Empty streets, busy Internet. A time series analysis of cybercrime and fraud
trends during COVID-19

Steven Kemp¹, David Buil-Gil², Asier Moneva³, Fernando Miró-Llinares⁴ and Nacho
Díaz-Castaño⁴

¹Department of Public Law, University of Girona, Spain, and Crímina Research Center for the Study and
Prevention of Crime, Miguel Hernández University of Elche, Spain
²Department of Criminology, University of Manchester, UK
³Netherlands Institute for the Study of Crime and Law Enforcement, Netherlands, and The Hague
University of Applied Sciences, Netherlands
⁴Crímina Research Center for the Study and Prevention of Crime, Miguel Hernández University of Elche,
Spain

Abstract: There have been many warnings about the rising threat of cybercrime and fraud
resulting from the COVID-19 lockdown measures and the associated increase in Internet
use. However, there is still relatively little data with which to support the alerts and any
changes may be nuanced. The present paper applies time series analysis methods to
historical data on cybercrime and fraud reported to Action Fraud in the UK to examine
whether any potential increases are beyond normal crime variability. Furthermore, the
discrepancies between fraud types and individual and organisation victims are also
analysed. The results show that while both total cybercrime and total fraud did increase
beyond predicted levels, the changes in victimisation were not homogenous across fraud
types and victims. The implications of these findings on how changes in routine activities
in the UK have influenced cybercrime and fraud opportunities are discussed in relation to
policy, practice and academic debate.

Keywords: crime trends; coronavirus; ARIMA; cybersecurity; victims; crime statistics

Acknowledgments: The authors would like to thank the City of London Police and UK
Action Fraud for sharing the data used in this study.
1. Introduction

Since the beginning of the COVID-19 pandemic, many sources have warned of possible increases in cybercrime and fraud. In March 2020, Europol had already alerted about new ways in which cybercriminals were benefiting from the pandemic and associated lockdown measures (Europol, 2020a), and more recently, in October 2020, Europol’s (2020b) Internet Organised Crime Threat Assessment stated that “COVID-19 caused an amplification of existing [cybercrime] problems” (p. 6) and noted an increase in fraud against businesses “as a result of the global outbreak of COVID-19” (p. 47). Similarly, Interpol’s (2020) report entitled ‘Cybercrime: Covid-19 impact’ affirms there has been “a sharp increase in cybercriminal activities” (p. 4) related to the virus. As a preventive measure against such threats, UK law enforcement agencies used Twitter to raise public awareness, devoting 57.2% of their messages to fraud schemes and 16.9% to cybercrime problems (Nikolovska et al., 2020).

Yet, despite the warnings from some of the world’s largest law enforcement organisations, there has been relatively little supporting data released by these or other sources with regard to these types of crimes. From an opportunity perspective, it seems logical to expect an increase in cybercrime and fraud when more people use the Internet (Miró-Llinares & Moneva, 2019); however, both these umbrella categories encompass a very diverse range of conducts and it is unlikely the trends are replicated for all types of cybercrime and fraud and for all types of victims (e.g. not all frauds can be considered a form of cyber-enabled crime). Furthermore, detected fluctuations may be very short term and may simply bounce back to the initial trend, or they could even be within normal crime variability. In fact, literature on traditional street crime, such as serious assaults, indicates the relationship between lockdown measures and crime is not always as expected (Ashby, 2020), while preliminary analysis on cybercrime and COVID-19 has indicated that individual and organisational victims may not be affected in the same manner (Buil-Gil et al., 2021a).

Thus, the main aim of the present paper is to provide further understanding of the relationship between the changes in daily activities brought about by the COVID-19 pandemic and cybercrime and fraud in the UK. To this end, the paper begins by describing the changes in routine activities in the UK and how these may have influenced cybercrime and fraud opportunities. Subsequently, a brief overview of the existing literature on the
relationship between crime and COVID-19 will be provided. Next, the data and the methods will be introduced. A detailed description of the results comprises the penultimate section of the paper. Finally, discussion and conclusions are provided with regard to the implications of the findings for policy, practice and academic debate.

2. COVID-19 and shifts in crime opportunities

2.1 COVID-19 and routine activities in the UK

The unprecedented rapid changes in routine activities brought about by COVID-19 and the associated lockdown measures have been evidenced around the globe. In the UK, Figure 1 visualises the changes in mobility as documented by Google (2020) in their ‘UK COVID-19 Community Mobility Reports’ based on user location data. In this regard, Figures 1a, 1b and 1d highlight the notable drop in work, recreation and retail, and transit mobility, respectively, in comparison to baseline measurements of the median value for the corresponding day of the week, during the five weeks between January 3rd and February 6th, 2020. On the other hand, Figure 1c illustrates a clear rise in mobility trends for places of residence. As can be observed in the plots, the most pronounced changes occurred around March 23rd, which was the date the UK introduced strict lockdown measures.

The Office for National Statistics (ONS) provides support for these trends. They found that in April 2020 over 40% of UK workers did some work from home as a result of the coronavirus pandemic (Office for National Statistics, 2020a). They also found that in the period between April and June, total hours worked in the UK were approximately 20% less than in the previous three years (Office for National Statistics, 2020b). These findings indicate a reduction in mobility, a rise in teleworking, and an increase in leisure time. Similarly, the ONS has highlighted a change in retail activities with many physical retail stores reporting decreased footfall but online sales showing a 46.8% increase since February (Office for National Statistics, 2020c). This ties in with data on UK and global Internet use. Ofcom (2020) found a notable increase in the time adults spend online in April 2020 in comparison to September the previous year. The London Internet exchange shows a pronounced spike in Internet traffic between March 11th and March 28th far greater than any spike in the upwards trend of recent years (see original data from https://portal.linx.net/stats/lans). Traffic decreased April to August 2020 but generally
remained above the levels found pre-coronavirus. Finally, Datavault’s Broadband Insight reports for 2020 (OpenVault, 2020) and their COVID-19 Broadband Impact Tracker (available from https://openvault.com/trusted/) detail increases in global broadband use by both individuals and businesses that are above the general rising trend found in previous periods, especially in the months of March and April 2020.

Figure 1. Changes in UK mobility Feb-July 2020. Source: produced by authors with data from Google Community Mobility Reports

2.2. COVID-19, routine activities and traditional crime

For many decades, criminologists have studied crime trends in relation to routine activities and how these can shape criminal opportunities. Cohen and Felson (1979) formulated this as the Routine Activity Approach and stated that crime occurs when likely offenders and suitable targets converge in both space and time in the absence of capable guardians. Employing time series analysis, these authors identified that changes in
household structures and activities, such as the increasing proportion of females in the workforce or the greater number of single-adult households, reduced people’s capacity to serve as capable guardians and correlated positively with homicide, forcible rape, aggravated assault, robbery and burglary. They postulated, for example, that the increase in ownership of valuable and movable goods combined with the increase in the time households were unattended during the day increased the opportunities for burglary.

Given the huge changes in routine activities in the UK detailed in the previous section, it seems likely that criminal opportunities will also have seen marked changes during 2020 (Stickle & Felson, 2020). In this sense, several authors have examined the effects of COVID-19 and related containment measures on traditional crime around the globe using a variety of statistical techniques (e.g. Felson et al., 2020; Gerell et al., 2020; Piquero et al., 2020). Many studies employing time series analysis techniques, such as Autoregressive Integrated Moving Average (ARIMA) models, have found an overall reduction in crime but notable differences in trends between crime types (e.g. Ashby, 2020; Campedelli et al., 2020; Estévez-Soto, 2020; Hodgkinson & Andresen, 2020; Mohler et al., 2020; Payne et al., 2020).

2.3 COVID-19, routine activities and cybercrime and fraud

Prior to COVID-19, academic research had already noted how changes in offline and online routine activities are associated with a shift in crime opportunities from physical space to cyberspace (Miró-Llinares & Moneva, 2019). The popularisation of the Internet has changed work and leisure activities meaning criminals may dedicate more time to online crimes, such as certain types of cyber-enabled fraud. Indeed, studies have found that overall increases in fraud are being driven by pronounced upward trends in fraud with a cyber element (Kemp et al., 2020). Given the already existing association between the expansion of the Internet and digital platforms and the growth in online criminal opportunities, it seems likely that the boost in online activity since March 2020 is correlated with a similar boost in online crime (Horgan et al., 2021; Miró-Llinares, 2021).

A nascent body of literature has begun to explore this relationship. For example, Collier et al. (2020) describe a rise in certain cybercrimes such as denial of service attacks and an increase in opportunities for fraud globally. They observe that cybercriminals have mainly adapted already existing attack strategies to exploit psychological effects of the
pandemic, for example, higher levels of fear. Similarly, Vu et al. (2020) examined underground cybercrime markets during the pandemic, finding a significant increase in the volume of products involved but no notable differences in the types of transactions, users or behaviours in the markets they studied. Payne (2020) used data from the US Federal Trade Commission to identify an overall increase in reported fraud cases in the first three months of 2020 in comparison to the same period in 2019. A significant increase in losses from fraud in the same period was also highlighted. However, the growth was not the same across all fraud types or all age groups, with the author noting marked upticks in frauds connected to the Internet, such as imposter businesses, fraudulent text messages, online shopping complaints, counterfeit checks, and romance scams. Disparities between crime victims were also found by Buil-Gil et al. (2021a) in their preliminary analysis of reported cybercrime and fraud in the UK. Despite detailing statistically significant changes between May 2019 and May 2020 in most fraud and cybercrime categories as well as for the total number of reports, they highlighted differences in trends between organisation (a slight non-significant decrease in cyber-dependent crime and a slight increase in online fraud) and individual victims (an overall significant increase). This may be related to distinct variations in routine activities or reporting practices between these types of victims. Finally, Hawdon et al. (2020) employed online panel surveys to measure cybercrime victimisation during the pandemic. Surprisingly, they found little change between the pre- and post-COVID sample; however, the overlapping question periods between the two samples mean these results should be interpreted with caution.

3. The Present Research

Despite the incipient research primarily identifying an increase in cybercrime and fraud during the pandemic, there is still a salient lack of time series analysis as found in the literature on COVID-19 and more traditional crime types. The present study aims to fill this gap by applying ARIMA models, which are explained in greater detail in section 3.2, to analyse trends in cybercrime and fraud known to the police in the UK. In the review of the literature set out in Section 2, it was identified that many crimes have been significantly affected by the mobility restrictions associated with COVID-19 and it was noted that cybercrime and fraud are generally believed to have increased. However, pre-COVID literature on fraud has shown that offline variants of fraud appear to be declining in recent years while cyber-enabled fraud types are rising (Kemp et al., 2020; Miró-
Llinares & Moneva, 2019). ‘Cyber-enabled’ refers to fraud types that existed previously but that are now mainly committed via the Internet as this allows them to increase “their scale and reach” (McGuire & Dowling, 2013, p. 4), for example, online shopping fraud. In addition, law enforcement agencies (Interpol, 2020) and academic studies (Buil-Gil et al., 2021a) have highlighted that the changes in routine activities during the pandemic have not had identical effects on cybercrime and fraud victimisation of individuals and organisations. Based on these conclusions from prior research, the following hypotheses have been formulated for the present study:

H₁ Changes in cybercrime and fraud during COVID-19 are greater than expected crime variability.

H₂ Traditional offline fraud has decreased during COVID-19 while cyber-enabled fraud has increased.

H₃ Relative increases in victimisation by cybercrime and cyber-enabled fraud during COVID-19 have been greater for individuals than for organisations.

3.1 Data

3.1.1 Crime Data

The data on cybercrime and fraud used in the present study were obtained via a freedom of information request to the City of London Police who, alongside the National Fraud Intelligence Bureau, run Action Fraud, the UK’s national reporting centre for fraud and cybercrime. Data were requested for Action Fraud data on individual and organisational victims for each month from April 2017 to July 2020. This period was chosen because records disaggregated by victim type and month only became available from April 2017. Due to resource limitations and the provisions of the Freedom of Information Act, the City of London Police were unable to provide data for reports for all crime types recorded by Action Fraud, thus, the following 6 types were requested:

- Total cybercrime. In accordance with the Home Office Counting Rules (Home Office, 2020), this category is comprised of Computer virus/malware/spyware; Denial of Service attacks (with or without extortion); Hacking of personal computer; Hacking of social media and email; Hacking of PBX/Dial Through; and Hacking combined with extortion.
- Total fraud. This includes all 46 of the fraud types in accordance with the aforementioned Home Office classification.

- Online shopping and auction fraud. The Home Office defines this category as “fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site”. This fraud was chosen as one of the individual fraud types for two main reasons. On the one hand, the Internet plays an essential role in the commission of this type of fraud, as illustrated by its name. On the other hand, it was considered that online shopping and auction fraud was a crime type that would affect both individuals and business, thereby permitting comparisons.

- Dating fraud. In this type of fraud “the intended victim is befriended on the Internet and eventually convinced to assist their new love financially by sending them money for a variety of emotive reasons”. This was also requested because the Internet plays an essential role in its commission, especially when the typical physical places for meeting a potential partner, such as pubs or nightclubs, are closed or restricted during lockdown.

- Ticket fraud. This category “involves the victim purchasing tickets remotely e.g. over the phone or internet”. Data on this fraud were solicited because although often cyber-enabled, the opportunity to commit ticket fraud is created by the desire to carry out activities in the physical world. This crucial link to the physical world allows analysis of the connection between activities in physical space and crime in cyberspace.

- Door-to-door sales and bogus tradesmen fraud. This is one of the only crimes in the Action Fraud data that they consider not cyber-enabled and that is committed in relatively large numbers (more than 1,000 cases per year).

Data on crime reports submitted to Action Fraud which contain a valid postcode address in England, Wales, Scotland or Northern Ireland were received by authors and will be used in this research. Authors received no information about which proportion of reports was associated with invalid or unknown postcode addresses. Thus, it is not known how many reports were removed from the dataset due to not containing a valid address. In order to ensure that using data with removed reports does not have a large impact on our results, we accessed the Action Fraud open data dashboard for crimes recorded in the last thirteen months (https://www.actionfraud.police.uk/data), downloaded available monthly
records of cyber-dependent crime, fraud and online shopping fraud from May 2019, which allow comparisons with data received by authors, and calculated the percentage difference and the Pearson's correlation coefficient between open data published by Action Fraud and data received via freedom of information request to Action Fraud. Differences observed were smaller than 30 percent in every month. The average difference between cyber-dependent crimes reported in the open data portal and cyber-dependent crimes received was -6.07 percent, while this difference was -8.73 percent for fraud and -9.98 percent for online shopping fraud. Correlation coefficients were significant in all three cases (i.e., cyber-dependent crime: \( r = 0.87, p - value < 0.001 \); fraud: \( r = 0.51, p - value < 0.05 \); online shopping fraud: \( r = 0.87, p - value < 0.001 \)). The moderate correlation coefficient observed for fraud is likely to be explained by the small number of months examined in this sensitivity analysis (15). Thus, data received are expected to provide valid indicators of crimes known to Action Fraud.

### 3.1.2 Routine Activities Data

In order to further explore the influence of COVID-19 on crime opportunities, it was considered relevant to examine whether routine activities that are potentially linked to fraud opportunities followed a similar trend to reported fraud. Although historical data are scarce, some sources were identified that could be analysed with the same methods as the crime data in order to show the potential impact of the pandemic on activities potentially related to crime opportunities. Firstly, the Office for National Statistics (2020d) collects data on retail activities; in particular, data on the value of sales conducted via the Internet. Shopping online has been identified as a potential predictor of online fraud victimisation (e.g. Leukfeldt & Yar, 2016; Reyns & Henson, 2015). On the other hand, some sources publish information regarding ticket sales, which is likely related to ticket fraud. In this sense, data from the Civil Aviation Authority (2020) show the number of air passengers that pass through UK airports, which provides an indication of the effects of COVID-19 on air ticket sales in the UK. In addition to this evidence of changes in tickets related to mobility, monthly cinema admissions provided by the UK Cinema Association (2020a; 2020b) serve as an indication of changes in leisure activities.
3.2. Analytic Strategy

In order to test the three hypotheses posed at the beginning of Section 3, univariate ARIMA models have been applied to the Action Fraud data described in the previous section. ARIMA models are a method for time series data analysis that employs past observations of one variable to predict its own future values. They are one of the most common approaches to time series analysis (Hyndman & Athanasopoulos, 2018) and, as described in the review of the literature in Section 2, they have been frequently used to study the effects of COVID-19 on crime. To apply the ARIMA modelling approach in the present paper, the values were selected for crime reports each month up until lockdown was introduced in March 2020, that is April 2017 to March 2020. This allowed computation of 95% prediction intervals for the time period up to March 2020 and, subsequently, parameters obtained from ARIMA models were used to forecast 95% prediction intervals for crime from April 2020 to July 2020. This allowed the known values of crime for April to July 2020 to be compared to the 95% prediction intervals in order to identify whether the known values of crime fall within the 95% prediction intervals given by the parameters from pre-COVID models.

In order to select the ARIMA model with the best goodness-of-fit for each variable (i.e., crime types and types of victims), we followed a variation of the Hyndman-Khandakar algorithm (see Hyndman & Khandakar, 2008) that automates the selection of the components $p$ (i.e. the order of the auto regressive model), $d$ (i.e. the order of differencing) and $q$ (i.e. the order of the moving average) of each ARIMA model estimated for each variable. This approach uses a stepwise search to select the model with the lowest AICc, a bias-corrected version of the Akaike Information Criterion (AIC) for small sample sizes, in each case. This is done to effectively select the best model for each variable in our data, and in turn improve the forecast accuracy of the ARIMA models. The auto.arima() function from the ‘forecast’ package (Hyndman, 2020) in R (R Core Team, 2020) was used to implement the Hyndman-Khandakar algorithm to estimate a univariate time-series ARIMA model for each of the crime types described above. R codes used in this research can be found as an Appendix. Moreover, an interactive data visualisation tool has been created to allow readers to visualise bivariate associations between crimes known to the police and changes in routine activities in the UK (see: data_visualisation_app).
4. Results

4.1 Total Cybercrime and Fraud

Figure 2 plots the 95% prediction interval for total cybercrime and total fraud from the corresponding ARIMA models as well as the actual count of recorded offences for the period April 2017 to July 2020. As can be observed in Figure 2a, in March, April and May 2020, total recorded cybercrime was markedly greater than the levels forecast based on the data from the previous 3 years. This three-month period witnessed a sharp spike in recorded cybercrime that dropped back to within the 95% confidence interval in June and July. Similarly, though with a slight delay in comparison to cybercrime, Figure 2b shows total recorded fraud also increased clearly beyond the bounds of the prediction interval in May and June 2020, and then bounced back to the original trend in July.

With regard to H\(^1\), based on the application of the ARIMA models to historical data of recorded cybercrime and fraud in the UK, we can reject the null hypothesis and conclude that the changes in cybercrime and fraud during the COVID-19 pandemic are greater than the crime variability that would be expected given historical trends.

![Figure 2](image)

**Figure 2.** ARIMA forecast and actual count of recorded cybercrime and fraud in the UK, April 2017-July 2020

4.2 Fraud Types

As set out in Section 3, H\(^2\) posits that trends for different types of fraud will not be homogenous during the pandemic; in particular, it states that online types may rise, and
offline types may fall. Figure 3 visualises the range of values forecast from the historical series as well as the known count rates for the four individual fraud types analysed in this research. Firstly, Figure 3a shows a steep increase in recorded online shopping and auction fraud in March, April and May 2020 that is far beyond the values that would be expected 95% of the time in accordance with the ARIMA prediction intervals. The number of recorded offences then dropped back down in June and July but is still out with the range of predicted values. Figure 3b indicates a similar trend with regard to dating fraud: a pronounced increase immediately subsequent to the introduction of lockdown measures in the UK followed by what appears to be a return to the less steep historical upward trend in June and July. In Figure 3c, we can discern that the trend for ticket fraud is clearly the inverse of that observed for the previous two fraud types. Ticket fraud appears to have a seasonal pattern, with peaks beginning in spring and continuing throughout summer in the three years prior to 2020. However, recorded ticket fraud during the COVID-19 pandemic has been reduced to close to zero. In April, May, June and July 2020, it was below the prediction interval and far below the numbers recorded in the spring and summer of 2017, 2018 and 2019. Finally, as shown in Figure 3d, door-to-door frauds have been on a downward trend since April 2017. This trend appears to have continued during the pandemic with a notable drop in April 2020; however, the reduction in this fraud type is within the values that were forecast by the ARIMA model.

Thus, based on the analysis of these four individual fraud types, the null hypothesis with regard to \( H^2 \) is not rejected because even though the cyber-enabled online shopping fraud and dating fraud did increase, ticket fraud, which is also cyber-enabled, decreased. As such, it appears not all cyber-enabled fraud has been affected in the same manner by the mobility restrictions associated with the pandemic. Furthermore, the decline in door-to-door sales fraud identified in the present study follows the pre-COVID downward trend and the variability during the pandemic is not beyond the 95% prediction intervals.
Although data are still scarce at this stage, some sources offer support for routine activities explanations regarding the disparities in the direction of certain fraud trends. For example, as can be identified in Figure 4a, the value of Internet retail sales (Office for National Statistics, 2020d) has followed a markedly similar trend to online shopping and auction fraud since March 2020. There was a sharp increase in the value of sales that were conducted online, far beyond the forecast values based on historical data, and sales may be beginning to return to closer to the original trend in July. Similarly, regarding ticket sales, data from the Civil Aviation Authority (2020) plotted in Figure 4b demonstrates the drastic effects of COVID-19 on air travel as the number of passengers passing through
UK airports plummeted between March and April. However, since the number of passengers began to drop before lockdown measures were launched in the UK, ARIMA prediction intervals were able to capture the observed values of air passengers in May, June and July. The air passenger data serve as an indication of changes in tickets sales related to mobility. In addition, monthly cinema admissions provided by the UK Cinema Association (2020a, 2020b) indicate enormous changes in ticket sales related to leisure activities. Figure 4c shows cinema admissions reached zero for the months with the strictest lockdown measures. In short, both these data sources that are related to ticket sales show very steep declines between March and April 2020, similar to that identified in recorded ticket fraud victimisation. The relationship between shifts in routine activities and shifts in crime opportunities is discussed in greater detail in Section 6.

Figure 4. ARIMA forecast and actual count of routine activities, April 2017-July 2020
4.3 Cybercrime and Fraud Suffered by Individuals and Organisations

This paper also enquires about potential divergences between individual and organisation victims (i.e. that individuals will experience a greater relative increase in victimisation than organisations) and, in this sense, the Action Fraud data do appear to indicate certain contrasts. Figure 5 details the prediction intervals and known counts of reported victimisation for total cybercrime, total fraud, and online shopping and auction fraud. Before proceeding to examine the results, three points should be noted. Firstly, City of London Police stated that disaggregated data for the two victim types are unavailable for October and November 2018. This can be observed by the gap in the time series plots. Secondly, the ARIMA models were not applied to dating fraud, ticket fraud and door-to-door sales fraud because the sample size of organisation victims was so small that the ARIMA models could not be correctly estimated. Thirdly, data about crimes suffered by organisations show unusual, very small values in December 2018, and January and February 2019. This is likely to be due to inconsistencies in recording, rather than actual changes in crime, but this does not have a major impact on the ARIMA models’ forecast accuracy.

With regard to cybercrime, Figures 5a and 5b show a difference in reported offences between individuals and organisations. The spike found in individual cybercrime victimisation is not present in the results for organisation victims, which remain firmly within the 95% prediction intervals for the period after the introduction of lockdown measures. There is a similar discrepancy in relation to total fraud in Figures 5c and 5d. The post-lockdown jump in fraud reported by individuals is not found for organisation victims in terms of values greater than the forecast prediction intervals. In this sense, while there does appear to be an increase in reported fraud in May and July 2020, this does not go beyond the ARIMA prediction intervals. Finally, Figures 5e and 5f show both a concordance and a divergence with respect to online shopping and auction fraud. On the one hand, reported victimisation climbs steeply for both individuals and organisations after the onset of the COVID-19 pandemic. On the other hand, the rise in cases reported by individuals took place in April and May 2020 and then dropped back, while reports by organisations rose slowly from April to June and then rocketed in June and July.

As a consequence of the aforementioned results for individual and organisation cybercrime and fraud victims, $H^3$ cannot be rejected and it can be stated that cybercrime
and fraud victimisation trends for individuals exceed the upper limits of the expected volume as opposed to victimisation trends for organisations, which do not.

![Figure 5. ARIMA forecast and known count of individual and organisation cybercrime and fraud victims in the UK, April 2017-July 2020](image)

5. Discussion

In his address to the American Society of Criminology, Rosenfeld (2018) advocated research on exogenous shocks and crime rates with the aim of testing theoretical expectations in criminology. In modern times, there has been no event that has potentially...
affected crime opportunities as greatly in such a short period of time as the COVID-19 pandemic. While the devastating impacts are felt by millions, criminologists have been presented with an unprecedented situation to study how short-term shocks to society affect crime trends.

Changes in mobility are arguably one of the most important variables to explain the convergence of the minimum elements of crime, as stated in the Routine Activities Approach (Cohen & Felson, 1979). However, it is also among the most difficult variables to control for. National lockdowns in response to the pandemic have created a natural experiment to capture this variable through time spent at home (Stickle & Felson, 2020).

In a paper prior to the pandemic, Miro-Lлинаres and Moneva (2019) already stressed the importance of time spent at home as an explanatory factor in the shift of criminal opportunities from physical space to cyberspace. In that piece, emphasis was placed on the growing adoption of online forms of entertainment, such as online shopping, streaming content, TV series, or computer games, to the detriment of traditional leisure in parks, bars, and streets. Yet the result regarding the convergence of offenders, targets and guardians is the same as that caused by lockdowns: more time at home and less time on the street. In other words, empty streets and a busy Internet. This scenario in which online convergence takes on a prominent role could explain an increase in certain forms of cybercrime and fraud that were observed in recent research (Kemp et al., 2020) as a result of a shift in opportunities from one environment to another (Miró-Lлинаres & Moneva, 2019). The relevance of such findings justifies further research to challenge these assumptions.

The present paper has responded to these calls and shown that the opportunity structures for fraud are indeed nuanced and that the recent reductions in offline routine activities are associated with disparate effects on distinct fraud types. As we have seen, less offline retail activity appears related to more online activity and, therefore, more online shopping fraud. On the other hand, less ticket-related offline leisure and transport activities have led to a decrease in ticket fraud. In this sense, ticket fraud provides an interesting example of online opportunity structures being affected by offline changes in routine activities; it demonstrates how a decline in activities in the physical world can also reduce opportunities for cyber-enabled frauds. Crime science has promoted the benefits of crime specificity for crime analysis since long before the current health crisis (Andresen & Linning, 2012; Clarke, 2010) and recent research has urged the study of particular
offences with respect to crime patterns and the pandemic (Stickle & Felson, 2020). As a consequence of the discrepancies found in this study, a crime-specific approach to fraud research and prevention appears more urgent than ever given the apparent boost to long-term upward trends in total reported fraud seen in 2020.

Similarly, reported cybercrime and fraud have evolved differently for organisation and individual victims. The reduced activity in the physical world was associated with marked effects on the general trends for the latter but had little effect on the former. This raises at least three very pertinent yet distinct possibilities. Firstly, it could be that with many businesses closed, opportunities to attack organisations have in fact been reduced rather than grown. It has been widely stated that attacks against organisations have risen (Europol, 2020b; Interpol, 2020), but it may be that such a general statement is overly simplistic and greater victim specificity is required when researching trends in cybercrime and fraud against organisations. In fact, academic literature has begun to examine the organisational characteristics related to cybercrime and fraud victimisation (Buil-Gil et al., 2021b) and future research could examine this within the context of COVID-19.

Secondly, it is unclear to what extent the divergences in individual and organisational victimisation during the pandemic are the result of differences in reporting. It seems plausible that with many organisations experiencing great changes to their daily functioning, many attacks have gone undetected and, thus, unreported. The move to teleworking in many industries may have impeded organisations’ ability to detect and respond to cybercrime and fraud events. This would highlight the crucial role of newly teleworking individuals as ‘guardians’ for their organisations with regard to cybercrime and fraud. In this sense, the peak in online shopping fraud in July 2020 may be due to IT services reporting all undetected offences from previous months. Or, thirdly, could it be that the difference in victimisation rates found in this paper is evidence of homeworking shifting risk onto the individual and away from the organisation (e.g. spam and computer viruses being received in personally-owned laptops instead of business computers)? Is a target being placed on underprotected individuals as opposed to organisations with IT support? This seems unlikely given the potentially greater spoils available to criminals who target organisations, but nevertheless further research is required.

Finally, further discussion is also necessary on the apparent return to longer-term trends identified in many of the general and specific crime types analysed in this paper. This coincides with the Google Mobility Data discussed in Section 2 and the Internet retail
sales data in Section 4, which seem to show a slow return to routine activities that are closer to pre-COVID levels. This is an indication of the potentially fundamental role of crime opportunities even in the short-term and compels future research on the criminal actors that are taking advantage of the changes in opportunity structures (Miró-Llinares, 2021). Was it already existing offenders who simply increased their offending during spring and early summer 2020 or did new actors enter the market inspired by the new opportunities? Given the partial return to the general trend rather than sustained increases, as well as the prior research that has highlighted adaptations of existing attack vectors to take advantage of the social and psychological turmoil created by COVID-19 (Collier et al., 2020; Europol, 2020a), it appears that the first option is more likely. Nevertheless, further analysis in this sense could add to wide-ranging theoretical debates on cybercrime, fraud and opportunity approaches.

6. Conclusion

The present paper contributes to the growing body of research on the impact of COVID-19 on crime by showing that in the UK, overall counts of reported cybercrime and fraud in the period immediately after the introduction of lockdown measures were notably higher than predicted by the time series technique applied in this research. However, and importantly for policy and practice, these general trends are not homogenous throughout all fraud types or when comparing individual and organisation victims. It has also been indicated that many initial spikes in cybercrime and fraud identified at the beginning of the pandemic appear to be dropping back to the longer-term gentler upward trend. All these conclusions open the door to future research as discussed in the previous section.

In reaching these conclusions, the present research is not without limitations. Notably, the secondary data used is the result of cybercrime and fraud offences reported to the relevant law enforcement body and collated by Action Fraud. On the one hand, the low levels of fraud reporting (Kemp, 2020) and cybercrime reporting (van de Weijer et al., 2019) mean that there may be a significant dark figure that is not accounted for in these figures. On the other hand, the methods for registering crime may vary across time, which could distort historical analysis. Despite these rather typical limitations with the official crime data, the results and conclusions contained herein can help inform future research and practice with regard to changes in routine activities and the consequent shifts in crime opportunities.
References


