European Journal on Criminal Policy and Research (2020) 26:285–291
https://doi.org/10.1007/s10610-020-09463-2

Fraud in the Twenty-first Century

Lars Korsell[1]

Published online: 14 August 2020

Fraud is by no means a new phenomenon. In their contribution, Steven Kemp, Fernando Miró-Llinares and Asier Monevare mind us of the Sicilian corn trader who deceived a potential customer for illicit gain in ancient Greece. Since then, the Internet has created new and substantial crime opportunities. The electronic use of payment card data to commit fraud is currently the fastest growing area of fraud crime in Sweden (Brå 2016). Fraudsters are increasingly analysing data from social media to target potential fraud victims.

Another development, connected with information and communications technology, is the growingly cashless society. Some stores do not even accept cash any longer. Instead of cash, the money is circulating in an account environment with the use of payment cards and electronic transfers. The cashless society makes it more difficult for perpetrators to use traditional means to get access to money. Fraud might be the answer, but it is not as easy as merely taking money, especially not since Chip and PIN made stolen cards harder to use at scale. It is also a way of using modern technology to reach more victims.

The idea behind the title *Fraud in the Twenty-first Century* of this special issue of *The European Journal of Criminal Policy and Research* is that fraud seems to become an even more increasing crime problem as society changes from "taking" someone's item to deceive someone or a system to get access to what is valuable: money, information or access to different systems. That makes fraud the crime for the twenty-first century a crime which is enhanced and assisted by information and communications technology.

This change from traditional property crimes and a society with visible banknotes and coins is obvious in the study of crime statistics. Since 2008, the levels of fraud in Sweden have increased in terms of both self-reported exposure to fraud and the number of fraud offences dealt with by the criminal justice system (Brå 2016). A large increase has been observed in both online fraud and payment card fraud. According to the "Swedish Crime Survey 2018", 5.2% of the Swedish population have been victims of sales fraud, and 5.4% of card/credit fraud (Brå 2019). In 2019, 28% of the population (aged 16–84) stated that they were concerned about being a victim of fraud on the Internet. The proportion has increased slightly compared to 2018, when it was 25%. Seen over time, a slight increase can be discerned since 2017.

✉ Lars Korsell
lars.korsell@bra.se

[1] The Swedish National Council for Crime Prevention, Box 1386, 111 93 Stockholm, Sweden

The increase of fraud is a good reason to pay more attention to the situation and the development. This special issue of journal contains six articles dealing with the problem of fraud in different aspects:

- Property crime drops and the rise of fraud (Kemp et al. 2020))
- A national fraud strategy and its problematic translation to the local level (Levi and Doig 2020)
- Online fraud analysis (Rossy and Ribaux 2020)
- The financial management of counterfeit goods fraud (Antonopoulos et al. 2020)
- Document fraud (Baechler 2020)
- Cyberscam victims (Whitty 2020)

This Special Issue

The Property Crime Drops and the Rise of Fraud

In their contribution, *The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain*, Kemp et al. (2020) discuss the development of fraud and cyber fraud according to police statistics. Different researchers have studied police statistics and identified a property crime drop in Western societies, but fraud or cyber fraud has not been considered in the analysis. One explanation is that fraud is an extremely wide-ranging issue and definitional difficulties can obstruct recording. Victims also tend not to report fraud to the police because of the insignificance of the event, the complexity of the reporting process and a lack of confidence in police ability to respond adequately. However, a broad definition of property crime includes fraud, and the authors argue that it seems useful to consider fraud in the property crime drop analysis.

Fraud appears to be rising fast, if one includes police fraud statistics and bank card fraud data from the Bank of Spain in the crime rate analysis. Their conclusion is that it is hard to maintain that there has been a property crime drop, if fraud is included. Instead, it appears that there may have been a property crime rise in recent years in Spain. Fraud has been one of, if not, the most prevalent property crimes in the cybercrime era.

Improved crime data will enable criminal justice institutions and other public institutions involved in crime control to better allocate resources and formulate strategies and policy. An interesting observation is the changing role of the police. Instead of being the main actor in prevention, the role of the police is reduced. The future is new multi-agency cybercrime policing, and the authors also suggest that organisations involved in ICT design and supply should produce and use products that reduce crime opportunities.

A National Fraud Strategy on the Local Level

In their contribution, Levi and Doig (2020) explain that fraud is not naturally regarded as a major social problem because, historically, it has not been associated with the "dangerous classes" and does not require a violent takeover of others' property or person. Fraud has never been a high policing priority.

As mentioned in the earlier article, there is also another side of the coin, the changing role of the police and the criminal justice system in the Internet era. The role of the police is

reduced and there is a need for a wider focus to tackle fraud with more actors who can prevent, raise awareness, audit, detect and carry out other anti-fraud measures. Crime control in general is influenced by policies and strategies which include several agencies and partnership.

With this in mind, it is interesting that the UK has adopted a fraud strategy, which Levi and Doig had examined on the local level in their article: *Exploring the 'Shadows' in the Implementation Processes for National Anti-fraud Strategies at the Local Level: Aims, Ownership, and Impact* (Levi and Doig 2020).

In the UK, the risks of fraud were highlighted during the early twenty-first century and a national policy response was required. Fraud was not treated as only a police matter. The focus was much broader, and especially auditing and information-sharing for fraud prevention became an important tool. The UK anti-fraud approach started with good intentions. A national strategy was launched in 2008 and was led by the National Fraud Authority. In 2011, the "Fighting Fraud Together" strategy was presented and it encompassed both the public and private sectors' response to fraud.

But soon, it became hard to count the number of anti-fraud governmental initiatives and organisational changes. Authorities and commissions were abolished, responsibilities were diffused and there were no means to review and revise the strategy using real knowledge of how it was operating around the country. It therefore remains hypothetical what effects the strategy has had, or would have had, on actual levels of fraud. The authors' conclusion is that "strategies have to be evolving or adaptable rather than purely deliberate and top-down, and that the strategic implementation process needs to be 'owned' by a body with the authority or the means to ensure appropriate guidance, resources, and support, as well as feedback to review and adapt the strategy to changing circumstances". This requires much central government consistent focus, policy alignment and a willingness to reach out to distant parts of the country: lessons that apply everywhere.

Online Fraud Analysis

A study based on online crime cases registered by one cantonal police force in Switzerland shows that 85% were frauds. Nearly half were e-commerce frauds related to fake sellers or buyers of diverse goods. The increasing online shopping and use of online banking systems create opportunities for online fraud. Internet dating sites are a playground for fraud. Sites and e-mails contain false qualities, identities and made-up stories. Rossy and Ribaux (2020) conclude that "opportunities for developing innovative frauds have dramatically increased due to digitalisation". In their contribution, *Orienting the Development of Crime Analysis Processes in Police Organisations Covering the Digital Transformations of Fraud Mechanisms*, the authors argue that the police need to develop new approaches to face the rising problem of online fraud, to be a credible interlocutor when interacting with the public and other professional stakeholders.

One way for the police to take a further step is an integrative project presented in the article. Six police services in Switzerland are involved in the project with a forensic intelligence approach. The project consists of two elements. The first element is an operational crime script analysis with 5 steps: (1) search and contact potential "marks" (victims), (2) reinforce the credibility of the scenario and establish trust, (3) trigger delivery of the asset, (4) distance yourself from the mark, and (5) make use of the asset. The second element is to detect links between cases: the perpetrators' use of banks (IBAN), pseudonyms, email and Internet Protocol addresses, phone numbers and websites.

The article describes different aspects of frauds — following the 5 steps in the script analysis — in the category of "confidence game", which were chosen because they possess a

certain degree of genericity and served as a building block in the perspective of constructing a more ambitious framework. The term "confidence game" was coined based on an event in 1849 in New York. The con man's modus operandi was to convince a chosen person in the street that he was an old acquaintance and to borrow his watch until tomorrow. The purpose with the project is that understanding of the fraud schemes allows the detection of weaknesses in the modi operandi, which give opportunities to use preventive initiatives or law enforcement tools.

The Financial Management of Counterfeit Fraud

Counterfeit goods fraud — from fashion items, watches and jewellery to medicines, electrical equipment and aeroplane parts — has become an important part of world economy. In their contribution, *Counterfeit goods fraud: an account of its financial management*, Antonopoulos et al. (2020) refer to almost unbelievable figures: The trade of counterfeit goods costs the global economy an estimated $1.77 trillion in 2015, which is nearly 10% of the global trade in merchandise. The authors have concentrated their article not on the counterfeit market as such but on the financial mechanisms that enable the trade.

As with fraud, information and communications technologies play an increasingly significant role. Internet service providers, registrars, payment processors and payment gateways are integral nodes of the infrastructure needed to trade in counterfeit products online. Apart from allowing the electronic transfer of money, information and communications technologies have transformed the retail activity of traders, coupled with a remarkable increase in the number of small parcels. Entrepreneurs with a legal business can integrate their counterfeiting proceeds with financial streams in the legal business.

Counterfeiting is embedded in legal production and trade practices in a globalised economy. There are numerous convergence points between legal and illegal supply chains, and occasionally, there is a symbiotic relationship between the legal and counterfeit products supply chains. "In a sense, in the counterfeiting business what one can observe is the infiltration of the illegal business by the legal business, rather than the other way around". As in other illicit markets, "brokers" work as facilitators. Normal commercial channels are used as postage services, transportation, shipping and delivery companies.

Start-up money for counterfeiting schemes comes from legitimate work, savings and social security benefits. Schemes are also funded with money from legal business as logistics companies or legitimate companies trading in the same commodity that is counterfeited. At the wholesale level, credit is more common. Criminal entrepreneurs engaging in other illegal activities could invest in counterfeiting ventures.

Profits from the counterfeiting business are often spent on lifestyle consumption, including luxuries. Family-oriented entrepreneurs have a more long-term strategy and pay off debts and mortgages, buy or renovate houses and other properties.

Antonopoulos et al. (2020) conclude that the financial management practices in the counterfeit products trade are generally unsophisticated because it is fragmented, decentralised and competitive, and crime-money is widely distributed rather than gathered in the hands of a few big players.

Document Fraud

Criminals began to use counterfeit and forged official identity and travel documents in the late Middle Ages. Today, according to Europol, document fraud has been one of the major cross-cutting engines of an organised crime — a crime enabler — ranging from financial scams and

trafficking in human beings to terrorism. The production and use of fraudulent identity and travel documents lies at the crossroads of identity fraud and document fraud. Simon Baechler (2020) asked a question in the title to his contribution: *Document Fraud: Will Your Identity Be Secure in the Twenty-first Century?*

Deviants and criminals have understood that the use of fraudulent documents could open up numerous advantages such as maintaining their anonymity and easily moving across borders. Simon Baechler's intention is to raise awareness amongst researchers, professionals and policy makers as to which responses may be devised to efficiently impact on this kind of fraud, and to inform about challenges and relevant avenues for the future.

Document traffickers have taken advantage of the licit and illicit trade environments offered by the web space and online markets to sell their products and promote their crime-as-a-service. Driving licences are the most frequent type of fraudulent document encountered on online markets. Passports come second and identity cards third. The median price for fraudulent driving licences is 250 USD; for identity cards, 150 USD; and for passports, 1200 USD. Fraudulent documents ordered over the Internet can be delivered by mail, airmail and fast parcel companies between 1 day and 6 weeks later, depending on the platform.

Fraudulent documents often bear a specific "signature" of its forger. The forgers have their own specific set of knowledge and techniques. They use certain papers or printers. Taken together, this information describes a specific forger's profile. By this forensic profiling, it is possible to uncover forgers and their network. The method represents a shift from the traditional case-by-case approach to an intelligence-led police work.

Back to Simon Baechler's question: "Will your identity be secure in the 21st Century?" The answer is that he sees four main challenges.

1. A need for collaboration between criminology and forensic science researchers, law enforcement and the security document industry. A pure technological race to make more secure documents and better control technologies "serves the security document industry rather than the actual fight against crime".
2. Implementing intelligence-led policing in the fight against document fraud, which should include forensic experts and use their full potential. Not only to examine documents but also to be an active part in the police work in order to understand crime and provide security.
3. Better education and training in the authentication of documents. The police, border control, bank clerks, shop assistants and others need to improve their awareness of fraudulent documents and their detection capabilities.
4. The digital transformation poses new threats, such as morphs or the sale of fraudulent documents over the Internet. There is a need to harmonise documents in order to prevent frauds. This is not easy in Europe with so many countries and standards. Till when, the aim is to combine the best human expertise with that of machines and artificial intelligence.

Cyberscam Victims

Even if scams have a long history, as a consequence of the Internet, fraudsters can easily access many more potential victims, and "we are witnessing an explosion of this type of crime". By studying victimology of cyberscams — consumer, charity, investment and

romance scams — it will be possible to develop more effective measures to protect citizens from such crime. For her article, *Is There a Scam for Everyone? Psychologically Profiling Cyberscam Victims*, Whitty (2020) used an online questionnaire (10,723 non-victims and 1057 victims). The participants were asked if they had been scammed that involved the Internet in some way. Are there any psychological and socio-demographic differences between victims of different types of cyberscams?

Age: Investment scam victims were older than romance and charity scam victims, and consumer scam victims were older than romance and charity scam victims; *Gender*: Women were much more likely to be a victim of a consumer scam and men were more likely to be a victim of an investment scam. In general, men were more likely to be scammed than women; *Education*: Consumer scam victims were less educated than romance and charity scam victims. In general, educated people were more likely to be scammed than less educated people; *Locus of control*: Investment scam victims scored significantly higher on internal locus of control compared with romance, charity and consumer scam victims. Victims were more likely than non-victims to believe that they had control over the outcomes of events in their lives; *Emotional stability*: Scam victims are more likely to be emotionally unstable compared with non-victims.

The study shows that here are differences between cyberscam victims. Therefore, a preventive "one size fits all model" has its limitations. Preventive training programmes need to be better directed to different groups of possible victims.

Lessons Learned from This Special Issue

The contributions have shone a light on different dimensions of the fraud problem. The common conclusions are that fraud is increasing, especially on the Internet and that the response from the police and other stakeholders are not impressive. Why has the fraud problem been so neglected, and still not received the necessary attention?

I think there are two explanatory factors. The first has to do with the core element in fraud, deception: to mislead someone or a system. Deception can be done in many ways and is rather abstract and vague, not as clear-cut as theft or violence. The second factor is the amplitude of the crime: consumer, tax, long-firm, investment, cyber, financial, benefit, romance fraud as well as fraud against elderly and fraud in connection with bankruptcy, to that can be added the fraud element in white-collar crime, organised crime and financing of terrorism.

It seems that the future will see different ways of tackling fraud: The role of the police will change and more actors will step forward to prevent fraud in a wide range of measures. There is also a need for better statistics, more knowledge and preventive measures to deal better with the crime of the twenty-first century.

References

Antonopoulos, G. A., Hall, A., Large, J., & Shen, A. (2020). Counterfeit goods fraud: an account of its financial management. *European Journal on Criminal Policy and Research, 26*(3).

Baechler, S. (2020). Document fraud: will your identity be secure in the twenty-first century? *European Journal on Criminal Policy and Research, 26*(3).

Brå. (2016). *Fraud in Sweden*. Stockholm: The Swedish National Council for Crime Prevention.

Brå. (2019). *Swedish crime survey 2019*. The Swedish National Council for Crime Prevention.

Kemp, S., Miró-Llinares, F., & Monevare, A. (2020). The dark figure and the cyber fraud rise in Europe: evidence from Spain. *European Journal on Criminal Policy and Research, 26*(3).

Levi, M., & Doig, A. (2020). Exploring the 'shadows' in the implementation processes for national anti-fraud strategies at the local level: aims, ownership, and impact. *European Journal on Criminal Policy and Research, 26*(3).

Rossy, Q., & Ribaux, O. (2020). Orienting the development of crime analysis processes in police organisations covering the digital transformations of fraud mechanisms. *European Journal on Criminal Policy and Research, 26*(3).

Whitty, M. T. (2020). Is there a scam for everyone? Psychologically profiling cyberscam victims. *European Journal on Criminal Policy and Research, 26*(3).