DOI: 10.1111/1745-9133.12629

CRIMINOLOGY & Public Policy

SPECIAL ISSUE ARTICLE

CYBERCRIME AND CYBERSECURITY

Dating hot spot to fraud hot spot: Targeting the social characteristics of romance fraud victims in England and Wales

Richard Sinclair[1] | **Matthew Bland**[2] | **Bradley Savage**[1]

[1]City of London Police, Guildhall Yard East, London, UK

[2]Institute of Criminology, University of Cambridge, Cambridge, UK

Correspondence
Richard Sinclair, City of London Police, London, UK.
Email: richard.sinclair@cityoflondon.police.uk

Abstract

Research Summary: We found that romance fraud was rising year-on-year across every region in England and Wales, increasing 55% during the 3 years between October 2018 and October 2021. Fifty percent of all the romance fraud victims in the period resided in 17% of the places where romance fraud had occurred. A total of 439 locations (outward postcode areas) were identified as the "power few" in the first year of the data set. Of these 439 locations, 162 of them recurred in both of the following years, becoming chronic "hot spot" locations containing more than one in six of all reported romance fraud victims. The demography of victims in repeat locations differed considerably, but hot spots were more frequently predominantly populated by less affluent populations.

Policy Implications: We conclude that the current national one-size-fits-all fraud prevention approach may not be the most efficient or effective way to reach those victims who most require crime prevention advice. The National Fraud Intelligence Bureau, based in the City of London Police, could adopt a tailored approach to providing preventative information to local police forces

based on the year-to-year patterns in crime and the associated intelligence provided by sociodemographic data sources such as Acorn.

KEYWORDS
Acorn, cybercrime, evidence-based policing, fraud prevention, fraud victims, romance fraud, sociodemographic analysis

Romance fraud has penetrated broader public consciousness in recent years following a number of high-profile cases and media coverage such as Netflix's "Tinder Swindler" documentary and MTV's "Catfish" reality show. Romance fraud occurs where "a person is defrauded by an offender(s) through what the victim perceives to be a genuine relationship" (Cross et al., 2018, p. 1304). In many respects, it is like any other type of online or offline fraud in that the offence involves dishonesty and manipulation of the victim and victim vulnerability is often a key ingredient in the commission of the crime. But unlike most other forms of fraud, the victims of romance fraud suffer a double victimization, the financial loss and the emotional loss of a perceived romantic relationship. Romance fraud is different to other frauds in that it involves intimacy, one of the "most important features of an individual's life, and it goes to the heart of their autonomy" (Gillespie, 2017, p. 231). Victims of online romance fraud are targeted in their own homes, where they are supposed to feel safe, using online platforms they trust to protect them. However, with the popularity of online dating, romance fraud has become one of the fastest growing high-harm fraud types (Buil-Gil & Zeng, 2022). Colloquially referred to as "online dating scams" or "catfishing," fraudsters will often groom victims during a long period, enhancing the emotional pain when the victims finally realize they have been scammed. As we will describe, like other online frauds, reports of romance fraud cases have been rising, but scholarly research, particularly focusing on potential intervention strategies, has not (yet) kept pace with this growth. This paper seeks to contribute to that growth through the exploration of demographic trends among romance fraud victims. It will demonstrate that this crime type is pervasive across demographics and will explore the theoretical and practical implications of this new finding in the context of geographic concentrations commonly known as "hot spots."

In England and Wales, the City of London Police is the lead policing agency for fraud and cybercrime. They are funded to host both Action Fraud, which is the national centralized reporting center for all fraud and cybercrime reports, and the National Fraud Intelligence Bureau (NFIB), which analyzes, reviews, and disseminates fraud reports to police forces and law enforcement partners. Crime reports from the public and businesses are received through a telephone call to the Action Fraud national call center or through the Action Fraud online self-reporting service, where reports are recorded on a single information technology (IT) platform called the Strategic Analysis and Intelligence Platform (SAIP). For the financial year 2020/2021, Action Fraud received 413,945 reports of fraud directly from victims, which equated to £2.35 billion of financial loss to victims (National Fraud Intelligence Bureau, 2021).

The NFIB publishes analytical products and reports for its fraud priorities, one of which is romance fraud, as part of its role as the national policing lead for fraud and cybercrime. Each year, the NFIB's main products provided to police and law enforcement partners are the national annual assessments for both fraud and cybercrime, which provide the previous year's overview of fraud and cybercrime in England and Wales. These reports are designed for police forces, government

departments, and law enforcement partners to effectively target their resources and outputs at tackling fraud in line with the U.K. government's drive to reduce fraud and cybercrime. These priorities have grown in weighting in recent years as online criminality rapidly appears to take over from "in-person" criminality as the majority form of crime. Currently, a person in the United Kingdom is more likely to be a victim of fraud and cybercrime than any other crime (Home Office, 2021), and extra government funding has been invested for law enforcement to tackle this. Further, the National Police Chiefs Council (NPCC) has published the National Policing Digital Strategy 2020–2030, advising police and law enforcement to utilize big data and machine learning as a strategic asset, to tackle modern day crimes such as cybercrime, increasingly effecting victims in England and Wales (National Police Chiefs Council, 2020).

A major part in protecting victims from fraud and cybercrime is crime prevention. Often there are few viable lines of inquiry for police investigators or the suspects are believed to reside abroad, meaning normal criminal justice response of prosecute to protect is not possible and preventative responses are one of the response options open to agencies. In 2020, the NFIB and the National Economic Crime Centre (NECC) jointly ran a national campaign targeting romance fraud, and as part of this campaign, victims were targeted with generic crime prevention communications through the conventional police communication methods of Twitter, Facebook, and Instagram, plus media releases on police forces and law enforcement partners Web sites. Arguably, this type of communication will only reach those people already involved with or engaging with those digital media, who are already receptive to crime prevention information. Police use of social media is challenging (Bullock, 2018; Israni et al., 2017) and police resources are often geographically focused rather than organized for online response. The fact remains that victims of romance fraud live somewhere and the organization of fraud in England and Wales means that the residence of the victim is the determining factor in the allocation of a case. The patterns of geographical incidence of romance fraud are so far under explored, but we argue that they are not theoretically redundant, we just do not know enough to rule them in or out as useful for devising prevention activities. For example, we content that it is feasible that theoretical constructs that may be linked to romance fraud vulnerability, such as social bond theory (Hirschi, 1969) or self-efficacy theory (Bandura, 1977), could be influenced at least in part by geographical context. If this were the case, then police may be able to develop a more familiar preventative framework such as hot spot policing (see Weisburd & Eck [2004] for a description), but this area also has broader scientific importance because the issue of geographic patterns in cybercrime victimization is not well studied. The data set we work with offers opportunities to classify communities and tailor responses *if* there are geographical concentrations of romance fraud victims. This study seeks to address these issues by answering the following research questions:

1. Can geographic hot spots of romance fraud be identified and cross-referenced with "segmentation data?"
2. If so, how stable are romance fraud hot spots throughout time?
3. To what extent might preventative approaches be locally tailored using segmentation data?
4. What types of preventative activity does the profile of key segmentation groups suggest?

We define "segmentation data" as geodemographic consumer data that "segment" populations into groups, categories, and types according to multiple data sources. As we will describe, we use data provided by the Acorn data set, provided by CACI,[1] which provides a unique addition to fraud-targeting literature. This approach has been used before in fraud prevention (National Fraud Authority, 2011) but is not common practice nor has it been revised in more than a decade.

Segmentation data are most commonly used in marketing, where it is used to tailor advertising campaigns to maximize effectiveness.

This paper proceeds with a short exploration of the existing romance fraud literature to place the analysis in the proper context. We then discuss our data sources and the descriptive analysis applied to them before turning to the results and their implications for policy, practice, and future research.

1 | ROMANCE FRAUD

Romance fraud is one of the highest forms of financial loss of all fraud types internationally (Cross & Holt, 2021) but as with general types of fraud, there is a dearth of research on the personality characteristics of fraud victims (Buchanan & Whitty, 2014) especially concerning what characteristics put people most at risk of harm. Buchanan and Whitty examined surveys of 853 online daters to try and identify risk factors for victimization, finding that higher levels of "romantic beliefs" increased the likelihood of becoming a victim. This is a simple premise: if the victim craves romance and a relationship, they are more vulnerable to an offender's fraudulent techniques. The promise of this simple premise is powerful nevertheless: if law enforcement agencies can identify characteristics of potential victims, then if they cannot act as a capable guardian online, they could use their resources to target these potential victims with crime prevention advice.

Demographics might prove to be a source of such characteristics. Victim demographics were researched by Whitty (2018) who tested the predictive power of 12 demographic factors via victim and nonvictim surveys that focused on psychological characteristics of scam victims and nonscam victims. Whitty broadly found that victims tended to be characterized as middle-aged, well-educated women, impulsive, less kind, and more trustworthy and have an addictive disposition. However, of the sample of 11,780 people Whitty surveyed, 10,723 were not in fact victims and only 200 had been subjected to a romance fraud. Whitty suggests there is something more to becoming a victim than solely romantic attitudes, but establishing this requires research using a much larger sample size of actual romance fraud victims to understand effectively.

Research on romance fraud, like Whitty's (2018) study, has normally featured small sample sizes of actual victims and relied on victims volunteering to speak with a researcher about their experiences. Samples are unverified against police crime records, and subjective to that individual's perspective. Pease et al (2018) stated that victims often "flag" themselves as vulnerable to crime, and "boost" themselves to offenders. In the case of romance fraud, it could be victims have flagged themselves by being on a dating site looking for love, and because they believe they are in a romantic relationship, they are rendered more vulnerable to crime by disclosing details of the money and assets that could be targeted by an offender. What is difficult to ascertain from the current body of romance fraud research is exactly what demographics are common in such victims.

A frequent way for offenders to build trust with victims is using online dating profiles claiming to be in a position of authority (Cross & Layt, 2022; Whitty, 2013). The use of military personnel, teachers, lawyers, and doctors as professions on dating profiles are used to gain trust with victims, as there is an expectation in society that those are professions of honesty and integrity (Cross & Holt, 2021; Cross & Layt, 2022). Professions like military service provide the offenders with a plausible reason for not meeting in person or by a video call, which helps support the fictious identity of the offender. Cross and Holt (2021) conducted a study of victims ($n = 3259$) who reported victimization to the Australian Consumer and Competition Commission, finding 15% of offenders in these reports used a military profile. Common reasons for requesting money were

for the offender to send and receive consignments, or so they can leave the military and live with the victim. These cover stories are used to fool the victim into parting with their money for the promise of a romantic relationship (ibid). Other research suggests these findings might generalize to victims internationally (Rege, 2009; Whitty, 2018), so it is important to consider this when looking at early intervention with potential victims, and the likelihood of some profiles being more appealing than others, luring victims into the online space for offenders to defraud them.

What is clearer is that the longer the relationship continues, the more emotional investment is provided by the victim (Carter, 2021). Carter found that where the offender is allowed to build up a relationship of shared interests with the victim, persuasion is more likely to be successful. For law enforcement or partners to protect victims, they need to be engaged with at the earliest opportunity. If law enforcement can intervene before stage 1 and certainly before stage 4 of Whitty's (2013) Scammer Persuasive Technique Model,[2] then victimization might be averted by educating victims on their exposure to risk (Offei et al., 2022; Titus & Gover, 2001). In this vein, Burns and Roberts (2013) conducted an Australian study of online protective behaviors ($n = 150$), looking at people's attitudes to online privacy and protective behavior. This study found that influence from external parties had a significant bearing on whether an individual intends to engage or not, in protective behaviors. This echoes the notion that an influential predictor of students setting their social media profiles to private was if their friends have adopted the same security measure (Lewis et al., 2008) and gives encouragement to law enforcement agencies and other crime prevention parties that behavioral change is possible.

2 | DATA AND METHODOLOGY

2.1 | Action fraud data

All victims of fraud and cybercrime in England and Wales report crimes against them to Action Fraud, where they are recorded and then processed by the NFIB, on behalf of the 43 police forces in England and Wales. Reports can be made either by telephone to the Action Fraud call center or online through the Action Fraud Web site. Each crime report is given a unique reference number, called a National Fraud Reporting Centre number (NFRC), and key information is requested from the victim including their name, date of birth, address including postcode, ethnicity, when the offence occurred, and a description of what crime they have been a victim of.

The data from these crime reports are collated in the SAIP database. They are allocated a unique fraud code to identify the offence in accordance with the Home Office Counting Rules (HOCR), so they can be searched and retrieved for research, analysis, and auditing. The fraud code for romance fraud is NFIB1D and for this research, this was the search terminology to retrieve the data.

Action Fraud data are stored and handled in accordance with Management of Police Information (MOPI) guidelines and legislation under the Data Protection Act 2018. Data are stored electronically in a retrievable format, with protections in place to prevent them becoming altered, lost, damaged, or destroyed. These protections maintain the integrity of the data, ensure no variability in the data on further retrieval of them, and allow replication of the research.

The limitations of the Action Fraud records are that they are self-reported by victims of crime who, on 82% of occasions in the year 2020/2021, completed fraud reporting online (National Fraud Intelligence Bureau, 2021). Unless there was a need to verify the data, such as during a police investigation of the crime report, the details are often unchecked by the NFIB so this could mean thstbl-ere are inaccuracies or false reports. Research has found that the coding of variables such

as vulnerability is a gap in these data (Skidmore et al., 2020a). A dip sample of 500 records from the extracted data found misclassification rate of 4% with the crime recorded. These records were not removed from the data set analyzed.

2.2 | Acorn data

Acorn is the name of the consumer classification data tool that segments the U.K. population by postcode and is provided and maintained by CACI. CACI uses a variety of sources to build demographic profiles of addresses in the United Kingdom, so that companies, government departments, and local authorities can tailor their services to specific groups of people effectively. CACI use Open Data, Government Data, Commercial Data, and CACI Proprietary Data sources to build the Acorn database. It also utilizes data from the U.K. census, rental data, and third-party data sets, including Land Registry. Surveys such as the Crime Survey of England and Wales are used to enhance the accuracy of the database. The data set is commercially sensitive so we were unable to investigate the methodology in full, but the output is granular enough to potentially enable targeted prevention activity based on consumer behaviors and other routine activities. The following paragraphs explain how.

Acorn assigns areas of the United Kingdom into segments using Ordinance Survey and Royal Mail data sources. This then allows them to segment the people within those localities by demographic segments and further into hierarchical subgroups. There are six Acorn "categories," followed by 18 Acorn "groups" that in turn are composed of 62 Acorn "types," as illustrated in Table 1. The hierarchical Acorn terminology of "categories," "groups," and "types" and their color codes are consistently used in the Acorn data and will be used as terms throughout this research.

From these segments, Acorn "pen portraits" are created, which summarize each segment's demographics, financial status, and lifestyle traits. For finer demographic detail, CACI created Acorn "knowledge sheets," giving a further detailed insight into the demographic expectations for that postcode or household, predicting behaviors such as online use, and marketing channels likely to engage that household. Acorn data were provided in a data package that worked with Microsoft Excel, and an Acorn directory was also provided that allowed for the Action Fraud-reported victim postcodes to be matched to the Acorn data set to generate the Acorn categories, groups, and types for that postcode and household.

The principal limitation of the Acorn data set is that it is "black box" in nature. It is a commercial product, and the researchers had no access to the exact methodology used to determine a classification or build a pen picture or knowledge sheet. Other commercial products (e.g., Mosaic by Experian) are available but are equally opaque in methodology. This research does not seek to test the validity of the Acorn data set, it is instead an exercise in describing patterns of romance fraud victims through the lens of these data.

3 | ANALYTICAL PROCEDURE

Action Fraud data that were allocated the NFIB fraud code NFIB1D for the period of October 13, 2018 to October 12, 2021 was extracted from SAIP to provide 3 years of romance fraud victim data. This resulted in the retrieval of 21,954 victim records. A data cleaning process followed. First, records were removed where the address was not in England and Wales ($n = 1064$), and the address was incomplete or did not exist ($n = 3157$). This was required to conduct comparisons with the Acorn data set by postcodes in England and Wales.

TABLE 1 Acorn classifications

Acorn Category	Acorn Group	Acorn Type	
1 Affluent Achievers	1.A Lavish Lifestyles	1.A.1	Exclusive enclaves
		1.A.2	Metropolitan money
		1.A.3	Large house luxury
	1.B Executive Wealth	1.B.4	Asset rich families
		1.B.5	Wealthy countryside commuters
		1.B.6	Financially comfortable families
		1.B.7	Affluent professionals
		1.B.8	Prosperous suburban families
		1.B.9	Well-off edge of towners
	1.C Mature Money	1.C.10	Better-off villagers
		1.C.11	Settled suburbia, older people
		1.C.12	Retired and empty nesters
		1.C.13	Upmarket downsizers
2 Rising Prosperity	2.D City Sophisticates	2.D.14	Townhouse cosmopolitans
		2.D.15	Younger professionals in smaller flats
		2.D.16	Metropolitan professionals
		2.D.17	Socialising young renters
	2.E Career Climbers	2.E.18	Career driven young families
		2.E.19	First time buyers in small, modern homes
		2.E.20	Mixed metropolitan areas
3 Comfortable Communities	3.F Countryside Communities	3.F.21	Farms and cottages
		3.F.22	Older couples and families in rural areas
		3.F.23	Owner occupiers in small towns and villages
	3.G Successful Suburbs	3.G.24	Comfortably-off families in modern housing
		3.G.25	Larger family homes, multi-ethnic areas
		3.G.26	Semi-professional families, owner occupied neighbourhoods
	3.H Steady Neighbourhoods	3.H.27	Suburban semis, conventional attitudes
		3.H.28	Owner occupied terraces, average income
		3.H.29	Established suburbs, older families
	3.I Comfortable Seniors	3.I.30	Older people, neat and tidy neighbourhoods
		3.I.31	Elderly singles in purpose-built accommodation
	3.J Starting Out	3.J.32	Educated families in terraces, young children
		3.J.33	Smaller houses and starter homes

(Continues)

TABLE 1 (Continued)

4 Financially Stretched	4.K Student Life	4.K.34	Student flats and halls of residence
		4.K.35	Term-time terraces
		4.K.36	Educated young people in flats and tenements
	4.L Modest Means	4.L.37	Low cost flats in suburban areas
		4.L.38	Semi-skilled workers in traditional neighbourhoods
		4.L.39	Fading owner occupied terraces
		4.L.40	High occupancy terraces, culturally diverse family areas
	4.M Striving Families	4.M.41	Labouring semi-rural estates
		4.M.42	Struggling young families in post-war terraces
		4.M.43	Families in right-to-buy estates
		4.M.44	Post-war estates, limited means
	4.N Poorer Pensioners	4.N.45	Pensioners in social housing, semis and terraces
		4.N.46	Elderly people in social rented flats
		4.N.47	Low income older people in smaller semis
		4.N.48	Pensioners and singles in social rented flats
5 Urban Adversity	5.O Young Hardship	5.O.49	Young families in low cost private flats
		5.O.50	Struggling younger people in mixed tenure
		5.O.51	Young people in small, low cost terraces
	5.P Struggling Estates	5.P.52	Poorer families, many children, terraced housing
		5.P.53	Low income terraces
		5.P.54	Multi-ethnic, purpose-built estates
		5.P.55	Deprived and ethnically diverse in flats
		5.P.56	Low income large families in social rented semis
	5.Q Difficult Circumstances	5.Q.57	Social rented flats, families and single parents
		5.Q.58	Singles and young families, some receiving benefits
		5.Q.59	Deprived areas and high-rise flats
6 Not Private Households	6.R Not Private Households	6.R.60	Active communal population
		6.R.61	Inactive communal population
		6.R.62	Business areas without resident population

Then, repeated entries for the same victim were removed ($n = 2158$). These repeat entries were where a victim, or representative, re-entered the same data in the Action Fraud reporting system multiple times, or a system-generated error had meant several versions of the same entry had been created. As this research looked at demographics by location, the victims only needed to be counted once; therefore, after removal of the duplicate entries, 15,575 victims, or units of analysis, were left to analyze for the 3-year period. These were the only cleansing methods used to avoid selection bias, and there was no specific removal of individual victims due to any demographic

or location details. The Action Fraud victim data set was subdivided into three annual blocks by date to allow for year-on-year comparisons. Year 1 contained the victims from October 13, 2018 to October 12, 2019; Year 2 victims from October 13, 2019 to October 12, 2020; and Year 3 victims from October 13, 2020 to October 12, 2021.

CACI provided its Acorn data in a directory format, which was downloaded to the City of London Police IT system and allowed for victim postcodes to be entered in bulk. This generated an Acorn category, group, and type for each romance fraud victim record. Owing to the size of the data set, and some full postcodes having so few romance fraud victims, we altered the unit of analysis from "full postcode" to "outward postcode." This term refers to the first part of a U.K. postcode (a character or two characters followed by one or two digits) that contains information about the local post district. There are around 2900 such districts in the United Kingdom. We assigned a number of victims to each of these units and ranked ordered them to establish a "power few" (Sherman, 2007) concentration of the postcodes that were attributed the most romance fraud offences. In practice, this meant establishing a threshold of three or more offences on different victims each year as the definition of a "hot spot." Our units of analysis are substantially larger than those conceived in most hot spot studies (see Braga et al., 2019), but we justify this because our scope is much broader—a whole two nations—our sample of crimes is much smaller and we are more concerned with predominant demographic trends than hard features of the local environment.

To visualize the geographic location of victims, the locations of the power few by outward postcode were input into ArcGIS Pro. This visually identified the hot spot locations of victims, and illustrated what Acorn category, group, and type most victims in that outward postcode area were in. The demographics of the victims in the locations, according to the Acorn data, were analyzed to see if demographic characteristics suggested victims have individual requirements in different geographic locations across England and Wales. Within some of the locations, multiple Acorn groups ranked joint top for frequency, and we include all of these in our findings.

For a comparison of two areas of England and Wales with high rates of romance fraud, but different demographic categories, Crawley in England and Whitchurch in Wales were chosen for a comparison of demographic characteristics from the Acorn knowledge sheets. This was to ascertain key differences in how victims and potential victims may be accessible and respond to crime prevention by law enforcement based on the recommendations of CACI. The demographic characteristics chosen were those deemed most relatable to accessing victims and potential victims for crime prevention communication and education. This selection is called "feature engineering" and is used to reduce large raw data sets to a more manageable dimension (Spiegelhalter, 2019).

4 | RESULTS

4.1 | Trends and hot spots

The data indicated that romance fraud reports increased annually throughout the period of study. As Table 2 shows, between years 1 and 3 victim reports increased by 55% in England and Wales. Regionally, this increase was consistent across the entirety of England and Wales.

Combining the Action Fraud victim data for 15,575 victims and the corresponding victim demographic data from the Acorn directory, the postcodes for the 15,575 victims generated the Acorn category, group, and type for each victim at a full postcode level. At this level, only 3.2% of full postcodes had more than one romance fraud offence in the 3 years (487 full postcodes that contained 1001 of the total victims). At the outward postal code level, concentrations and repeats

TABLE 2 Annual reports of romance fraud by policing region

Region	Year 1	Year 2	Year 3
South East	835	932	1119
London	659	720	1070
East	477	516	744
South West	444	493	694
North West	408	445	639
East Midlands	387	427	613
West Midlands	361	428	619
Yorkshire and the Humber	342	390	486
Wales	182	272	361
North East	142	162	208
England and Wales total	4237	4785	6553

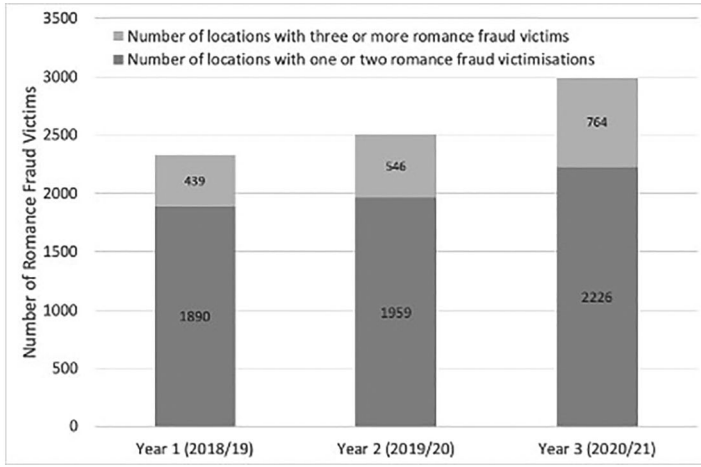

FIGURE 1 Annual breakdown of "hot spot" numbers of romance fraud in England and Wales 2018–2021.

are naturally greater. As Figure 1 shows, at least 18% of affected outward postcodes had three or more victims in each of the 3 years we analyzed. The figure also shows that this concentration of multiple victimization locations increased in each year. Overall, 50% of all romance fraud victims resided in 17% of the locations where it had occurred.

We isolated these "hot spot" outward postcodes to assess for stability across the 3 years. As Figure 2 shows, in year 1 there were 439 hot spots. In year 2, 216 (49%) of these were hot spots again. Of these 216, 162 remained "hot" in year 3, a 75% conditional probability that a hot spot that has been stable for 2 years will stay hot for a third. For the purposes of our analysis, we label these "chronic hot spots." Of the 223 outward postcodes from year 1 that did not appear in year 2, 103 of those featured again as having three or more victims in year 3 and we label these as "secondary hot spots." Of those 216 outward postcodes that were in the power few in years 1 and 2, 54 were not in year 3. We also classed these as secondary hot spots for this research as they featured twice during the 3 years but in a different configuration.

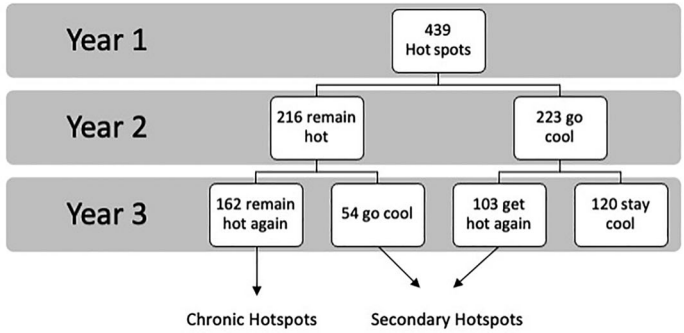

FIGURE 2 Year on year stability of hot spots for romance fraud.

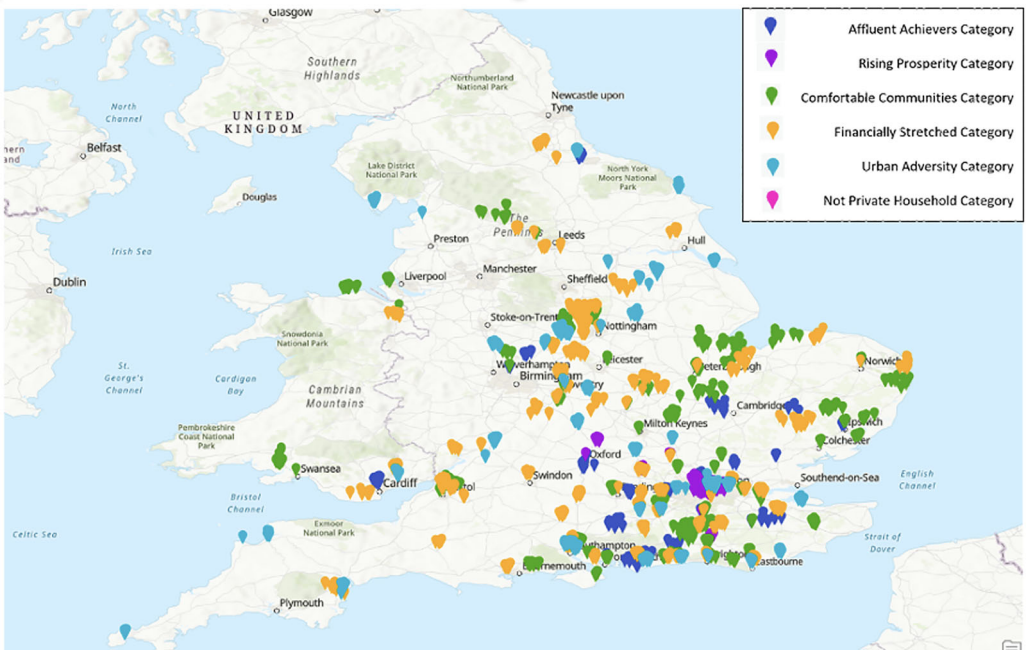

FIGURE 3 Map showing victim locations by Acorn category in "chronic" hot spots. [Color figure can be viewed at wileyonlinelibrary.com]

4.2 | Targeting and prevention in hot spots

The most frequently occurring segmentation data "categories" and "groups" in the chronic and secondary hot spots are listed in Table 3.

The totals in Table 3 exceed 100% because Acorn groups featured as joint most frequent for a hot spot and are counted twice. For example, Striving Families was the most prevalent group in 11 outward postcode hot spots and in a further 14 it was the joint most prevalent. These results depict prevalence rather than rate and merely describe the distribution of romance fraud hot spots by segmentation classification, not the per population in each classification.

We mapped the classification categories of chronic and secondary hot spots to examine geographic patterns (Figures 3 and 4). Our results indicate two premises: first, that romance fraud

TABLE 3 Breakdown of Acorn categories and groups in chronic and secondary romance fraud hot spots

Acorn category	Percentage of secondary hot spots where most prevalent	Percentage of chronic hot spots where most prevalent	Acorn group	Percentage of secondary hot spots where most (or joint most) prevalent	Percentage of chronic hot spots where most (or joint most) prevalent[a]
Financially Stretched	42%	35%	Modest Means	16%	1%
			Poorer Pensioners	16%	9%
			Striving Families	13%	15%
Urban Adversity	24%	22%	Young Hardship	13%	13%
			Difficult Circumstances	13%	7%
			Struggling Estates	11%	10%
Comfortable Communities	20%	27%	Successful Suburbs	13%	%
			Steady Neighborhoods	10%	11%
			Countryside Communities	6%	5%
			Starting Out	6%	6%
			Comfortable Seniors	3%	4%
Affluent Achievers	9%	9%	Executive Wealth	10%	15%
			Mature Money	10%	6%
Rising Prosperity	4%	8%	Career Climbers	11%	13%
			City Sophisticates	2%	6%

[a]Percentages sum to >100% due to inclusion of joint most prevalent.

TABLE 4 Distribution of individual postcode classification in chronic and secondary hot spots

Region	Affluent achievers	Rising prosperity	Comfortable communities	Financially stretched	Urban adversity
East Midlands	4%	0%	10%	55%	32%
East	9%	1%	43%	37%	10%
London	3%	44%	7%	10%	36%
North East	11%	0%	0%	51%	39%
North West	26%	0%	31%	9%	34%
South East	11%	4%	29%	36%	19%
South West	4%	0%	17%	55%	24%
Wales	0%	15%	27%	46%	12%
West Midlands	10%	0%	22%	40%	29%
Yorkshire and the Humber	0%	5%	11%	46%	38%

affects all demographics but second, that it affects different groups in different places. For example, "Rising Prosperity" hot spots largely emanate from the greater London region. "Affluent Achievers" hot spots cluster around London and the South East. By contrast "Financially Stretched" hot spots are widely present in England and Wales.

We offer Table 4 as a further deconstruction of regional variations and examination of the distribution of individual postcodes within the chronic and secondary hot spots. The predominance of "Financially Stretched" locations in the most frequently victimized places stands out but so do acute variations in London, the East, and the North West. If we consider the premise of segmentation data as true—that there are inherent differences in the way each category, group, and type consume and engage with information—then these data speak to a need for differing approaches within each region to engaging with potential victims.

To contrast how engagement approaches might differ from Hot spot to Hot spot, based on their classification we cross-referenced two chronic hot spots: Crawley in the South East, where the predominant classification was "Financially Stretched," and Whitchurch in Wales, where the predominant classification was "Affluent Achievers." Table 5 gives a sample of the different "likely interactions" provided by segmentation data.

The next section discusses what these findings could mean for crime prevention for romance fraud victims in chronic and secondary postcodes. The discussion will detail the limitations of the research and these data sets, what the policy implications are for police forces and law enforcement, and what crime prevention changes could possibly be provided to victims across England and Wales.

5 | DISCUSSION

5.1 | Implications for theory

Our findings do not explore victimization in the context of population rates. We chose to analyze absolute numbers of crime to begin this line of scientific inquiry and the results clearly demonstrate that although there is some concentration in demographic groupings, every major

TABLE 5 Comparison of different types of engagement opportunities between differing hot spots

Activity	Crawley (Financially Stretched)	Whitchurch (Affluent Achievers)
Newspaper	The Sun	Daily Telegraph
Magazine	Health	Travel
	Celebrity	Home and gardening
	Music and film	
Typical internet use (per week)	0–2 h	20+ h
Digital attitude	"Computers confuse me and I'll never get used to them"	"I am worried personal information I enter online will not remain secure"
Social media use	Daily	Less than weekly
Use of social media	Take part in groups/forums	Checking email
Top online activities	Redeem vouchers	Studying
	Shopping	Checking investments
	Games with children	Using search engines
Favorite Web sites	Very.co.uk	Santander
	JamieOliver.com	Marks and Spencer
	Hungry Horse	John Lewis
	Just Eat	BBC Good Food
Occupations	Shop worker	Retired
	Skilled/manual worker	Director/Managerial
Marketing channel most likely to see and respond to	Leaflet at the door or newspaper	Newspaper adverts
		Cinema adverts
		Mail
How they get information on retail and leisure	Email	Mobile apps
How they manager their current account	By post or in branch	Online

Acorn grouping experienced chronic romance fraud somewhere. This is particularly interesting for future theoretical explorations of this crime type, not by singling out any one type of driving theoretical framework but by emphasizing the need for a plural approach. Although Acorn is not a pure measurement instrument of deprivation, economic well-being is clearly a key component. That all of the major categories were the most populous in chronic locations of romance fraud somewhere infers that economic status is not the predominant determinant of propensity for vulnerability, or at least, not based on these data. This does not exclude the possibility that weaker social bonds play a role. The presence of the two "least affluent" categories as the most commonly prevalent group in chronic hot spots (Table 3) indicates that there is some potential for the conventional application of social bond theory to apply, but we argue the theoretical framework for understanding romance fraud at large is more complex. All Acorn categories are connected by the human desire to form romantic relationships, but the mechanisms for vulnerability among "poorer pensioners" and "career climbers" are probably quite different and therefore require different theoretical analyses.

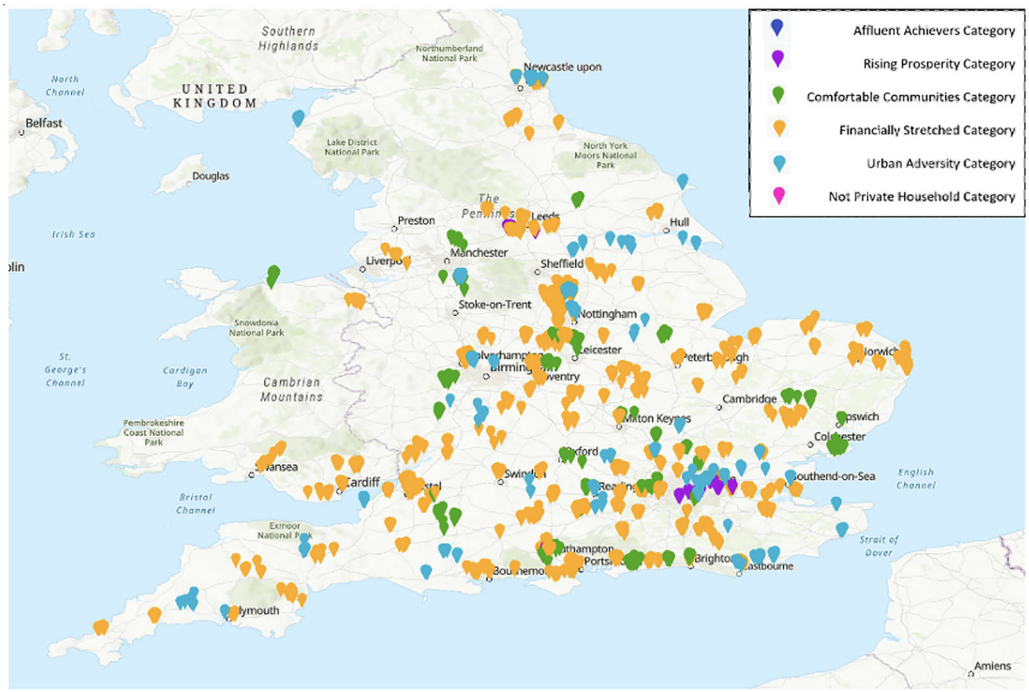

FIGURE 4 Map showing victim locations by Acorn category in secondary hot spots. [Color figure can be viewed at wileyonlinelibrary.com]

One unifying construct may lie in routine activity theory (Cohen & Felson, 1979). We are not the first scholars to make the connection between cybercrime, fraud, and routine activities (Holt & Bossler, 2008; Payne, 2020; Pratt et al., 2010) and our speculation is based on straightforward premises. The proliferation of smartphones and mobile dating applications has caused more connection between vulnerable victims and motivated offenders in unprotected spaces, although the establishment of geographic repeat locations in this study must not be entirely conflated as those unprotected spaces. As Rege (2009) points out, the internet has changed the way people meet and form relationships. Dating can now be anonymous, private, 24 hours-a-day, and with instant results through direct messaging. Algorithms also have a key role in "matching" people. Our data set gives a window to prevention opportunities in this digital space, not increased risk by geographical environment. To properly establish a framework for routine activities, we would need to collect data on dating application use and this was beyond our scope to achieve. However, this does not mean that action to intervene cannot be taken now based on the hypothesis that routine activities play a role both in the vulnerability of the victim and in providing an opportunity for prevention treatment to be applied through the trends established in Acorn data.

5.2 | Implications for practice

We make several recommendations for practice, which have broader implications than just for England and Wales and are constructed primarily in the operating context of that setting. Previous research has identified that some, including officers themselves, perceive gaps in the local

responses to fraud (Button, 2021; Skidmore et al., 2020b). In the report *A Review of Fraud: Time to Choose* (HMICFRS, 2021), it was highlighted that the NFIB provided crime prevention advice to police forces and Regional Organized Crime Units (ROCUs), but this advice was rarely evaluated as to the effectiveness of it. In the U.K. government's *Beating Crime Plan* (Home Office, 2021), the government has prioritized fraud, cybercrime, and online crime for targeting by law enforcement, emphasizing that fraud, cybercrime, and online crime represent more than 50% of all crime in the United Kingdom, and that better support must be given to victims of fraud. Subsequently, the U.K. government's spending review for 2022–2025 has allocated increased funding to law enforcement in England and Wales to build the capacity and capability to tackle fraud. This has led to an uplift of staff in police forces and ROCUs to provide a better service to victims and tackle organized crime groups targeting victims with fraud. Police forces and ROCUs must review their outputs in relation to fraud and how they protect fraud victims, including romance fraud victims.

Fraud education and training is part of the City of London Police's role as lead force for fraud and cybercrime. Fraud investigation in England and Wales utilizes the Fraud Investigation Model (FIM), taught by the City of London Police's Economic and Cyber Crime Academy to law enforcement staff across the United Kingdom and Internationally. This investigation model was devised by the City of London Police and differs from other models for investigation, where instead of gathering suspect evidence prior to taking overt police action, the FIM puts crime prevention right at the start of the response and encourages prioritizing overt action to stop repeat victimization. Information, data, and advice for crime prevention come from generic national crime prevention advice provided by the NFIB, often included in their national assessments of fraud and cybercrime. These are disseminated in the same format to all police forces and law enforcement partners across England and Wales to inform their outputs for fraud and cybercrime.

This research suggests that in the case of romance fraud, targeting crime prevention in nationwide blanket campaigns is unlikely to be the most efficient method. The findings of this research show romance fraud continued to rise year-on-year in every region, so arguably the crime prevention messaging that has been used by law enforcement and partners has not been effective at reducing crime (although we acknowledge this argument cannot be won on this premise alone). This research found chronic and secondary areas of England and Wales that at an outward postcode level are recurrent with romance fraud, but across those areas the demographics of the victims vary widely. Through the pen portraits and knowledge sheets compiled for Acorn, the recommendations on reaching out to potential victims, in a manner they are more likely to interact with, could potentially be tailored by different locations. The stereotype portrayed of a romance fraud victim being a middle-aged, well-educated woman, impulsive, less kind, and more trustworthy and having an addictive disposition (Whitty, 2018) is often like that provided to law enforcement as part of the NFIB national assessment of fraud, and, based on this study, is uncontestably not the right approach. In an increasingly diverse population, police and law enforcement partners need to consider victims by more than age, gender, and ethnicity. This research explored how demographically diverse victims can be, how access to them is likely to be different, and how victim demographics vary geographically across England and Wales and through dissemination of the findings early changes in practice are already appearing, including the assignment of uniformed personnel to deliver leaflets in the types of premises identified as being popular among the most vulnerable people (first author's personal knowledge). These activities need evaluation but are an indication of the potential for tailoring preventative responses.

In the National Policing Digital Strategy, the NPCC recommends that policing in England and Wales should be utilizing big data more effectively in all areas of modern policing. The NPCC recommend police forces should be harnessing the analytical powers from their IT to do this

(National Police Chiefs Council, 2020). This research supports that recommendation and further recommends for romance fraud, exploring the utility of commercially obtained demographic big data sets to provide potentially effective opportunities to target prospective victims by location. It also provides an opportunity to understand how to target victims with bespoke crime prevention approaches (even if the underlying message is the same). This research has only explored this method with romance fraud, however, and a logical next step or recommendation is to test the same method with other fraud and cybercrime types. Other traditional crime types could also be studied to explore if the findings generalize across crime types.

Another recommendation from the findings of this research is for the NFIB, which is currently procuring a replacement recording platform to analyse fraud and cybercrime, to consider building sociodemographic datasets into the new platform to record and analyze fraud and cybercrime and consider building sociodemographic data sets into the replacement platform. This would involve longer term licensing of Acorn demographic data or a similar product from another provider not tested in this research and might eventually involve machine learning techniques that initiate tailored prevention advice at the point a victim enters their report, alerting local forces to a chronic problem expeditiously. This pathway need not be restricted to England and Wales. Agencies in the process of building fraud recording systems should consider whether the integration of demographic reference data is possible, affordable, and useful in conjunction with core records.

Finally, a policy recommendation to all law enforcement tackling romance fraud is that they should request the bespoke crime prevention advice in their localities at a low level of geography. When police forces and law enforcement partners in England and Wales are made aware of a chronic or secondary hot spot in their geographic area, they should be asking the NFIB for the detail required to make efficient and effective use of their resources to tackle the problem. Crime prevention communication outputs could then be delivered by police and law enforcement communications or media teams, local policing and safeguarding teams, victim care units, investigations teams, and any teams that encounter persons likely to suffer romance fraud. Forces should consider diversifying from the one-size-fits-all crime prevention messaging, often a media release on the force's Web site or social media, toward a model of targeted crime prevention messaging and deployment of resources to physical locations where they are most likely to interact with their target victim groups. There is also the potential for dating Web sites to engage in prevention activity tailored in the same way, using commercial intelligence to maximize efforts to prevent criminality. These sites are far better positioned than law enforcement to reach potential victims efficiently.

5.3 | Future research

This research is the first study to use a national multiyear romance fraud data set and enrich it with commercial demographic data, but it is just the first step in a broader exploration of this topic. Research at a household level would be worthwhile to test the findings of this research. At an outword postcode level, there is inevitably some generalisation of demographics so research to explore if targeting victims at a household level could provide more precision in targeting crime prevention measures. This could possibly allow for an enhanced service from the NFIB on a micro level in chronic locations and beyond just one type of fraud. Similarly, further cross-referencing of underlying demographic data of the victims alongside the segmentation data may provide additional opportunities for refining targeting.

Like all types of fraud, romance fraud remains underreported (see Button et al., 2012) and research on victims is at least partially dependent on crime reporting. There are, however, key private industry partners that could support policing with crime prevention for romance fraud. Further research could be conducted using this design and integrating data held by online dating platforms such as those in the Match Group (Match.com, Plenty of Fish, and Tinder), Bumble, and eHarmony. If the NFIB were to work with these companies, chronic and secondary outward postcodes could be compared against users on dating platforms, with bespoke crime prevention advice targeted at people registered in some way in those geographic areas. Experimental designs might reveal if such prevention is effective but although crime prevention advice is of a blanket nature, it is impossible to establish meaningful counterfactuals. It might also be possible to conduct qualitative research with a dating platform provider, engaging dating platform users to test whether bespoke crime prevention messaging, based around the method of this study, affected user's attitudes to self-protection.

5.4 | Limitations

The Action Fraud data are self-reported data, which is a clear limitation. The reporting process relies on the victim, or representative, understanding and giving the correct information to a call handler, or in most reports, inputting the correct information online at the time of reporting the crime. It also relies on the victim, or representative, being honest that a crime has occurred or that the details provided are accurate. In retrieving these data for the purpose of this research, the study was reliant on the data being tagged correctly so other fraud types were not ingested into the data set or romance fraud victims missed from it, which would affect the findings. As discussed, we believe a small proportion of records were misclassified in this way.

Action Fraud data can only account for romance fraud crimes that have been reported via Action Fraud. The Crime Survey of England and Wales suggests that crimes of all types are under reported each year (Ariel & Bland, 2019), which is an international problem and accepted as a limitation in criminological research. Because this data set represented victims across the whole of England and Wales, the findings of this research cover a national perspective, but they only represent those victims who have realized they are a victim of romance fraud and chosen to report it to Action Fraud.

The Acorn data rely on multiple sources of information in building the database and then use machine learning to generate the Acorn categories, groups, and types before allocating them to geographic segments with CACI's custom algorithm. The census data Acorn was originally built from are from 2011 and will not be updated with the 2021 census data until 2023 at the earliest. To improve the accuracy of their data, CACI uses other data sources to enrich their database, but there is a chance that the household- or postcode-level data do not equate to the romance fraud victim in question. Some of the Acorn data are created with forecasting and predictive models and estimates derived from samples and are subject to the limits of statistical errors from rounding up or down. The data also require CACI to continually maintain the data set and keep it current.

6 | CONCLUSION

This study examined a cleansed data set of 15,575 individual victims of romance fraud throughout the period of October 13, 2018 to October 12, 2021 from across England and Wales who had

reported to Action Fraud. Utilizing their outward postcode, it was found that 50% of all reported romance fraud victimizations occurred in 17% of places. Where more than three victims in a 12-month period were in the same outward postcode area, these outward postcodes were tracked during the following 2-year period. After 3 years, 162 had become chronic outward postcodes, re-occurring every year, containing 17% of all reported romance fraud victims. A further 157 became secondary outward postcodes that re-occurred in one of the following 2 years but not both, containing another 10% of all reported romance fraud victims. These hot spots of romance fraud were more frequently populated with less affluent communities.

These findings indicated that a national one-size-fits-all recommendation of crime prevention measures for romance fraud is ineffective and theoretical constructs for understanding romance fraud should account for its prevalence across populations and not just in particular segments. The NFIB could facilitate the 43 police forces and their law enforcement partners' use of victim data, enriched with demographic profiling, to understand their victims and the locations most at risk of chronic or secondary victimization, to then build bespoke crime prevention messages and outputs. Police and law enforcement partners arguably cannot rely on simply looking at victims by age, gender, and ethnicity as a national average of what a victim of crime will be. Bespoke crime prevention with detailed demographic data is more likely to identify and reach those people most at risk in a geographic area.

CONFLICT OF INTEREST

The authors confirm that they have no conflict of interest to declare.

ORCID

Matthew Bland https://orcid.org/0000-0002-7038-1879

ENDNOTES

[1] Contains Royal Mail data © Royal Mail copyright and database right 2016 ©1979–2021 CACI Limited. This report shall be used solely for academic, personal, policing, and/or noncommercial purposes.

[2] Whitty's model has seven stages, and the first four of which are (1) motivation to find the ideal partner, (2) presentation of the ideal profile, (3) grooming, and (4) the sting, and the final stages include escalation and repetition, but the fourth step is theoretically where a crime is first committed and this is where we argue prevention interventions need to be focused prior to.

REFERENCES

Ariel, B., & Bland, M. (2019). Is crime rising or falling? A comparison of police-recorded crime and victimization surveys. In M. Deflem & D. M. D. Silva (Eds.), *Methods of criminology and criminal justice research* (Vol. 24, pp. 7–31). Emerald Publishing Limited.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191–215.

Braga, A. A., Turchan, B. S., Papachristos, A. V., & Hureau, D. M. (2019). Hot spots policing and crime reduction: An update of an ongoing systematic review and meta-analysis. *Journal of Experimental Criminology*, *15*, 289–311.

Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime & Law*, *20*(3), 261–283.

Buil-Gil, D., & Zeng, Y. (2022). Meeting you was a fake: Investigating the increase in romance fraud dating during covid-19. *Journal of Financial Crime*, *29*(2), 460–475.

Bullock, K. (2018). The police use of social media: Transformation or normalisation? *Social Policy and Society*, *17*(2), 245–258.

Burns, S., & Roberts, L. (2013). Applying the theory of planned behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety*, *15*(1), 48–64.

Button, M. (2021). Hiding behind the veil of action fraud: The police response to economic crime in England and Wales and evaluating the case for regionalization or a National Economic Crime Agency. *Policing: A Journal of Policy and Practice*, *15*(3), 1758–1772.

Button, M., Lewis, C., & Tapley, J. (2012). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, *27*(1), 36–54.

Carter, E. (2021). Distort, extort, deceive and exploit: Exploring the inner workings of a romance fraud. *British Journal of Criminology*, *61*(2), 283–302.

Cross, C., & Holt, T. J. (2021). The use of military profiles in romance fraud schemes. *Victims & Offenders*, *16*(3), 385–406.

Cross, C., & Layt, R. (2022). "I suspect that the pictures are stolen": Romance fraud, identity crime, and responding to suspicions of inauthentic identities. *Social Science Computer Review*, *40*(4), 955–973.

Cross, C., Dragiewicz, M., & Richards, K. (2018). Understanding romance fraud: Insights from domestic violence research. *The British Journal of Criminology*, *58*(6), 1303–1322.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588–608.

Gillespie, A. A. (2017). The electronic Spanish prisoner: Romance frauds on the internet. *The Journal of Criminal Law*, *81*(3), 217–231.

Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS). (2021). *Spotlight report: A review of fraud: Time to choose*. https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/a-review-of-fraud-time-to-choose.pdf

Home Office. (2021). *Beating crime plan*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1015382/Crime-plan-v10.pdf

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, *30*(1), 1–25.

Hirschi, T. (1969). *Causes of delinquency*. University of California Press.

Israni, A., Erete, S., & Smith, C. L. (2017). *Snitches, trolls, and social norms: Unpacking perceptions of social media use for crime prevention. Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing(CSCW '17), Portland, OR, 25 February–1 March; pp. 1193–1209. Association for Computing Machinery*.

Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer Mediated Communication*, *14*(1), 79–100.

National Fraud Intelligence Bureau. (2021). *Assessment of the threat posed to the UK from fraud 2020/21*. City of London Police.

National Fraud Authority. (2011). National Fraud Segmentation. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118481/national-fraud-segmentation.pdf

National Police Chiefs Council. (2020). *National policing digital strategy*. https://www.apccs.police.uk/media/4886/national-policing-digital-strategy-2020-2030.pdf

Offei, M., Andoh-Baidoo, F. K., Ayaburi, E. W., & Asamoah, D. (2022). How do individuals justify and rationalize their criminal behaviors in online romance fraud? *Information Systems Frontiers*, *24*, 475–491.

Payne, B. K. (2020). Criminals work from home during pandemics too: A public health approach to respond to fraud and crimes against those 50 and above. *American Journal of Criminal Justice*, *45*(4), 563–577.

Pease, K., Ignatans, D., & Batty, L. (2018). Whatever happened to repeat victimisation? *Crime Prevention and Community Safety*, *20*(4), 256–267.

Pratt, T., Holtfreter, K., & Reisig, M. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267–296.

Rege, A. (2009). What's love got to do with it? Exploring online dating scams and identity fraud. *International Journal of Cyber Criminology*, *3*(2), 494–512.

Sherman, L. W. (2007). The power few: Experimental criminology and the reduction of harm. *Journal of Experimental Criminology*, *3*(4), 299–321.

Skidmore, M., Goldstraw-White, J., & Gill, M. (2020a). Vulnerability as a driver of the police response to fraud. *Journal of Criminological Research, Policy and Practice*, *6*(1), 49–64.

Skidmore, M., Goldstraw-White, J., & Gill, M. (2020b). Understanding the police response to fraud: The challenges in configuring a response to a low-priority crime on the rise. *Public Money & Management*, *40*(5), 369–379.

Spiegelhalter, D. (2019). *The art of statistics: Learning from data*. Penguin Random House.

Titus, R. M., & Gover, A. R. (2001). Personal fraud: The victims and the scams. In G. Farrell & K. Pease (Eds.), *Repeat victimisation: Crime prevention studies* (Vol. 12, pp. 133–151). Criminal Justice Press.

Weisburd, D., & Eck, J. E. (2004). What can police do to reduce crime, disorder, and fear? *Annals of the American Academy of Political and Social Science*, *593*(1), 42–65.

Whitty, M. T. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology*, *53*(4), 665–684.

Whitty, M. T. (2018). Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, Behavior, and Social Networking*, *21*(2), 105–109.

How to cite this article: Sinclair, R., Bland, M., & Savage, B. (2023). Dating hot spot to fraud hot spot: Targeting the social characteristics of romance fraud victims in England and Wales. *Criminology & Public Policy*, 1–21. https://doi.org/10.1111/1745-9133.12629

AUTHOR BIOGRAPHIES

Richard Sinclair is a serving police detective superintendent, Richard was responsible for research and analysis conducted by the National Fraud Intelligence Bureau, and is now Head of National Lead Force Fraud Investigation for the City of London Police. Richard is currently exploring further research on the effectiveness of varying communication methods to protect people from fraud and cybercrime victimization.

Matt Bland is an Associate Professor of Evidence Based Policing at the University of Cambridge. He was formerly a crime analyst and specializes in applied and experimental criminology across a range of topics including domestic abuse, hot spot policing and police misconduct.

Bradley Savage studied forensic linguistics at the University of Cardiff. Bradley has spent throughout a decade working in intelligence analysis and is now Head of Digital Exploitation Services at the City of London Police.