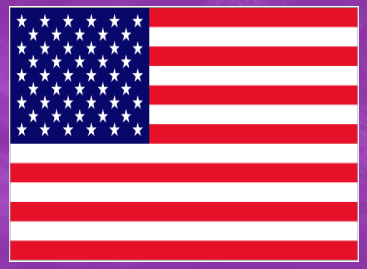
17. Whilst there are similar systems in Australia, Canada and the USA for reporting and intelligence analysis of fraud cases, **no other national fraud system appears to be as comprehensive as Action Fraud/NFIB**. Other systems have a narrower focus, either in terms of their breadth of coverage or in their range of intelligence analysis functions.

International Systems

Australia – The Australian Cybercrime Online Reporting Network (ACORN) model is perhaps the closest to the UK's and the most recent version was launched in 2014. It is a national policing initiative that provides an online reporting mechanism for the public to report cyber crime (such as hacking, online scams, online fraud, identity theft and attacks on computer systems) securely. The remit includes:

- production of awareness-raising material and advice to victims;
- using data to understand the enablers of cyber crime;
- making referrals to law enforcement agencies for action via the Australian Criminal Intelligence Commission.

Canada - The Canadian Anti-Fraud Centre (CAFC) is a national centralised fraud repository. It was established in 1993 but only looked at telemarketing fraud under the title 'Project PhoneBusters'. It expanded to its current model in 2010.
The CAFC has prevention and education, disruption and intelligence gathering functions, but it is limited to mass marketing fraud and identity fraud.



USA – The Internet Crime Complaint Centre (ICCC), established 2000, is an online self-report tool for the public to submit information to the FBI regarding internet-facilitated criminal activity. It includes online fraud e.g. intellectual property rights, hacking, espionage, money laundering and identity theft. The ICCC analyse and disseminate information for investigative and intelligence purposes to law enforcement agencies and for public awareness.

Button and Cross, 2017

Appendix

Fraud Against Individuals: Fraud Groups and Fraud Types

INDIVIDUAL VICTIMS

Fraud Groups	Fraud Types
Bank & credit card fraud	Payment card fraud Prepayment card fraud
Consumer/retail fraud (also known as non-investment fraud)	Online shopping and auctions Consumer phone fraud Door-to-door sales and bogus tradesmen Computer software service fraud Ticket fraud
Advance fee fraud	'419' scams Lottery scams Dating scams Fraud recovery scams Inheritance fraud Rental fraud Counterfeit cashier's cheque and banker drafts
Investment fraud	Boiler room scams Pyramid or ponzi schemes Time shares and holiday clubs
Pension fraud	Pension fraud on pensioners Pension liberation fraud
Other scams	Charity donation scams Gaming fraud 'Stranded traveller' scams 'Fake escrow' scams

Fraud Against Businesses: Fraud Groups and Fraud Types

FINANCIAL SERVICES SECTOR

Fraud Groups	Fraud Types
First party fraud	Application fraud Transaction fraud False insurance claims Pension fraud
Third party fraud	Payment (card) fraud Business identity theft 'CEO fraud' Mandate fraud Remote banking fraud
Fraud by employees & others	Procurement fraud False accounting Fraudulent employee exploitation of (business/client) assets Bankruptcy and insolvency offences Insider dealing Insurance broker fraud

OTHER BUSINESS

Fraud Groups	Fraud Types
Fraud by customers	Payment card fraud Voucher fraud Customer account takeover Retail fraud • Refund fraud • Label Fraud • Obtaining goods with no intention to pay Phone contract fraud
Fraud by employees & others	Procurement fraud False accounting Fraudulent employee exploitation of (business/client) assets Bankruptcy and insolvency offences 'CEO fraud' Mandate fraud Short/long firm fraud Gaming frauds PABX fraud Business identity theft

References

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T. and Savage, S. (2012) *Measuring the Cost of Cybercrime.* Conference paper. January 2012.

Boony, P., Goode, S. and Lacey, D. (2015) 'Revisiting Employee Fraud: Gender, Investigation Outcomes and Offender Motivation', *Journal of Financial Crime,* vol. 22 (4). pp. 447–467.

British Retail Consortium (2016). *BRC Retail Crime Survey 2015.* www.brc.org.uk

British Retail Consortium (2017), *2016 Retail Consortium Survey*. *www.brc.org.uk*

Button, M. and Cross, C. (2017) *Cyber Frauds, Scams and their Victims.* London: Routledge.

Button, M., Lewis, C. and Tapley, J. (2009) *Fraud Typologies and the Victims of Fraud Literature Review.* London: National Fraud Authority.

Button, M., Lewis, C. and Tapley, J. (2014) 'Not a victimless crime: The impact of fraud on individual victims and their families', *Security Journal,* 27 (1), pp 36–54.

Button, M., McNaughton Nicholls, C., Kerr, J. and Owen, R. (2015) 'Online Fraud Victims in England and Wales: Victims' Views on Sentencing and the Opportunity for Restorative Justice?', *The Howard Journal,* vol. 54 (2), pp 193–211.

Cifas (2017) *Fraudscape 2017: External and Internal Fraud Threats – Essential Reading for Fraud and Financial Crime Strategists.* www.cifas.org.uk.

Department for Culture, Media and Sport (2017) *Cyber Security Breaches Survey 2017: Main Report.*

FFA UK (2017) *Fraud the Facts 2017: The Definitive Overview of Payment Industry Fraud.* www.financialfraudaction.org.uk

Home Office (2013) *Crime Against Businesses: Headline Findings from the 2012 Commercial Victimisation Survey,* January 2013.

Home Office (2014) *Crime Against Businesses: Headline Findings from the 2013 Commercial Victimisation Survey,* February 2014.

Home Office (2015) *Crime Against Businesses: Findings from the 2014 Commercial Victimisation Survey,* April 2015.

Home Office (2016) *Crime Against Businesses: Findings from the 2015 Commercial Victimisation Survey.* Statistical Bulletin 03/16, April 2016, ed. Williams, L.

Home Office (2017) *Crime Against Businesses: Findings from the 2016 Commercial Victimisation Survey.* Statistical Bulletin 06/17, ed. Williams, L.

Isenring, G. L., Mugellini, G. and Killias, M. (2016) 'The Willingness to Report Employee Offences to the Police in the Business Sector', *European Journal of Criminology 2016,* vol. 13 (3), pp 372–392.

Kerr, J., Owen, R., McNaughton Nicholls, C. and Button, M. (2013) *Research on Sentencing Online Fraud Offences*, Sentencing Council, June 2013.

Ministry of Justice (2017) *Criminal Court Statistics Quarterly. Data to year ending December 2016,* March 2017.

Ministry of Justice (2017) *Criminal Justice System Statistics. CJS Outcomes by Offence 2006 to 2016. Pivot table analytical tool for England and Wales*, May 2017.

Office for National Statistics (2017) *Crime in England and Wales: Year Ending September 2016.* Statistical Bulletin, January 2017.

Office for National Statistics (2017) *User Requested Data: Percentage of incidents of fraud and computer misuse reported to Action Fraud, and reasons for not reporting incidents to Action Fraud, year ending September 2016 CSEW.* Ad Hoc Release, February 2017.

Office for National Statistics (2017) *Reimbursement of Money Lost to Victims of Fraud, by Offence Type, Year Ending September 2016, CSEW (Experimental Statistics).* Ad Hoc Release, June 2017.

Office for National Statistics (2017) *Crime in England and Wales: Year Ending March 2017. Appendix, bulletin, experimental and crime outcomes tables*. Statistical Bulletin, July 2017.

Scholes, A (2018). *The Scale and Drivers of Attrition in Reported Fraud and Cyber Crime.* Home Office Research Report 97.

Acknowledgements

This evidence review was compiled by Laura Blakeborough and Sara Giro-Correia for the Home Office Analysis and Insight Unit with support from Samantha Dowling and Tom Bucke.

The authors would like to thank policy colleagues for their support for this work – particularly Tim France and Neal Barcoe. Also to statistics colleagues for assistance in compiling and quality assuring data - Lucy Webb and Rosanna Currenti in Home Office statistics and Caroline Youell and Mark Bangs at the Office for National Statistics. Our thanks are also extended to a number of colleagues who helped to quality assure the data and the slide pack in the Home Office and the Ministry of Justice.

ISBN: 978-1-78655-682-0