

# **The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain**

Steven Kemp<sup>a\*</sup>, Fernando Miró-Llinares<sup>b</sup> and Asier Moneva<sup>b</sup>

*<sup>a</sup>Department of Public Law, University of Girona, Girona, Spain; <sup>b</sup>Crímina Research Centre, Miguel Hernandez University, Elche, Spain;*

Correspondence: Carrer Universitat de Girona, 12. Facultat de Dret. 17003, Girona (Spain).

## **The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain**

A reduction in property crime has been a central feature of criminological discussion in the last 25 years, and numerous studies have used police statistics to identify a drop throughout the Western world. However, fraud, which is included in a broad definition of property crime, has typically not been considered in the analysis. This study examines fraud in the Spanish and European context to further understanding of its nature, prevalence, evolution and role in the overall panorama of property crime. Furthermore, the present study explores the extent to which we are experiencing widespread fraud underreporting to police and the implications of this for crime control policy. To this end, the present paper analyses secondary data provided by the Spanish Ministry of Interior, Spanish and European central banking authorities as well as large-scale victimization surveys from a number of European countries. In contrast to other property crimes, the findings indicate that cyber fraud is rising and that reporting is considerably lower. Some of the main reasons for reporting or not reporting fraud victimization are also identified. The dark figure of fraud suggests the design and evaluation of policing and crime prevention policies based solely on police statistics may be inadequate.

Keywords: dark figure; cyber fraud; crime trends; crime drop; evidence-based prevention; crime reporting

### **Defining Before Measuring: An Introduction to Cyber Fraud**

Fraud is by no means a new phenomenon, as evidenced by the Sicilian corn trader who deceived a potential customer for illicit gain in ancient Greece (Johnstone 1998). Yet, fast forward to the present and fraud in the Internet era persists and has developed and expanded within the social and technological changes related to information and communication technology (Clough 2015; Smith 2010). While the Internet brings innumerable benefits, it also presents criminogenic features (Leukfeldt et al. 2017; Miró-Llinares 2012; Savona and Mignone 2004) which have changed the way much crime is committed. Indeed, many authors talk of “cyber”, “online” or “Internet” fraud (Button and Cross 2017; Levi et al. 2017; Miró-Llinares 2013; Williams 2016) to differentiate a modern globalized variant from the traditional face-to-face methods and to highlight the

role that the Internet plays in the twenty-first century manifestations of this property crime. Various types of cyber fraud have been highlighted as particularly widespread; for example, card-not-present fraud is a significant threat (Europol 2018), bank and credit account fraud victimization is extensive (Levi 2017) and romance fraud constitutes a global problem (Whitty 2013). In fact, Williams (2016) has stated that online fraud is Europe's most widespread property crime.

Meanwhile, in studies using police statistics, various authors have identified a property crime drop in Western societies (Fernández-Molina and Gutiérrez 2018; Tonry 2014) or in Europe (Aebi and Linde 2010a; Gruszczyńska and Heiskanen 2018), but fraud or cyber fraud have not been considered in the analysis. As Baumer et al. (2018, p. 40) state, there has been "insufficient attention to differences in crime trends by offense type". A broad definition of property crime includes fraud (Tcherni et al. 2016; Wright and Jacques 2017); thus, it seems useful to consider fraud in the property crime drop analysis.

The present article begins by defining fraud and cyber fraud. The subsequent section employs both police statistics and data provided by central banks to analyse the nature and evolution of the issue in recent years. The aim of this second section is to examine whether fraud trends follow a similar pattern to other property crimes and if their inclusion in the property crime drop analysis affects the overall picture. Next, the article examines the results of victimization surveys from a number of European countries with the objective of estimating fraud prevalence and determining whether there exists a property crime drop or, on the contrary, a cyber fraud "police recording flop" (Caneppele and Aebi 2017). To answer this question, the paper revises fraud reporting rates and motivations in several European countries. Finally, the implications of the findings are discussed with regard to the challenges for policing and prevention policy and whether this exemplifies the new multi-agency cybercrime policing network (Holt and Bossler 2015) in which public police forces no longer play the title role (Wall 2007/10).

The measurement of any criminal act requires prior definition of the act itself (Gadd et al. 2012; Maguire 2012), yet fraud is difficult to define (Anderson et al. 2013; Leukfeldt et al. 2013; Levi and Burrows 2008). Deceit and illicit gain (or evasion of a liability) are the essential elements that have been identified by a variety of sources (American National Academies of Sciences, Engineering, and Medicine 2016; Beals et al. 2015; Miró-Llinares 2013; Levi 2012; Spanish Criminal Code N.D.; UNODC 2015), in other words, fraud is an act of wilful deception that produces an economic benefit (or evasion of a loss) for the deceiver and a loss for the victim. This highlights the broad

nature of fraud and with the aim of providing a clearer vision of the actions that typically constitute fraud in a criminal sense; Button and Cross (2017) adapt Beals et al.'s (2015) Framework for a Taxonomy of Fraud perpetrated against individuals. Their adaptation includes the initial seven categories of fraud and an additional eighth category of identity fraud. All eight fraud types are also present in the Fraud section of Modernizing Crime Statistics by the American National Academies of Sciences, Engineering, and Medicine (2016) as shown in Table 1 <sup>1</sup>.

Table 1. Eight categories of fraud against individuals

Consumer investment fraud.	The use of false information to wilfully deceive a potential investor, commonly involving the promise of high returns.
Consumer products and services fraud	The sale of worthless and non-existent products or worthless, unnecessary and non-existent services as well as unauthorized billing for products and services. Includes very common fraudulent activity such as online marketplace fraud, tech support scams or spoofing websites.
Employment fraud	Consists in an initial payment in return for inexistent future employment or training.
Prize and grant fraud	Advance payments made in expectation of future winnings which do not exist.
Phantom debt collection fraud	An individual is led to believe they must pay an inexistent debt.
Charity fraud	Fraudulently presenting oneself as a genuine charity in order to collect money.
Relationship and trust fraud	The exploitation of a personal relationship with a victim in order to obtain financial gains.
Identity fraud	The use of another party's personal information, such as bank card details, for financial benefit. Personal information is often obtained using deception and when the information is used, deception often occurs in the process, for example, card-not-present fraud involves the deception of a financial institution or payment service.

Source: adapted from Button and Cross (2017) and American National Academies of Sciences, Engineering, and Medicine (2016)

As can be appreciated from the above eight categories, fraud is an extremely wide-ranging issue. On the one hand, it therefore seems surprising that it is often not considered in crime trend analysis; however, on the other hand, this may in fact explain its absence, since definitional difficulties can obstruct recording.

It should be remembered that the above classification refers only to those frauds perpetrated against individuals and not those involving an organizational victim. As

<sup>1</sup> Identity fraud is called identity theft but the definition is the same.

highlighted in Table 2, the National Academies of Sciences, Engineering, and Medicine (2016) and Beals et al. (2015) differentiate frauds committed against organizations. While this article focusses primarily on fraud offences involving individual victims, the existence of organizational victims should be recognized, especially as police and bank data on fraud should include any reports made by these.

Table 2. Fraud against organizations

Fraud against government agencies, programs, regulations, and society	Includes offences such as welfare fraud or tax fraud.
Fraud against an organization or business (public, private, or non-profit)	Subdivided into occupational fraud (carried out by internal actors) and frauds carried out by external perpetrators.

Source: adapted from Beals et al. (2015) and American National Academies of Sciences, Engineering, and Medicine (2016)

As regards the cyber element, cyber fraud is, in short, one of the aforementioned fraud types which is perpetrated via the Internet. This may be as a hybrid crime that combines offline and online activities or a fully online crime (Caneppele and Aebi 2017). Within cybercrime, the role of the Internet can vary significantly, but most cyber frauds fall into McGuire and Dowling's (2013) category of cyber enabled. This means that they are traditional types of fraud that have been enhanced by using the Internet in some capacity. For example, consumer fraud can now be perpetrated through online commercial retailers and market places from almost anywhere in the world in a fraction of the time and with reduced risk of police intervention.

### **Official Statistics, Crime Drop and Fraud in Spain**

As Rosenfeld (2018) stated in his address to the American Society of Criminology, if an evidence-based criminologist wants to know which measures to employ in order to reduce crime, they first need an accurate measure of crime rates. It is necessary to understand the nature and extent of crime so as to inform and evaluate crime control policies and agencies (Fafinski et al. 2010), and, in this sense, various authors have highlighted the importance of fraud measurement (e.g. Levi et al. 2017; Tunley 2014).

The so-called crime drop and its causes have generated great debate in Criminology in the last 25 years. A reduction in property crime has been a central feature of the discussion with numerous authors highlighting a drop in the USA (Blumstein and Wallman 2006; Levitt and Dubner 2005; Zimring 2006), internationally (Tonry 2014;

Tseloni et al. 2010; van Dijk et al. 2012) and Western Europe (Aebi and Linde 2010a; Gruszczyńska and Heiskanen 2018). However, the analysis has typically not examined fraud offences, and it has been suggested that the rise in property crime perpetrated via Internet may be greater than the offline drop (Tcherni et al. 2016), meaning an overall increase in property crime.

It has also been postulated that displacement has taken place from traditional forms of crime to online and hybrid crime (Caneppele and Aebi 2017; Levi 2017; Button and Cross 2017; Miró-Llinares and Moneva 2019; Tcherni et al. 2016). However, there are significant counter arguments against the displacement effect (Farrell and Birks 2018), specifically, a lack of robust evidence, inconsistencies regarding the timing and problems with causal mechanisms. While Farrell and Birks suggest that the timings are inconsistent in the USA, the UK and Australia, they do state that fraud may constitute one form of criminal activity which could plausibly have been subject to online adaptation. In contrast, Miró-Llinares and Moneva (2019) argue that there is enough empirical evidence to support the idea that “increases in criminal opportunities in cyberspace [...] go hand in hand with decreases in criminal opportunities in physical space, particularly with respect to dual crimes” (p. 4), which would help to understand the underlying mechanism of the shift.

The aim of this section is to examine how fraud trends in Spain can add to this property crime drop literature by including, in addition to police statistics, fraud data provided by banks. Combining data sources may shed new light on fraud prevalence and trends. If, as some authors suggest, displacement has indeed taken place between offline crime and cybercrime, it should follow that any rise in cyber fraud would be accompanied by a similar decrease in traditional fraud.

The analysis begins with crime drop statistics provided by the Spanish Ministry of the Interior (MIR). It should be highlighted that crime statistics in Spain have historically been notable for their unreliability (Aebi and Linde 2010b). However, transparency has improved in recent years, and they serve as a starting point for the present analysis. Furthermore, official crime statistics are often used to inform criminal policy, and as such it is important to evaluate their reliability with regard to fraud.

In Figure 1<sup>2</sup>, the Spanish Ministry of the Interior highlights a general crime drop (violent and property crime) between 2008 and 2016. The timing for the Spanish crime drop is considerably later than the trend identified in America; however, it has been shown that certain crime types increased in the European context until at least 2007 (Aebi and Linde 2012), crime trends in Europe vary from those in the USA (Killias and Aebi 2000) and occasional lags in crime trends between particular countries have been identified (Tonry 2014).

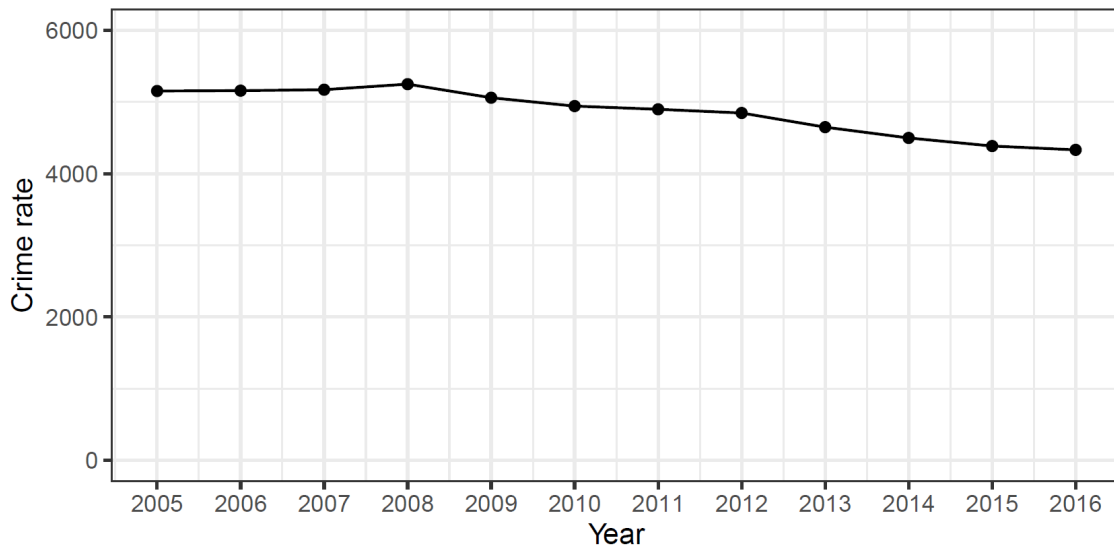


Figure 1. Police recorded crime in Spain per 100,000 population, 2005–2016. Source: Spanish Ministry of Interior.

[http://www.interior.gob.es/documents/10180/6865255/Presentacion+ministro\\_Balance+de+Criminalidad+2016.pdf](http://www.interior.gob.es/documents/10180/6865255/Presentacion+ministro_Balance+de+Criminalidad+2016.pdf)

According to the Spanish National Police (2016)<sup>3</sup>, the steep crime reduction detailed between 2012 and 2016 is due to increased police efficiency as a result of the introduction of a strategic plan focused on the fight against terrorism, organized crime, irregular immigration, human trafficking and cybersecurity, amongst others. As evidence

---

<sup>2</sup> All data transformation and visualization have been executed using the tidyverse R package version 1.3.0 (Wickham et al. 2019) in RStudio version 1.2.5033 for the R free software version 3.6.2.

<sup>3</sup> Retrieved from [http://www.interior.gob.es/prensa/noticias/-/asset\\_publisher/GHU8Ap6ztgsg/content/id/6222655](http://www.interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/6222655).

of its improved efficiency related to cybercrime, the police force stated that in this period, there was a significant rise in the number of detentions for cybercrimes, including identity fraud and online fraud.

Figure 2 shows the official data for the property crime types which are included in the MIR crime rate calculation (theft, robbery with forced entry, violent robbery, vehicle theft, fraud). With the exception of fraud, these show a decrease from 2010 (from when data for individual crimes is available) and above all from 2012 onwards.

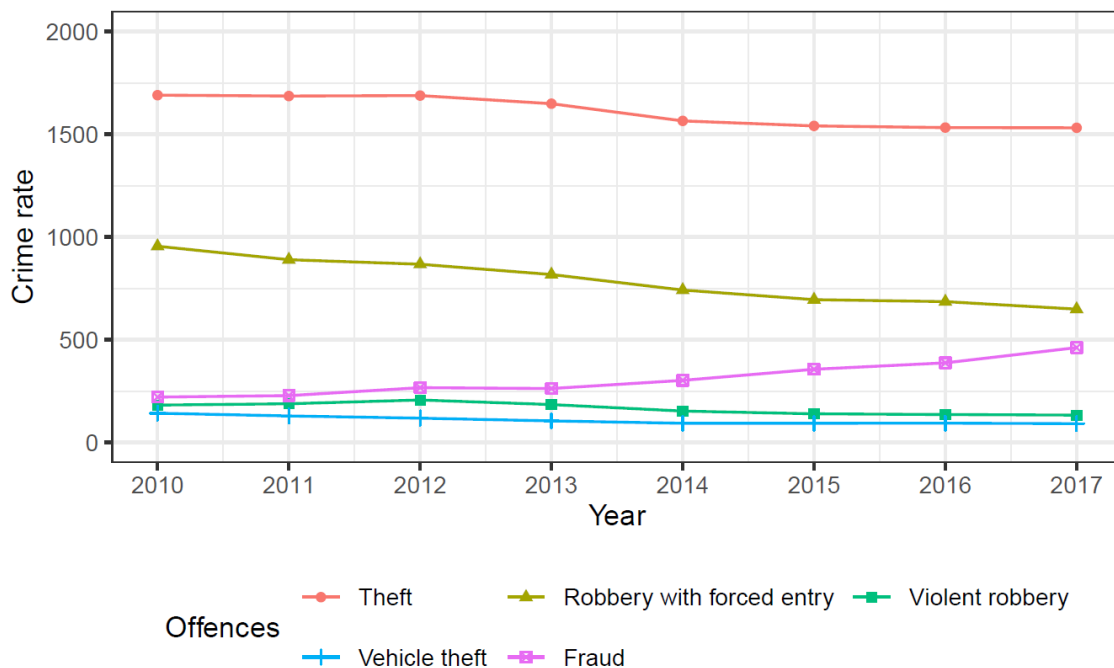


Figure 2. Police recorded property crime in Spain per 100,000 population, 2010–2017. Data includes cyber fraud figures. Source: Spanish Ministry of Interior. <https://estadisticasdecriminalidad.ses.mir.es/>

As detailed in Figure 3, data from the Ministry of the Interior show that reported frauds rose over 100% in the same period, increasing from approximately 200 per 100,000 inhabitants to over 450. This increase is particularly pronounced from 2013 to 2017.



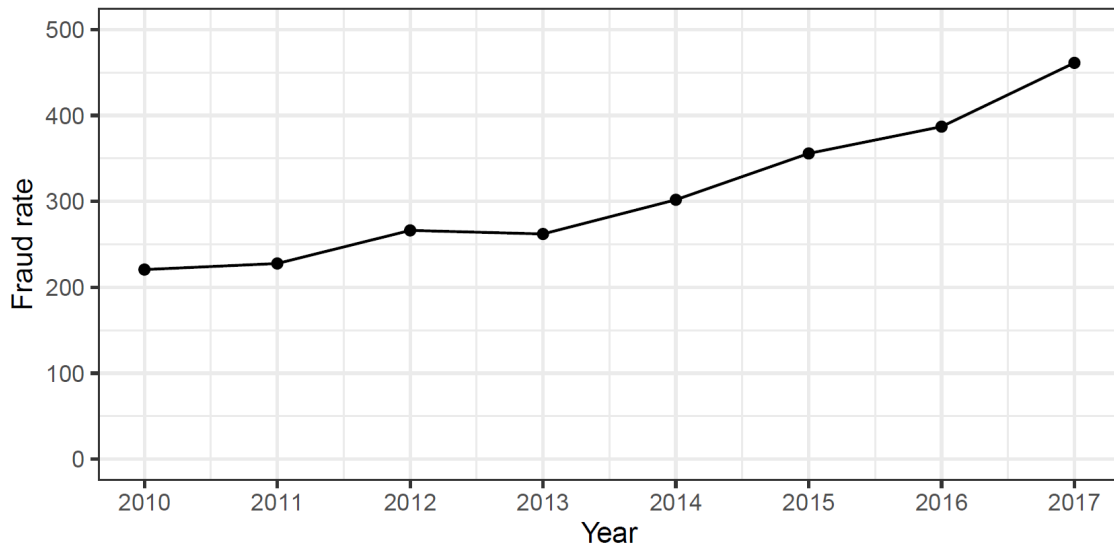


Figure 3. Police recorded fraud in Spain per 100,000 population, 2010–2017. Data includes cyber fraud figures. Source: Spanish Ministry of Interior. <https://estadisticasdecriminalidad.ses.mir.es/>

However, the unreliability of police data for crime trend analysis has been highlighted (Baumer et al. 2018; Van Dijk 2015), and it is highly unlikely that these official statistics provide an accurate picture of fraud prevalence as underreporting of fraud to police is common (Button and Cross 2017; Caneppele and Aebi 2017; Maras 2017; Wall 2007/10). There are a number of possible reasons explaining the low level of fraud reporting to police:

- The victim is often unaware of their victimization due to not checking their bank accounts or to a lack of understanding about financial cybercrime.
- The victim may be unsure of where to report cybercrime.
- In accordance with expected utility theory, if the amount lost is relatively insignificant, the victim may decide not to report as the time and resources required outweigh the losses that may be recovered.
- The victim may only need to report to their financial institution in order to obtain a reimbursement; thus, the police are not informed unless it is a requirement to recover losses.
- The victim may be embarrassed by the events or view themselves as partially responsible. In this sense, not reporting can be a defence technique to avoid secondary victimization.

- The victim may not believe the police are experts in cybercrime and therefore lack confidence in their ability to respond. They may believe the police do not have the resources or expertise to investigate and identify the perpetrators.
- The victim might not want to share their Internet activity with police in order to aid their investigations.

While many of the reasons enumerated above are applicable to both individuals and organizations, underreporting by the latter is strikingly common, and as a result, academic research on the nature and prevalence of fraud against organizations is scarce (Jansen et al. 2017; Tunley 2014). It has been noted that organizational victims prefer to carry out their own investigations and responses to fraud (Wall 2007/10). Furthermore, organizations involved in financial transactions are actively encouraged to act as a “front line of defence” to aid police services that do not have the resources necessary to be the main actor in fraud prevention (Levi and Burrows 2008).

### ***Bank Statistics***

As a consequence of significant underreporting to law enforcement agencies, it is necessary to identify statistics from alternative sources in order to obtain a clearer picture of crime trends (Caneppele and Aebi 2017). In Spain, one such industry source is the Bank of Spain (BoS). In its report entitled Annual report on the supervision of financial market infrastructures <sup>4</sup>, BoS provides statistics on fraudulent transactions recorded by the payment systems networks used in this territory. This means that it registers fraudulent transactions carried out in Spain using Spanish bank cards and overseas bank cards, as well as transactions conducted outside Spanish territory using bank cards emitted in Spain. BoS understands a fraudulent transaction to be a transaction involving a bank card, bank card information or bank account without the owner's authorization. The Spanish Criminal Code Article 248.2 (a) and (c) uses the same definition. In accordance with the terminology used in Section 1, this means BoS provides data on identity frauds. It should be noted that when reported to the Spanish police, these are recorded as bank frauds and are also included within the general fraud statistics.

---

<sup>4</sup> Available from:

[https://www.bde.es/bde/es/secciones/informes/Publicaciones\\_an/Memoria\\_anual\\_so/index2016.html](https://www.bde.es/bde/es/secciones/informes/Publicaciones_an/Memoria_anual_so/index2016.html).

Information on fraud has only been included in the BoS reports since 2012. In the period for which information is available at the time of writing (2012–2016) and as shown in Figure 4, there was a rapid increase in the volume of identity fraud. In this 5-year period, the rate of fraudulent transactions rose by over 50%.

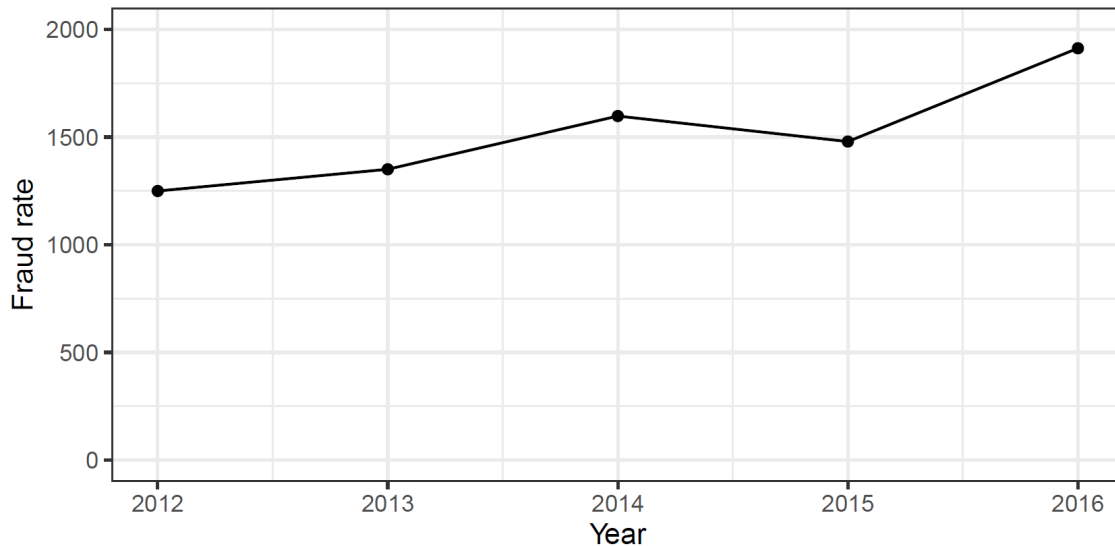


Figure 4. Fraudulent bank transactions per 100,000 population, 2012–2016. Data includes cyber fraud figures. Source: BoS

Interestingly, the BoS data reveals that this rise is due to increases in remote fraudulent transactions, in other words, fraud with a substantial cyber component (Figure 5). This is particularly relevant for the displacement debate as while non-remote bank card fraud has decreased slightly, the reduction is significantly less pronounced than the increase in cyber fraud. There are two possible explanations for this. On the one hand, there may be only slight displacement between the two types of fraud, and thus, the rise is due to the appearance of new fraud and fraudsters. On the other hand, it could result from the increased criminal opportunities provided by cyberspace, whereby a tactical crime displacement has occurred and the new modus operandi has permitted an escalation in offending.

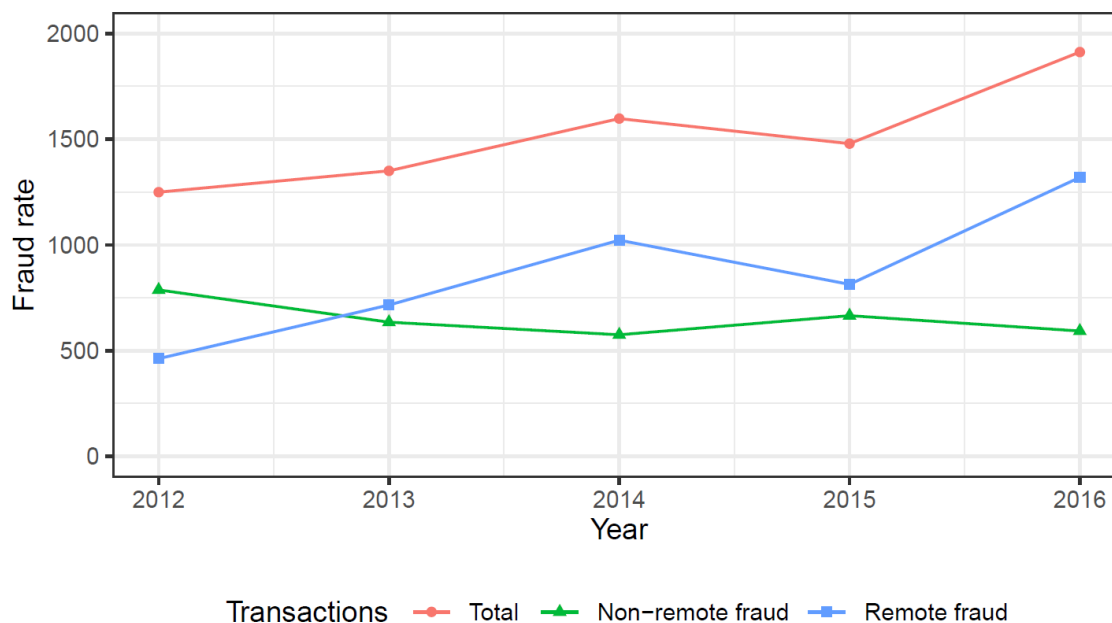


Figure 5. Remote and non-remote fraudulent transactions per 100,000 population, 2012–2016. Source: BoS

The Spanish fraudulent transaction data is analogous to data provided by the UK Finance (2018), the industry body for the UK banking and financial sector. Their most recent report shows that card fraud almost doubled, mainly due to nearly 700,000 more instances of remote card fraud (cyber fraud) per year. The other forms of card fraud detailed in their report show much less significant changes in absolute numbers.

At a European level, the European Central Bank (ECB 2018) in their Fifth Report on Card Fraud state that the value of card fraud using cards issued in the Single European Payment Area rose approximately 500 million euros between 2012 and 2016. This increase was mainly due to growth in remote fraud, as the other fraudulent transactions included in the study, point of sale fraud and ATM fraud, changed by comparatively small margins.

The data available from Spanish, the UK and European banking authorities thus suggest that the rise in identity fraud is above all the result of increases in remote bank card fraud rather than a displacement effect from face-to-face card or cheque fraud.

Further evidence for this trend is provided by data from the Mossos d'Esquadra, the Catalan police force. The Mossos d'Esquadra are the main police force in the autonomous region of Catalonia, which accounts for approximately 16% of the total Spanish population. They process their crime statistics separately from the centralized

Spanish Ministry of Interior, and freedom of information requests can be made to them directly. Unfortunately, the Spanish Ministry of Interior refused the authors access to the corresponding data for the other police forces active in Spanish territory, stating that they consider freedom of information requests for academic purposes to be “abusive”<sup>5</sup>. Figure 6 shows the frauds that were flagged as Internet frauds by the Mossos d’Esquadra in comparison to those that did not receive this tag. Non-Internet frauds have remained relatively stable during this period, while cyber fraud has increased significantly. In short, the Bank of Spain, UK Finance and European Central Bank data and the Catalan police statistics suggest that fraud offline-online displacement has been insignificant, and it is the rise of cyber fraud that is driving the current fraud boom. As Farrell and Birks (2018) state, it seems logical to imagine that if there were indeed some degree of causal relationship between increased cybercrime and a drop in traditional offences, this would be evident above all within a crime type such as fraud.

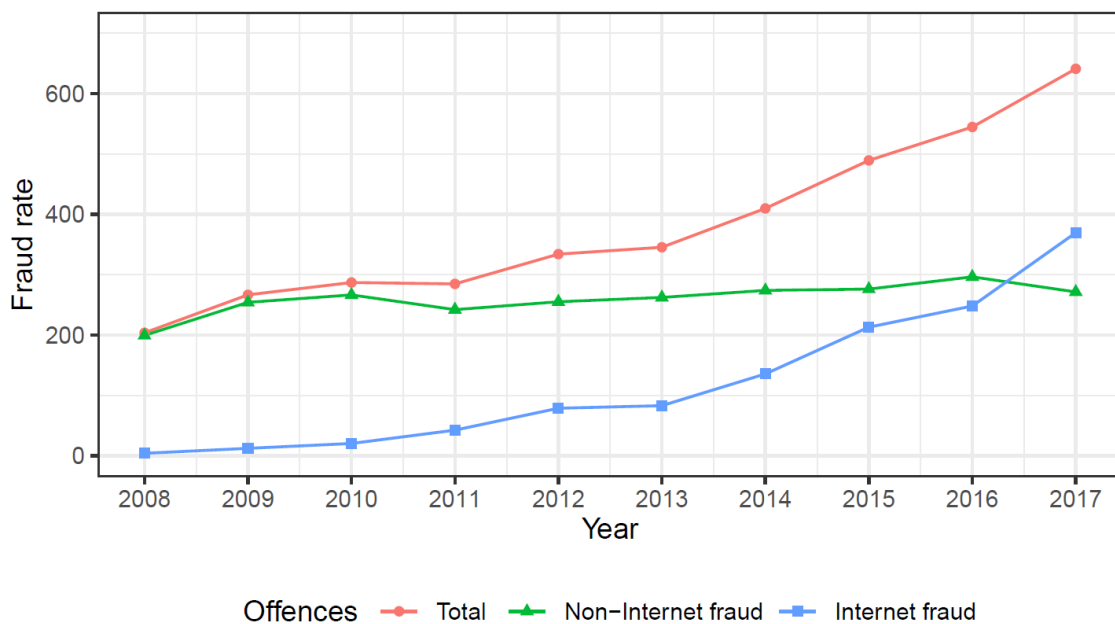


Figure 6. Police recorded fraud in Catalonia per 100,000 population, 2008–2017. Source: Catalan Ministry of the Interior

<sup>5</sup> The police in Spain is not made up of one homogenous body but rather several different forces: the National Police, Civil Guard, Local Police as well as the police forces that correspond to the autonomous communities of Catalonia, Basque Country and Navarra.

Returning to the Bank of Spain statistics, it is also relevant that in this period fraudulent transactions as a percentage of total transactions have risen only slightly (Fig. 7). This trend is similar in the UK Finance and European Central Bank data and leads to the conclusions that (a) in part, fraudulent transactions have risen in absolute terms as a consequence of the increase in the total number of transactions; (b) prevention has not improved in this 5-year period; and thus, (c) we can expect that as Internet-based transactions rise in the future, cyber fraud will continue to rise unless prevention is improved.

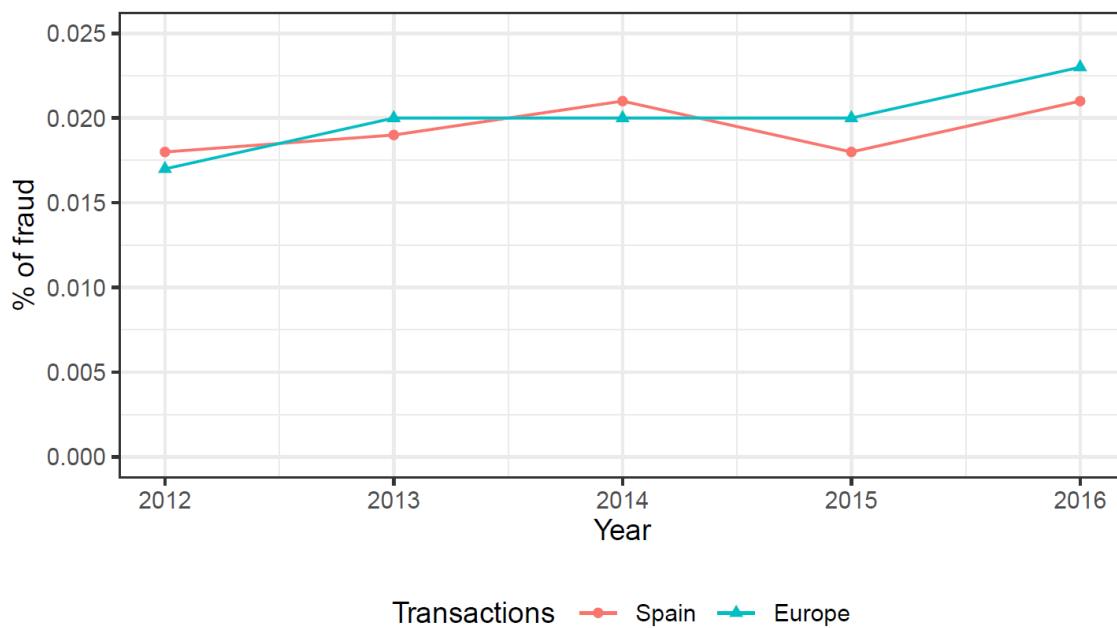


Figure 7. Percentage of fraudulent bank transactions relevant to total transactions, 2012–2016. Source: BoS

### *Property Crime Drop?*

Figure 8 shows the property crime rate when bank-recorded fraud is used to calculate the property crime rate rather than police-recorded bank fraud. The graph indicates it is difficult to affirm that there has been a property crime drop in Spain if we consider fraud statistics from both the MIR and the Bank of Spain. In fact, there may well be a rise, especially considering Spanish banks only provide data on identity fraud. In most types of fraud, such as advance fee fraud or romance fraud, the customer typically authorizes the transaction themselves, so therefore, the bank may not recognize it as fraudulent and, in addition, the offence may also not be reported to the police for the reasons enumerated previously. In such cases, these transactions will not be included in either the MIR

statistics or the data published by the Bank of Spain.

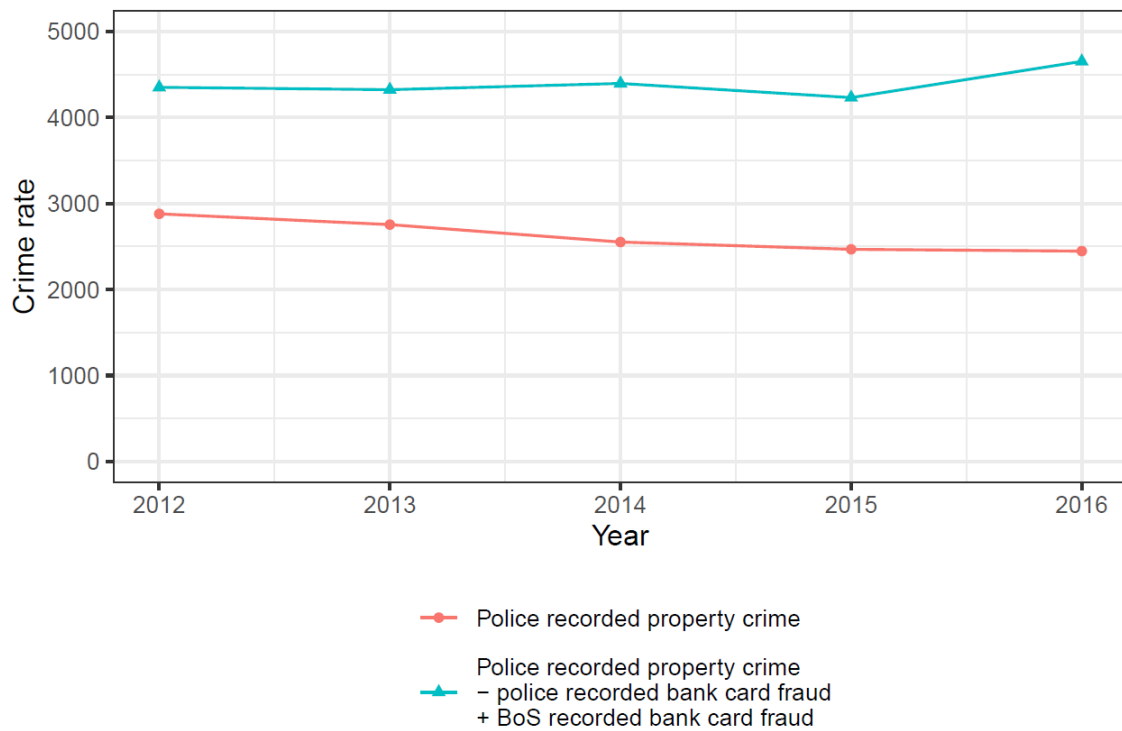


Figure 8. Police-recorded property crime per 100,000 population vs. police-recorded property crime – police recorded fraud + BoS recorded fraud per 100,000 population, 2012–2016. Data includes cyber fraud figures. Source: Spanish Ministry of Interior and BoS

It should be noted that counting is likely to be different for banks and police. For example, three fraudulent transactions involving one individual could constitute one reported fraud in police statistics. As such, adding the bank statistics to the police statistics is a very crude calculation. Nevertheless, in the Internet age, it seems unwise for the Spanish Ministry of Interior to draw conclusions on police efficiency and crime tendencies only from police statistics. This will lead to inefficient use of criminal justice resources and ineffective criminal justice policies. The limitations of the data analysed in this section mean it cannot be categorically stated that there has not been a property crime drop; however, the trends identified in the BoS data certainly call into question official sources that take this drop for granted. The Bank of Spain statistics show an increase of over 300,000 bank frauds in the period 2012–2016, which is due to an increase in remote bank card fraud. The bank card frauds registered by the police in 2016 were 35,824. This represents just 4% of the 888,000 bank card frauds detected by banks in Spain and thus

suggests extreme underreporting of bank card fraud to the police. Even if it were assumed that each bank card fraud recorded by the police corresponds to five fraudulent transactions, the reporting rate would only be 20.1%. It should also be highlighted that bank data include those fraudulent transactions detected by the bank as well as the customer.

In sum, fraud appears to be rising fast, and if we include police fraud statistics and bank card fraud data from the Bank of Spain in the crime rate analysis, it is hard to maintain that there has been a property crime drop; in fact, it appears there may have been a property crime rise in recent years in Spain. It also suggests that there has not been an increase in police efficiency as claimed by the Spanish National Police, but rather the public police's ability to record and respond to modern versions of property crime is diminished. Furthermore, it appears that the displacement effect from offline fraud to online fraud has limited explanatory power, as the increase in fraud with a strong cyber component is much greater than the decrease in traditional frauds. One possible explanation is that the characteristics of cyberspace allow many cybercrimes to be executed with little effort (Miró-Llinares 2011), unbalancing the proportion of crimes committed online and offline.

### **Victimization Surveys**

As with other crimes, victimization surveys can help shine further light on the dark figure of fraud (Mayhew and Dijk 2012) as well as the impact of fraud on the overall panorama of delinquency. The high levels of fraud underreporting combined with the fact that financial institutions may not identify many transactions that constitute criminal fraudulent activity mean these surveys can be especially useful for fraud analysis.

Reliable victimization surveys are scarce in Spain. To the authors' best knowledge, the only victimization survey which produces statistically representative results and includes data on fraud is the Catalan Public Security Survey. This is conducted in the Spanish autonomous province of Catalonia which, as previously mentioned, accounts for approximately 16% (7.5 million) of the total Spanish population. In its 2017 version, the survey asked whether, in the previous 12 months, respondents had been victim of a scam, fraud or deception that they considered to be criminal. In response, 7.7% of respondents affirmed that they had suffered fraud victimization, of which 20%



reported it to the police. Therefore, 1.5% of respondents stated they have been victim of a fraud and that they had reported it to the police.

Large-scale victimization surveys are carried out annually in a number of countries in the European Union, namely, France, the Netherlands, England and Wales, Denmark, Sweden and Finland. Direct comparisons between countries are hazardous (Van Dijk 2015), but these surveys can help determine whether the Catalan results are in line with other European countries. Furthermore, by analysing the results of victimization studies from various Western European countries, fraud prevalence and trends can be roughly estimated for Spain.

The methodology employed to choose the surveys was based on five factors. This methodology was chosen as it aligns with previous property crime victimization research (Levi 2017; Reep-van den Bergh and Junger 2018):

1. The survey includes a question on fraud, either in general or one particular type that refers to the previous 12-month period.
2. The survey publishes their methodology or made their methodology available to the authors on request.
3. The survey uses a random sample that is statistically representative of the population.
4. The survey is carried out annually or biannually, and the questions have remained significantly unchanged since 2010.
5. The survey has been carried out in a country belonging to the European Union.

Unfortunately, to the authors' knowledge, there are no surveys on organizations that meet the criteria; therefore, the results are only relevant for individual victims. The surveys that were finally selected for inclusion in the analysis were (1) England and Wales, Crime Survey for England and Wales; (2) Sweden, "National Security Survey"; (3) France, "Living environment and safety" survey report; (4) the Netherlands, "Security Monitor"; (5) Denmark, "Internet Criminality" and (6) Finland, "National Crime Research".

Figures 9 and 10 show the evolution of fraud results included in these surveys from 2010 to 2017. With the exception of the survey from England and Wales, for which only 2 years are available, all surveys indicate an upward trend in fraud victimization. It is worth noting that in the first 9 months of 2018, fraud victimization rose in England and Wales to slightly above the 2016 mark.

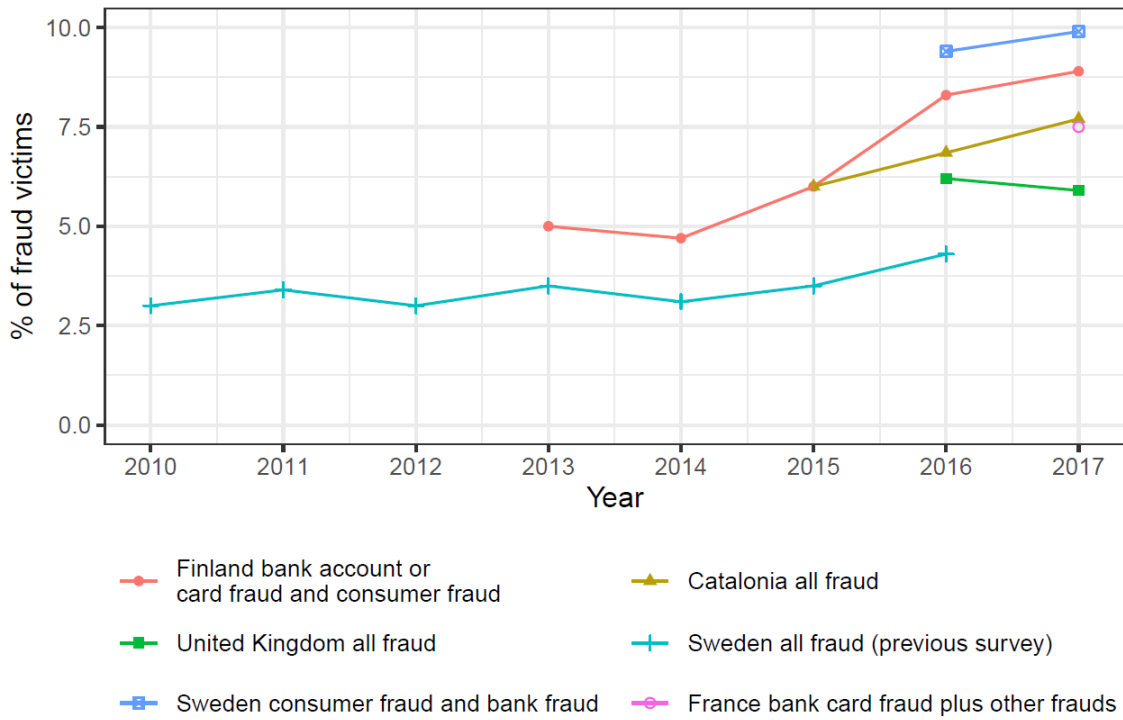


Figure 9. General fraud victimization rates in European victimization surveys, 2010–2017. Source: Catalan Public Security Survey; Crime Survey for England and Wales; Sweden, “National Security Survey”; France, “Living environment and safety” survey; Finland, “National Crime Research”

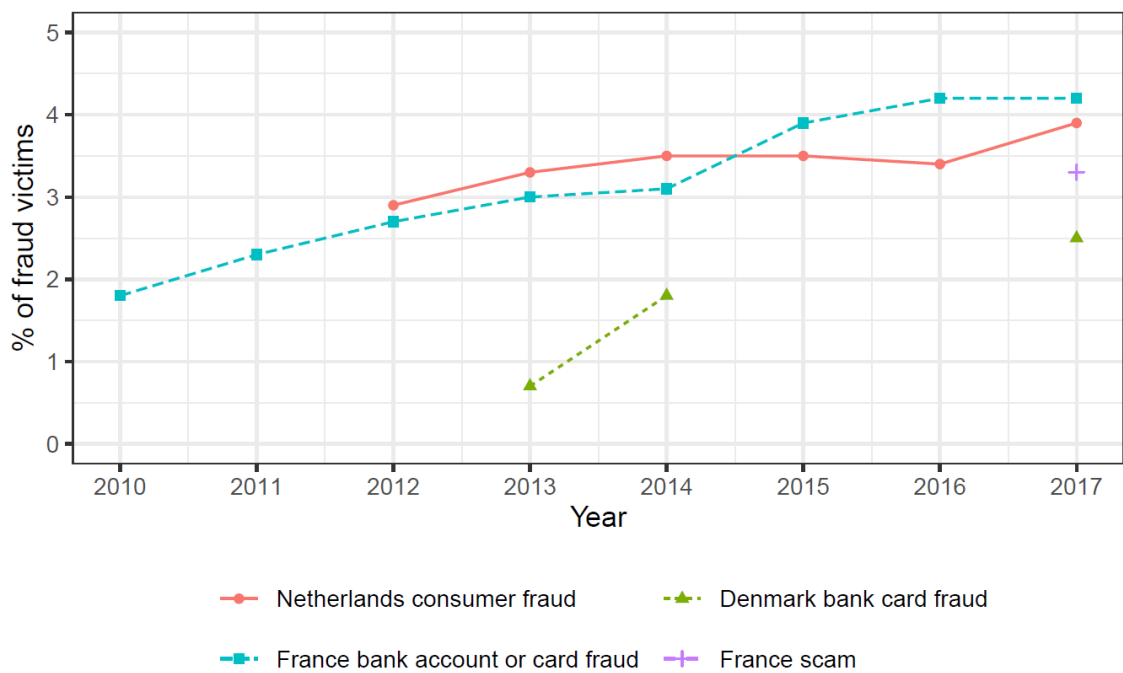


Figure 10. Specific fraud victimization rates in European victimization surveys, 2010–2017. Source: the Netherlands, “Security Monitor”; Denmark, “Internet Criminality”; France, “Living environment and safety” survey

It should be highlighted that significant differences exist in the questions used and also, therefore, disparities in the results. For the most recent year, data is available; the percentage of the population who have been victims of fraud is 7.7% in Catalonia, 5.9% in England and Wales, 8.9% in Finland, 7.5% in France and 9.9% in Sweden. In 2016, Sweden commenced an extended version of their original survey. The total fraud results for this study were considerably higher than the original, which the authors suggest it is due to the inclusion of questions on specific fraud types. The current survey found consumer fraud to be 4.8% and bank account or card fraud to be 5.1%, giving a total fraud victimization rate of 9.9%. As of 2017, the extended version is the only survey format employed.

On the other hand, the surveys conducted in the Netherlands, France and Germany enquired about victimization for particular fraud types, namely, consumer fraud and bank account or card fraud. In 2017, 3.9% of the Dutch population and 4.7% of the German population stated that they had been victims of online consumer fraud. In France, results indicate that the victimization rate for bank account or card fraud was 4.2% for 2017. However, in 2017, a new question was introduced to the French survey regarding scam victimization, which they define as all frauds and scams that are not fraudulent debits from a bank account or card. The response rate for scams was 3.3%, which means that overall, 7.5% of the French population were fraud victims that year.

As a result of the Europe-wide comparison, including one large Spanish region, a conservative, and rather crude, estimate of current individual fraud victimization rates in Spain would be between 3 and 5% of the adult population. The use of a conservative estimate is justified by the Eurobarometer <sup>6</sup> on Internet security and the European Central Bank data on fraudulent transactions, which indicate that fraud prevalence in Spain may be slightly below the European average. Moreover, this allows a margin for self-selection bias and inaccurate responses as a result of incorrect timings or overestimation of the criminality of the acts.

Although it is difficult to affirm this range of 3 to 5% with great confidence, the estimation can give us an indication of the dark figure of fraud. If, for example, we take the conservative 3% victimization rate for the adult population (lower than all other

---

<sup>6</sup> Special Eurobarometer 480.

European countries analysed even for only one specific fraud type), this would give almost 1.2 million instances of fraud victimization in Spain <sup>7</sup> for a 12-month period, compared with 214,000 registered by the police in 2017. At the top end of the estimated range, a 5% victimization rate converts to almost 2 million fraud victims, roughly equal to the total of all offences that are included in the Spanish national crime rate calculation.

At this point, it is worth reiterating that the victimization surveys do not include reports from organizations, whereas the police statistics should. In other words, the estimate of between 1.1 million and 2 million does not include frauds against organizations, which would undoubtedly increase the figures further.

In short, it appears fraud in Europe is rising, and in Spain, its prevalence is rather higher than that recorded by the official statistics, and, as a consequence, it is vital that criminal justice and policing policy decision makers are fully aware of this issue when designing and implementing crime prevention strategies.

The Swedish surveys also provide some insight into the nature of fraud growth. Firstly, in Sweden while the volume of reported fraud carried out via the Internet increased 100% between 2010 and 2015 (the 2016 surveys do not include this question), fraud that was not identified with this characteristic dropped only 10%. This indicates that rather than a clear displacement from offline to online, there is merely growth in cyber fraud.

### **Reporting Rates**

Some victimization surveys also include questions on fraud reporting rates which may assist in further illuminating the dark figure of fraud. As can be seen in Table 3, although the rate varies between countries, it can be concluded that in general, fraud reporting rates are very low, with approximately only 20 to 25% of frauds against individuals being reported to the police. In the most recent Catalan survey, fraud is the least reported economic offence with only 21% making a formal report in comparison to 38.4% for the other property crimes included in the survey. This provides further salient evidence that the official crime statistics are insufficient with regard to estimating the threat that fraud presents to society in the Internet era.

---

<sup>7</sup> Based on the Spanish adult population of 39 million on 1 January 2017.

Table 3. Fraud reporting rates by region

Region	Source	Crime	Year	Fraud reporting rate (%)	Average reporting rate for other property crimes (%)
Catalonia	Catalan Public Security Survey	Fraud	2017	21.0	38.4 <sup>a</sup>
England & Wales	Crime Survey for England & Wales	Fraud	2017	19.0	58.0 <sup>b</sup>
France	French National Victimization Survey	Bank fraud	2017	26.0	49.6 <sup>c</sup>
Netherlands	Weijer, Leukfeldt and Bernasco (2018)	Online consumer fraud	2018	24.0	55.5 <sup>d</sup>
Luxembourg	Luxembourg National Security Survey	Consumer fraud	2009-2013	22.4	54.9 <sup>e</sup>

<sup>a</sup> Vehicle related theft, burglary, robbery and other thefts.

<sup>b</sup> Theft from the person, other theft of personal property, burglary, other household theft, vehicle-related theft, bicycle theft.

<sup>c</sup> Burglary, thefts related to vehicles, bicycle theft, robbery.

<sup>d</sup> Burglary, theft from car, bicycle theft, robbery and pickpocketing

<sup>e</sup> Burglary, theft from a car, robbery, theft of personal property, bicycle theft.

Fraud reporting rates are considerably lower than other types of property crime in all the surveys providing this information. Table 3 also details crime reporting rates for other property crimes. Depending on the survey, these are a combination of vehicle theft, theft from a car, theft of a bicycle, burglary, attempted burglary, robbery and theft of personal property. For instance, in the case of England and Wales, the other property crimes were reported at a rate three times higher than fraud, 59% to 19%. Or, in the Netherlands, 55.5% reported traditional property crimes in comparison to 24% for consumer fraud.

Some surveys provide information on victims' motivations for reporting or not reporting to the police. Table 4 shows that the main reasons for reporting are related to the moral duty to report, punishing offenders, preventing reoffending and recovering losses. On the other hand, Table 5 shows that victims decided not to report primarily due to the insignificance of the event, the complexity of the reporting process and a lack of confidence in police ability to respond adequately. In this sense, we can see that both private costs and intrinsic and extrinsic benefits (Bowles et al. 2009) are taken into account when individuals decide whether to report.

Table 4. Reasons for reporting fraud to police

Region	Source	Crime	Year	Most common reason for reporting	2 <sup>nd</sup> most common	3 <sup>rd</sup> most common
France	French National Victimization Survey	All fraud except bank fraud	2017	Identify and punish offenders	Obtain reimbursement from offenders	Stop offenders reoffending
Germany	German Victimization Survey (2019)	Online consumer fraud	2017	Crime should be reported	So offenders are punished	So it does not happen again

Table 5. Reasons for not reporting fraud to police

Region	Source	Crime	Year	Most common reason	2 <sup>nd</sup> most common reason	3 <sup>rd</sup> most common reason
Catalonia	Catalan Public Security Survey	Fraud	2017	Too complicated, could not be bothered, too much bureaucracy and time	Not significant	The police cannot do anything
Germany	German Victimization Survey	Online consumer fraud	2013-2017	The incident was not serious enough	Police could not or would not have done anything	Victim or family solved the matter
Luxembourg	Luxembourg National Security Survey	Consumer fraud	2009-2013	Did not see the need, felt it would have been useless	Not serious Enough	Not enough evidence to involve the police

## Discussion

The evidence presented in this paper points to fraud being one of, if not, the most prevalent property crimes in the cybercrime era. Combining secondary data sources, which has been identified as an effective strategy for analysing crime patterns (Tilly et al. 2018), allowed fraud trends to be identified thereby making an important contribution to crime trend research. A more accurate depiction of this crime reality is necessary for

many reasons (Smith 2006). Firstly, criminologists and other academics require evidence to inform debate, research and policy. A necessary first step in much crime research is understanding the extent of the problem. Secondly, governments make claims about their ability to protect citizens from crime, yet the evidence provided suggests citizens are currently underprotected with regard to fraud. Crime data enables governments and other criminal justice institutions to be held accountable for crime control policy since evaluations of crime trends permit evaluations of prevention strategies. Similarly, identifying the prevalence of criminal activity enables criminal justice institutions and other public institutions involved in crime control to better allocate resources both in the short-term and with regard to long-term strategies and policy. Finally, highlighting increases in cyber fraud can encourage the organizations involved in ICT design and supply to produce and use products that do not expose users to unnecessary risks by creating crime opportunities. To foster safety by design, evidence must be provided that shows products and systems are failing the user. If, as this paper suggests, somewhere between 3 and 5% of the Spanish adult population are currently falling victim to fraud every 12 months, the failure is lucid. Even more so when taking into account that fraud can have significant negative consequences on victims, both financially and in terms of physical and mental well-being (Cross 2018).

The low levels of fraud reporting to the police combined with even lower rates of investigation and prosecution (Spanish Public Prosecutor 2018) reiterate the changing role of the police and the criminal justice system regarding crime control in the Internet era. The police have generally taken it for granted that they are the main actor in prevention, but this is not necessarily the case in the modern era (Wall 2007/10). In fact, the role of police is reduced with regard to detecting, preventing and investigating cyber fraud. Various studies have highlighted the insufficient training of police officers to deal with cybercrimes (Leukfeldt et al. 2013; Webster and Drew 2017), meaning investigations are often not even considered. The limitations regarding resources and a traditional organizational culture that is not conducive to change are combined with jurisdictional issues to put much technology-related crime out of the grasp of the public police. In this sense, and as many authors have previously noted (for example: Dupont 2017; Levi and Williams 2013; Wall 2007/10), policing crimes that involve the Internet requires a multi-agency response that goes beyond traditional reactive investigations. Security networks which involve cooperation and partnerships between the police, other government institutions, the private sector as well as end users should be created or

enhanced. Responsibilizing the private sector may be particularly effective as increased criminal opportunities can be a negative externality of private sector activity (Tilly 2018). This is not to say that traditional law enforcement bodies have no role in cybercrime prevention but, rather, to emphasize that they must form part of multistakeholder and transnational approaches that bring together different capabilities and resources.

## **Conclusions**

The evidence presented in this paper indicates fraud is rising both in Spain and Europe. Property crime trends are undergoing significant changes, as traditional offences are decreasing, while fraud, which can be enhanced and assisted by information and communication technology, displays an upward trend. As shown by comparing official fraud statistics, financial sector statistics and victimization surveys from Spain and throughout the European Union, fraud appears to be one of the most prevalent offences in the Internet era. As a result, it requires a suitable response from the institutions charged with crime control policy.

Contrary to expectations, there is evidence to suggest that fraud displacement from traditional to cyber is not sufficient to explain the increase in Internet-based fraud. Traditional fraud has only decreased slightly, while fraud involving a cyber element has demonstrated a strong upward trend. This trend is likely to continue as more transactions and banking are carried out online. It may be the result of new criminal actors or that the crime opportunities provided by cyber space have prompted changes in the modus operandi of existing fraud perpetrators.

By comparing official Spanish police statistics with Bank of Spain fraud statistics and self-reported victimization, it appears there is considerable underreporting with regard to fraud. While there is no survey data for all Spain, the results from Catalonia compared with the results from Europe and a large margin of error indicate the dark figure of fraud requires further research. This represents a basic yet extremely salient challenge to those involved in prevention and policing: the unknown cannot be prevented or policed.

The underreporting of fraud found in this investigation indicates that the overall crime rate in Spain may be considerably higher than the current MIR figure. If, as the evidence suggests, there are well over 1 million fraud victims in Spain every year, property crime could potentially be 100% higher than the official figure. On the other hand, the inclusion of fraud in the overall crime total may increase this by over 50%, since



the MIR calculation gives a total of approximately 2 million criminal acts in Spain. Furthermore, contrary to the official Spanish government position and much academic literature, a property crime rise may even have taken place in Spain in recent years.

The data employed in this study has its limitations, such as possible definitional differences, reporting biases and limited data points. In response to these limitations, firstly, to minimize definitional differences, a broad fraud definition has been employed. Secondly, the increasing fraud trend may be partially explained by increasing awareness of the problem and therefore increased reporting, but the data suggests that it is only cyber fraud that is rising, and fraud reporting remains particularly low according to the victimization surveys. Finally, with regard to trends, the measurement of fraud by central banking institutions and victimization surveys is recent, and therefore, the time period is short. However, this means the data provides new perspectives on property crime, and, moreover, this is one of the first attempts to include Spain, the fifth largest country in the EU, in European crime trend analysis. This initial insight into fraud trends may provide a blueprint for future research.

The aim of the study was not to categorically deny the existence of a property crime drop in Spain but rather to suggest that it is unclear in the digital age, to highlight differences in crime types and to show fraud can add to the analysis. This is especially salient for public police forces that should be aware of their limitations in the Internet era and avoid simplistic conclusions when evaluating their performance and deciding where to focus resources.

### **Acknowledgements**

This work was supported by the Spanish Ministry of Science, Innovation and Universities under Grant FPU16/01671.

This is a post-peer-review, pre-copyedit version of an article published in European Journal on Criminal Policy and Research. The final authenticated version is available online at: <https://doi.org/10.1007/s10610-020-09439-2>.

### **References**

Aebi, M. F., & Linde, A. (2010a). Is there a crime drop in Western Europe? *European Journal of Criminal Policy and Research*, 16(4), 251–277. <https://doi.org/10.1007/s10610-010-9130-y>.

- Aebi, M. F., & Linde, A. (2010b). El misterioso caso de la desaparición de las estadísticas policiales españolas. *Revista Electrónica de Ciencia Penal y Criminología*, 12(7), 1–30.
- Aebi, M. F., & Linde, A. (2012). Crime trends in Western Europe according to official statistics from 1990 to 2007. In J. van Dijk, J. A. Tseloni, & G. Farrell (Eds.), *The International Crime Drop: New Directions in Research*. London: Palgrave MacMillan.
- Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265–300). Berlin: Springer.
- Baumer, E. P., Velez, M. B., & Rosenfeld, R. (2018). Bringing crime trends back into criminology: a critical assessment of the literature and a blueprint for future inquiry. *Annual Review of Criminology*, 1, 6.1–6.23.
- Beals, M., DeLiema, M. & Deevy, M. (2015). Framework for a taxonomy of Fraud. Stanford: Stanford Centre for Longevity. Available at: <File:///E:/doctorate/fraud%20extension%20and%20demographics/full-taxonomy-report.Pdf>.
- Blumstein, A., & Wallman, J. (2006). *The crime drop in America*. Revised edn. Cambridge [etc.]: Cambridge University press.
- Bowles, R., Garcia Reyes, M., & Garoupa, N. (2009). Crime reporting decisions and the costs of crime. *European Journal on Criminal Policy and Research*, 15(4), 365. <https://doi.org/10.1007/s10610-009-9109-8>.
- Button, C., & Cross, C. (2017). *Cyber frauds, scams and their victims*. Abingdon: Routledge.
- Caneppele, S., & Aebi, M. F. (2017). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. *Policing: A Journal of Policy and Practice*, pax055. <https://doi.org/10.1093/policing/pax055>.
- Clough, J. (2015). *Principles of cybercrime*. Cambridge: Cambridge University Press.
- Cross, C. (2018). Victims' motivations for reporting to the 'fraud justice network'. *Police Practice and Research*, 19(6), 550–564. <https://doi.org/10.1080/15614263.2018.1507891>.

- Dijk, J. V. (2015). The case for survey-based comparative measures of crime. *European Journal of Criminology*, 12(4), 437–456. <https://doi.org/10.1177/1477370815585446>.
- Dupont, B. (2017). Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime Law and Social Change*, 67(1), 97–116. <https://doi.org/10.1007/s10611-016-9649-z>.
- European Central Bank. (2018). Fifth Report on Card Fraud.
- Europol. (2018). Internet Organised Crime Threat Assessment (Iocta).
- Fafinski, S., Dutton, W. H., & Margetts, H. (2010). Mapping and measuring cybercrime. Oxford internet institute forum discussion paper no 18.
- Farrell, G., & Birks, D. (2018). Did cybercrime cause the crime drop? *Crime Science*, 7, 1.
- Fernández-Molina, E., & Gutiérrez, R. B. (2018). Juvenile crime drop: what is happening with youth in Spain and why? *European Journal of Criminology*. <https://doi.org/10.1177/1477370818792383>.
- Gadd, D., Karstedt, S., & Messner, S. (2012). Editorial introduction. In D. Gadd, S. Karstedt, & S. F. Messner (Eds.), *The SAGE handbook of criminological research methods* (pp. 1–8). London: SAGE Publications Ltd. <https://doi.org/10.4135/9781446268285>.
- Gruszczyńska, B., & Heiskanen, M. (2018). Trends in police-recorded offenses at the beginning of the twentyfirst century in Europe. *European Journal on Criminal Policy and Research*, 24(1), 37–53. <https://doi.org/10.1007/s10610-018-9370-9>.
- Holt, T. J., & Bossler, A. M. (2015). *Cybercrime in Progress theory and prevention of technology-enabled offenses*. Oxford: Taylor & Francis.
- Jansen, J., Junger, M., Kort, J., Leukfeldt, R., Veenstra, S., van Wilsem, J. & van der Zee, S. (2017). Victims. In Leukfeldt, R. (Ed.). *Research agenda the human factor in cybercrime and cybersecurity*. The Hague: Eleven International Publishing.
- Johnstone, P. (1998). Serious white collar fraud: historical and contemporary perspectives. *Crime, Law and Social Change*, 30(2), 107–130. <https://doi.org/10.1023/A:1008349831811>.
- Killias, M., & Aebi, M. F. (2000). Crime trends in Europe from 1990 to 1996: how Europe illustrates the limits of the American experience. *European Journal on Criminal Policy and Research*, 8(43), 43–63. <https://doi.org/10.1023/A:1008745112022>.

- Leukfeldt, R., Veenstra, S., & Stol, W. (2013). High volume cybercrime and the organization of the police: the results of two empirical studies in the Netherlands. *International Journal of Cyber Criminology*, 7(1).
- Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal of Criminal Policy and Research*, 23(3), 287–300. <https://doi.org/10.1007/s10610-016-9332-z>.
- Levi, M. (2012). Assessing the cost of fraud. In D. Gadd, S. Karstedt, & S. F. Messner (Eds.), *The SAGE handbook of criminological research methods* (pp. 461–474). London: SAGE Publications Ltd. <https://doi.org/10.4135/9781446268285>.
- Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: overview and issues. *Crime, Law and Social Change*, 67(1), 3–20. <https://doi.org/10.1007/s10611-016-9645-3>.
- Levi, M., & Burrows, J. (2008). Measuring the impact of fraud in the UK: a conceptual and empirical journey. *The British Journal of Criminology*, 48(3), 293–318. <https://doi.org/10.1093/bjc/azn001>.
- Levi, M., & Williams, M. L. (2013). Multi-agency partnerships in cybercrime reduction: mapping the UK information assurance network cooperation space. *Information Management & Computer Security*, 21(5), 420–443. <https://doi.org/10.1108/IMCS04-2013-0027>.
- Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. (2017). Cyber fraud and the implications for effective risk-based responses: themes from UK research. *Crime Law & Social Change*, 67(1), 77–96. <https://doi.org/10.1007/s10611-016-9648-0>.
- Levitt, S. D., & Dubner, S. J. (2005). *Freakonomics: a rogue economist explores the hidden side of everything*. New York: William Morrow.
- Maguire, M. (2012). Criminal statistics and the construction of crime. In M. Maguire, R. Morgan, & R. Reiner (Eds.), *Oxford handbook of criminology* (5th ed., pp. 206–244). Oxford: Oxford University Press.
- Maras, M. H. (2017). *Cybercriminology*. New York: Oxford University Press.
- Mayhew, P., & Dijk, J. (2012). Assessing crime through international victimization surveys. In D. Gadd, S. Karstedt, & S. F. Messner (Eds.), *The SAGE handbook of criminological research methods* (pp. 253–267). London: SAGE Publications Ltd. <https://doi.org/10.4135/9781446268285>.

- Mcguire, M., & Dowling, S. (2013). Cyber crime: a review of the evidence. In Summary of key findings and implications (Vol. 75). London: Home Office. Home Office Research Report.
- Miró-Llinares, F. (2011). La oportunidad criminal en el ciberespacio: Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *Revista Electrónica de Ciencia Penal y Criminología*, 13(7), 1–55.
- Miró-Llinares, F. (2012). El cibercrimen Fenomenología y criminología de la delincuencia en el ciberespacio. Madrid: Marcial Pons.
- Miró-Llinares, F. (2013). La Respuesta Penal al Ciberfraude: especial atención a la responsabilidad de los muleros del phishing. *Revista Electrónica de Ciencia Penal y Criminología*, 15(12), 1–56.
- Miró-Llinares, F., & Moneva, A. (2019). What about cyberspace (and cybercrime alongside it)? A reply to Farrell and Birks “did cybercrime cause the crime drop?”. *Crime Science*, 8(1), 12. <https://doi.org/10.1186/s40163-019-0107-y>.
- National Academies of Sciences, Engineering, and Medicine. (2016). Modernizing crime statistics—report 1: defining and classifying crime. Washington, DC: The National Academies Press. <https://doi.org/10.17226/23492>.
- Reep-van den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. *Crime Science*, 7(5). <https://doi.org/10.1186/s40163-018-0079-3>.
- Rosenfeld, R. (2018). Studying crime trends: normal science and exogenous shocks. *Criminology*, 56, 5–26. <https://doi.org/10.1111/1745-9125.12170>.
- Savona, E. U., & Mignone, M. (2004). The fox and the hunters: how IC technologies change the crime race. *European Journal on Criminal Policy and Research*, 10(3), 3–26. <https://doi.org/10.1023/B:CRIM.0000037562.42520.d7>.
- Smith, A. (2006). Crime statistics: An independent review (carried out for the secretary of state for the home department). London, UK. Retrieved from <https://webarchive.nationalarchives.gov.uk/20110220155813/http://rds.homeoffice.gov.uk/rds/pdfs06/crime-statistics-independent-review-06.pdf>.
- Smith, R. G. (2010). Identity theft and fraud. In Jewkes & Yar (Eds.), *Handbook of internet crime* (pp. 273–301). London: Routledge.
- Spanish Public Prosecutor. Fiscal General del Estado. (2018). Memoria Anual. Ministerio de Justicia.

- Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). The dark figure of online property crime: is cyberspace hiding a crime wave? *Justice Quarterly*, 33(5), 890–911.
- Tilly, N. (2018) Privatizing Crime Control. *The ANNALS of the American Academy of Political and Social Science*, 697(1). <https://doi.org/10.1177/0002716218775045>.
- Tilly, N., Farrell, G., & Tseloni, M. (2018). Doing quantitative data analysis in criminological research. In P. Davies & P. Francis (Eds.), *Doing criminological research* (3rd ed., pp. 229–250). London: Sage.
- Tonry, M. (2014). Why crime rates are falling throughout the Western world. *Crime & Justice*, 43(1).
- Tseloni, A., Mailley, J., Farrell, G., & Tilley, N. (2010). Exploring the international decline in crime rates. *European Journal of Criminology*, 7(5), 375–394. <https://doi.org/10.1177/1477370810367014>.
- Tunley, M. (2014). *Mandating the measurement of fraud: legislating against loss*. Basingstoke: Palgrave Macmillan.
- UK Finance. (2018). *Fraud the Facts 2018*. Retrieved from <https://www.ukfinance.org.uk/wpcontent/uploads/2018/07/Fraud-the-facts-Digital-version-August-2018.pdf>
- United Nations Office on Drugs and Crime. (2015). *International classification of crime for statistical purposes*. Vienna.
- van de Weijer, S. G. A., Leukfeldt, R., & Bernasco, W. (2018). Determinants of reporting cybercrime: a comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology*. <https://doi.org/10.1177/147737081877361>.
- van Dijk, J., Tseloni, A., & Farrell, G. (2012). *The international crime drop: new directions in research*. New York: Palgrave Macmillan.
- Wall, D. S. (2007/10). Policing cybercrimes: situating the public police in networks of security within cyberspace (revised may 2010). *Police Practice & Research: An International Journal*, 8(2), 183–205.
- Webster, J., & Drew, J. M. (2017). Policing advance fee fraud (AFF): experiences of fraud detectives using a victim-focused approach. *International Journal of Police Science & Management*, 19(1), 39–53.
- Whitty, M. T. (2013). The scammers persuasive techniques model: development of a stage model to explain the online dating romance scam. *The British Journal of Criminology*, 53(4), 665–684. <https://doi.org/10.1093/bjc/azt009>.

- Wickham, H., Averick, M., Bryan, J., Chang, W., McGowan, L., François, R., Grolemund, G., Hayes, A., Henry, L., Hester, J., Kuhn, M., Pedersen, T., Miller, E., Bache, S., Müller, K., Ooms, J., Robinson, D., Seidel, D., Spinu, V., et al. (2019). Welcome to the Tidyverse. *Journal of Open Source Software*, 4(43), 1686. <https://doi.org/10.21105/joss.01686>.
- Williams, M. L. (2016). Guardians upon high: an application of routine activities theory to online identity theft in Europe at the country and individual level. *The British Journal of Criminology*, 56(1), 21–48. <https://doi.org/10.1093/bjc/azv011>.
- Wright, R., & Jaques, S. (2017). *Property Crime: Oxford Bibliographies Online Research Guide*. Oxford: Oxford University Press.
- Zimring, F. E. (2006). *The Great American Crime Decline*. New York, NY: Oxford University Press.