Tackling Online Fraud

Prof Alisdair A. Gillespie and Samantha Magor*

Online fraud continues to be one of the most challenging forms of cybercrime. It is an extremely varied species of crime, with multiple examples and definitions. The prevalence of online fraud is so vast that law enforcement and financial bodies can quickly become swamped. The EU recognises the threat that online fraud poses to the Union and has passed a new Directive that seeks to tackle online fraud. However, the Directive misses many forms of online fraud, potentially leaving citizens of Europe vulnerable to online fraud.

Keywords

CYBERCRIME – FRAUD – VICTIMS – SCAMS – EU LAW – FINANCIAL CRIME

Fraud is one of the oldest and most common forms of cybercrime.[1] Of course, fraud has existed long before the internet came into existence, and it is a classic example of what Barry Sandwell has described as a crime that is generalised and radicalised by the internet.[2] That is to say, it is a crime that has been changed by the internet in that it has been allowed to grow exponentially as a result of the internet's infrastructure. This article will consider the common forms of cybercrime, and identify how the law and law enforcement has responded to this.

1. Defining Internet Fraud

There is no single definition of internet fraud and, as will be seen later, this causes difficulties for the law. Perhaps the most comprehensive definition is a typology put forward by Amber Stabek and others.[3] Seven categories are identified:

1. **Fraud through low-level trickery**. This could include, for example, advertising non-existent products.

* Professor of Criminal Law and Justice and Research Assistant respectively, both at Lancaster University. Corresponding author is Prof Alisdair Gillespie, Lancaster University Law School, Lancaster, UK (a.gillespie@lancaster.ac.uk).

[1] *Gillespie* [12], p.155.

[2] *Sandwell* [18], p.46.

[3] *Stabek* [19], pp.44-45.

2. **Fraud through developed story-based application.** This where a person is tricked into giving money as part of a story. It is often used in advance-fee scams (discussed below).

3. **Participation through employment-based strategies.** This is where a person is tricked into paying money in anticipation of gaining employment (e.g. for a necessary qualification, a vetting fee or a uniform etc).

4. **Fraud through implied necessary obligation.** This is where money is taken fraudulently when a person does a positive act (e.g. subscribing to a site or telephoning a particular number), often without realising the full consequences.

5. **Information gathering through apparently authentic appeals.** This could be where, for example, a person sets up a fake charity or crowd-funding page for a fictitious problem (e.g. a non-existent child who requires expensive medical treatment).

6. **Financial gain through merchant and customer-based exploitation.** This can include most auction frauds or where a person pretends not to have received goods.

7. **Financial gain through marketing opportunities.** So-called 'Ponzi' schemes would be classic examples of this, or get-rich-quick schemes.

Missing from this list is technology-derived frauds. This would include, for example, 'formjacking' (where malicious code is used to steal credit card information inserted into legitimate sites), 'pharming' (where a person trying to access a legitimate site is directed towards an illegitimate site) or 'ransomware' (where a computer, storage device or cloud store is encrypted so that the user cannot access their data, with the encryption only being lifted when a ransom is paid). However, are these truly frauds or are they another branch of financial crime?

The term 'fraud' tends to conjure up the idea of a scam. That is to say, a swindle or trick. The seven examples discussed above could be considered scams: they involve person A tricking person B. Technology is simply the facilitator. Formjacking, pharming and ransomware are more akin to a computer attack than a scam. They have more in common with hacking and malware than the law of theft, but instead of causing damage to a system they are designed to lead to financial loss. Of course, the distinction is not perfect. Let us take two examples:

A, using malware, directs B to a false site when B tries to buy something on an e-commerce site. This allows A to steal B's credit card details.

C pretends to be a legitimate e-commerce shop. D enters his credit card details to buy something. C does not send the items, and uses D's credit card details to buy other things.

The second example would be a form of category 6 – customer and merchant exploitation – whereas the first example does not fit within the taxonomy. However, although the result is the same – the second party obtains credit card details inappropriately – the method is very different. This paper will consider online fraud to encompass scams rather than technological attacks, which are best thought of as computer misuse. Under this definition, internet fraud is best thought of as a 'computer assisted' rather than 'computer orientated' crime.[4]

1.1 Common forms

It is not possible to consider all forms of fraud in this piece, and reference should be made elsewhere.[5] Instead, brief mention will be made of some of the more common types of online fraud. Arguably the most common[6] are commerce frauds, confidence frauds, advance fee frauds and overpayment.

1.1.1 Commerce frauds

The most common online fraud according to most state statistics is commerce fraud. This includes a number of sub-species, including non-payment, non-delivery and auction frauds. That commerce frauds is one of the most common should not be surprising given the growth in e-commerce. It is easy to hide behind the appearance of respectability on the internet. An e-shop looks credible, whereas the same trader may not look as respectable in real life. Similarly, a picture of a legitimate product can be displayed on the internet, while a replica is despatched. A replica in a physical shop is easier to detect.

There are numerous examples of commerce frauds, and online auctions provide considerable opportunities to commit fraud. They also provide the opportunity for other financial crime, including the 'fencing' (selling) of stolen goods.[7] Aside from non-payment/non-delivery, which has been touched on already, a common form of auction fraud is so-called 'shill bidding'. This is where a person establishes a fake profile and bids upon a popular item, never intending that they

---

[4] *Wall* [23].
[5] For example, see *Gillespie* [12], ch. 6 or *Yar* [28], ch.6.
[6] *FBI* [11], p.19.
[7] *Aniello* [1], p.42.

would win.[8] This pushes up the price. If the fake bidder does accidentally win, the person who came second will be told that the winner has pulled out, and they can buy the item for their previous highest bid. If the fake bidder does not win, then the winner has paid more than they needed to. Either-way, therefore, the price could be falsely inflated.

Of course, the interesting argument with shill bidding is the extent to which a fraud has happened. Nobody is forcing the (eventual) winner to pay above what she or he wishes to. If they did not want to pay a particular price then they could choose not to. Yes, the price is higher because of a phantom bid, but ultimately the person continues to pay a price that they are prepared to pay.

1.1.2 Confidence frauds

Confidence frauds are one of the older forms of internet fraud and arguably one of the nastier ones. The name is given because the fraud is based on the perpetrator obtaining the confidence of the victim in order to carry out the scam. This could include, for example, a fake business relationship where a person believes that they are investing in a legitimate opportunity. They can be shown real estate and detailed plans, but when they invest, it turns out that the opportunity was never present.[9]

Perhaps one of the more common forms of confidence frauds that has emerged in recent years, is 'romance fraud'. This is where a person is led to believe that they are in a romantic relationship with a person, and yet the object of the romance is to cause financial loss to the victim.[10] There are numerous versions of the romance fraud.[11] Some are purely online. The perpetrator and victim meet in an online dating site and communicate exclusively by technology. In other situations, there may be real-world contact. While the scam will originate online, the perpetrator and victim will meet, often having romantic meals and even sexual intercourse, to make the victim believe that they are in a true relationship.

When the romance is formed, there will then be an 'event' that requires money to be spent. This could, for example, involve the scammer travelling to another country where they are allegedly injured or arrested, requiring the victim to pay money, either out of love, or because they think

[8] *Synder* [20], p.457.
[9] *Kieffer* [15].
[10] *Whitty* [25], p.181.
[11] *Whitty* [24].

they will be repaid by their 'lover'.[12] It is not difficult to fake medical certificates, pictures of hospitals or a convincing website for a legal firm that does not exist. Other frauds will exploit the victim's desire to start a life with their supposed lover. The perpetrator will claim to have a house that can be sold to provide funds for them to then jointly-purchase a house somewhere else. The house requires improvements, but because their capital is tied up in the house, they need the victim to pay for the improvements, with them getting the money as equity in the new house. When the money is paid, it is apparent that there is no house.

As will be seen later, the consequences of confidence fraud are often significant. It is not just the financial loss that the victim faces, but often feelings of betrayal as a result of the breach of personal trust inherent within a confidence fraud, or the feelings that one has somehow lost a loved one.[13]

1.1.3 Advance fee frauds

Advance fee fraud continues to be one of the more popular forms of internet fraud. It is also a type of fraud that everyone with an email address will have probably seen, although not necessarily fallen for. Advance fee frauds are often called 419 frauds after the provision of the Nigerian Criminal Code that was enacted to tackle these frauds.

The basic 419 fraud is the 'Nigerian Prince' or 'lost-long relative'. The email purports to be from a Nigerian prince who requires assistance to move vast sums of money out of the country due to corruption. In return for allowing access to their bank account, the victim is told they will receive a percentage of the proceeds (or be allowed to keep the interest earned from the sums of money in the account).[14]

Another example is prize draws. A person is told that they have been pre-selected for a (usually variable) prize, that requires them to enter a contest. Keen to claim the prize, the victim does not question the fact that they have not entered any contest. The other typical example is when a person is told that they are the last-surviving relative of a distant cousin, who died without a will. The 'sole beneficiary' needs to pay fees to unlock the inheritance, something that turns out to be false.

---

[12] *Buchanan* [2], p.261.
[13] *Buchanan* [2], p.279.
[14] *Holt* [13], p.137.

Advance fee scams divide opinion. They normally rely on the greed of the victims, who are often agreeing to do something that is certainly morally ambiguous and, in some instances, would be legally wrong (e.g. facilitating the circumvention of money laundering or currency export rules). 491 scams are often poorly worded,[15] causing many to believe that the victims have been silly to fall for such scams. As will be seen, victim-blaming is something that is unfortunately found throughout online fraud.

1.1.4 Overpayment

Overpayment is another form of commerce fraud. A person will purchase something valuable online. They will normally arrange to collect it in person, sending a representative. When the representative comes they will bring a cheque (or bankers draft etc) for a higher amount than the purchase price. As they are only a representative, they cannot write another cheque. They have travelled some distance and so they cannot return. A compromise is reached whereby the buyer will hand over the cheque/bankers draft, and the seller will provide a post-dated cheque for the difference. In fact, post-dated cheques do not exist, and can be honoured by banks. Thus the seller loses the item and the additional money because the buyer's cheque/bankers draft is false.[16]

The same trick can be used with electronic payment systems. The buyer's representative turns up with email proof that funds have been credited to, for example, PayPal. However, the sum is too much and thus the seller will either transfer money or give cash/cheque for the difference. The buyer will claim to be in a hurry, leading the seller not to check their account balances and to take the email at face value.

2. PREVALENCE OF ONLINE FRAUD

Identifying the prevalence of fraud is extremely challenging. It is known that online fraud is chronically under-reported.[17] There are a number of reasons why this is the case, including the belief that it is complicated, a belief that the amount is trivial, not appreciating that they are victims of fraud,[18] or, in some instances, embarrassment at being a victim.[19] This means that simply relying on police reports is too simplistic.

---

[15] *Holt* [13], p.149.
[16] *Gillespie* [12], p.159.
[17] *Cross* [6], p.1.
[18] *Cross* [7], p.1.
[19] *Whitty* [26].

Another difficulty in identifying the prevalence of online fraud is that there is no common definitions of what constitutes online fraud. This means that countries and organisations are counting the same behaviour in different ways. The EU has recognised this, at least, and its new Directive[20] requires Member States to collect statistics relating to fraud.[21] The European Commission will identify what statistics are required, and how they are to be gathered. This should improve an understanding of reporting, although, as will be seen, the Directive does not encompass all forms of online fraud.

The European Central Bank has estimated that card fraud across the Single Euro Payments Area in 2016 amounted to €1.8bn, with c.17.3m individual instances of fraud being used.[22] The absence of central statistics mean that individual statistics need to be considered, but these can be illustrative. In England & Wales,[23] official statistics suggest that 4.7 million incidents of fraud were experienced in the year to September 2017,[24] a decrease from pervious years. UK Finance, the industry body that represents banks and financial institutions, states that £566m was stolen from card-based fraud in 2017.[25] That only related to frauds connected to debit or credit cards. An additional £121.4m was stolen through online banking,[26] and a further £28.4m through telephone-based fraud.[27] In addition, £236m was stolen through so-called 'authorised push payments'.[28] These are frauds where a person is tricked into sending money to someone who they believe is in a position of responsibility (e.g. a person posing as a bank, or a police officer or a government department. These statistics show that almost £1bn was stolen in 2017 through online fraud. Yet even this is not the full picture. It does not include more personal fraud such as advance fee scams, romance frauds or other types of fraud that are based on personal contact rather than, for example, a stolen or skimmed debit or credit card.

---

[20] Directive 2019/713 on combating fraud and counterfeiting of non-cash means of payment.
[21] Article 18.
[22] *ECB* [10], p.7.
[23] The United Kingdom is constituted of four countries, with three different legal systems (England and Wales; Scotland and Northern Ireland). Crimes are recorded separately in each jurisdiction.
[24] *Overview of fraud and computer misuse statistics for England and Wales* (ONS, 2018). Available online at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudandcomputermisusestatisticsforenglandandwales/2018-01-25 (accessed June 2019).
[25] *UK Finance* [21], p.13.
[26] *UK Finance* [21], p.29.
[27] *UK Finance* [21], p.31.
[28] *UK Finance* [21], p.33.

The potential scale of online fraud is vast. However, large figures can sometimes be misrepresented. While clearly online fraud has led to large numbers of people losing (collectively) large sums of money, the prevalence needs to be put into context. For example, the 17.3m of card fraud detected by the ECB needs to be put into the context of the total number of card transactions across SEPA being 74.9bn.[29] That would mean that only c.0.2% of card transactions were fraudulent. The same is true in the USA where card fraud constitutes less than 0.1% of all card transactions, with welfare fraud, tax fraud and tax evasion costing society far more.[30] It is not just card frauds. The FBI's *Internet Crime Complaint Centre* (known as IC3) has estimated that in the USA, non-delivery frauds amount to over $183m.[31] However, it has been estimated that only 0.6% of items on eBay, probably the biggest delivery platform, are deliberately not delivered.[32] In other words, while online fraud involves large numbers of victims, and vast sums of money, its actual prevalence is relatively low, when set in the context of daily global e-commerce.

3. VICTIMS OF INTERNET FRAUD

Who are the victims of internet fraud? As noted above, although the number of victims is relatively high, the actual percentage of people who are victims is relatively small.

In recent years there has been discussion about whether there is a way of predicting which people are likely to be the victims of internet fraud. Perhaps unsurprisingly, it was noted that those who spend a lot of time on the internet and routinely use e-commerce are more likely to be victims.[33] It would be naïve to suggest that everyone who uses the internet is a potential victim, but perhaps Pratt et al's observation is more to do with the fact that those who are internet-savvy may be more likely to explore lots of sites to find 'the best price', meaning they may stumble across fraudulent sites that those who only use mainstream commercial sites would not. Van Wilsem believes that victimisation is more common where one's online presence is more visible through, for example, extensive use of social networking.[34]

---

[29] *ECB* [10], p.7.
[30] *Dean* [9].
[31] *FBI* [11], p.20.
[32] *Yar* [28].
[33] *Pratt* [16], p.267.
[34] V*an Wilsem* [22], p.170.

It has also been suggested that certain types of people are more susceptible to fraud. Many scams, for instance, are designed to make people believe that they have an offer that is just for them,[35] which attracts those who are always looking out for 'a bargain'. Other research has suggested that people who are impulsive and those who lack self-control are more likely to be the subject of a fraud, as are those who suffer from addictive dispositions.[36] Perhaps unsurprising is the conclusion that those who are gullible are more likely to be victims.[37]

3.1 Effect on victims

How victims feel will differ between persons and frauds. For some victims the effect will be minimal. Indeed, with some forms of commerce fraud it is quite possible that where the fraud is a small amount of money, the person may well just put the matter down to a 'bad experience' and not consider themselves defrauded. Where the scam involves larger sums of money then the financial loss to the victim can be significant. More than this, however, there is some evidence that victims blame themselves for not seeing the scam.[38] This blame can lead to victims choosing not to report fraud through embarrassment.

Of more concern, however, is the fact that victims of internet fraud are often blamed by others for falling for the scams.[39] This is not something that would happen in other forms of crime. A person who has £500 stolen from them would not ordinarily be blamed, yet someone who has £500 taken from them in a fraud is. A common complaint is that victims are greedy.[40] The argument goes that they are responsible for their own predicament because they tried to go for the 'easy win'. Such comments are not infrequently targeted against those who fall victim to 419 scams or advance fee frauds. The belief is that a person should know better when chasing something too good to be true.

There is also a belief that some victims should be able to see through the fraud.[41] Such a reaction is contradicted by the points above that many scams involve clever psychology. This belief that they will be blamed, however, can be very powerful and ensure that a person will perhaps not

[35] *Button* [3], p.403.
[36] *Whitty* [27].
[37] *Whitty* [27], p.106.
[38] *Cross* [7], p.5.
[39] See, for example, *Cross* [8].
[40] *Cross* [8], p.191.
[41] *Cross* [8], p. 193.

disclose that they have been the victim of a fraud.[42] Victim blaming is more common in confidence frauds, where there is a greater danger that victims will be affected emotionally by what has happened, due to the feelings of betrayal.[43] Family members of confidence frauds also often react badly, believing that their inheritance or support has been compromised.[44] The consequences of this can be severe, causing some victims to feel that the loss of money is the least important effect.[45]

4. CRIMINALISING ONLINE FRAUD

How then should online fraud be tackled? While prevention is important, it ultimately requires the establishment of criminal laws. The global nature of online fraud means that it is important that there is international consensus on how fraud is defined, and how it will be tackled.

4.1 Cybercrime Convention

Perhaps the first international instrument of note is the *Council of Europe Convention on Cybercrime*.[46] This was the first regional instrument that specifically tackled cybercrime, and from the beginning it was intended that online fraud would be covered by the instrument. Article 8 of the Convention requires member states to adopt legislative or other measures to prevent the loss of property by:

> (a) any input, alteration, deletion or suppression of computer data, [or]
> (b) any interference with the functioning of a computer system.

The emphasis is on interference with data or the functioning of a computer system. This means that not all forms of online fraud will fall into this definition. The Cybercrime Convention Committee has stated that in their opinion phishing and identity fraud may also be within the scope of the Convention,[47] although in most instances that is not through Article 8 but by reference to the other provisions within the instrument, including hacking.[48]

---

[42] *Cross* [8], p.198.
[43] *Buchanan* [2], p.279.
[44] *Gillespie* [12], p.162.
[45] *Rege* [17], p.494.
[46] ETS No 185. Budapest 23.xi.2001.
[47] 'T-CY Guidance Note #4: Identity theft and phishing in relation to fraud' T-CY (2013)8E Rev.
[48] Ibid., 4-5.

4.2 EU Legislation

The EU has recognised the importance of online fraud for some time. Its earliest intervention was the *Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment.*[49] Article 3 of the Decision required states to criminalise intentionally 'performing or causing a transfer of money or monetary value and thereby causing an unauthorised property for another person, with the intention of procuring an unauthorised economic benefit for the person committing the offence'. However, as with the Cybercrime Convention, this was to occur by:

(a) without right introducing, altering, deleting or suppressing data, in particular identification data, or
(b) without right interfering with the functioning of a computer programme or system.

The express inclusion of identity data was welcome as it would include those situations where a person uses a stolen credit card to make online purchases. However, the requirement that data or a system was altered meant that traditional scams would not be covered by the legislation.

The Framework Decision was starting to show its age and in 2017 the European Parliament sought to update it. Ultimately, in 2019, the *Directive on combating fraud and counterfeiting of non-cash means of payment* was passed,[50] replacing the Framework Decision. The recital specifically makes reference to the need to update the law 'in particular with regard to computer-related fraud'.[51]

The Directive requires participating member states[52] to establish 'minimum rules concerning the definition of criminal offences and sanctions in the areas of fraud and counterfeiting'.[53] Note, in common with other Directives relating to the criminal law, the Directive sets out a minimum standard, and it is open to states to set a higher standard. Six categories of offences are to be created:

Art. 3. Fraudulent use of non-cash payment instruments.
Art. 4. Fraudulent use of corporeal non-cash payment instruments.
Art. 5. Fraudulent use of non-corporeal non-cash payment instruments.

---

[49] 2001/413/JHA. OJ L 149, 02.06.2001.
[50] Directive (EU) 2019/713. OJ L 123/18. 10.5.2019.
[51] Recital (3).
[52] The United Kingdom, Ireland and Denmark are not bound by the Directive under the terms of Articles 1 and 2 of Protocol 21 of the TEU and TFEU (see recital (38) and (39) OJ L 123/23).
[53] Article 1 of Directive 2019/713.

Art. 6. Fraud related to information systems.

Art. 7. Tools used for committing offences.

Art. 8. Inciting, aiding and abetting and attempt.

While Article 2(a) defines 'non-cash payment instrument' it does not do so in a particularly user-friendly way. Perhaps a better definition is provided by the *European Central Bank*, who give the examples of cards, credit transfers, direct debits and e-money.[54] The directive draws a distinction between corporeal (meaning, in this context, physical) and non-corporeal forms. Corporeal forms would therefore be such things as credit cards, debit cards, traveller cheques etc. Non-corporeal forms would be direct debits, standing orders and money transfers.

Article 3 requires the following conduct to be criminalised:

(a) the fraudulent use of a stolen or otherwise unlawfully appropriated or obtained non-cash payment instrument;
(b) the fraudulent use of a counterfeit or falsified non-cash payment instrument.

This, therefore, would require countries to ensure that the use of stolen credit or debit cards, vouchers etc. is criminalised. This is unlikely to be problematic, and the vast majority of countries will already do this.

Article 4 relates to the fraudulent use of corporeal (physical) non-cash payments and requires the following conduct to be criminalised:

(a) their theft or other unlawful appropriation;
(b) the fraudulent counterfeiting or falsification of an instrument;
(c) the possession of a stolen or otherwise unlawfully appropriated, or a counterfeit or falsified instrument for fraudulent use;
(d) the procurement for oneself or another, including the receipt, appropriation, purchase, transfer, import, export, sale, transport or distribution of a stolen, counterfeit or falsified instrument for personal use.

[54] https://www.ecb.europa.eu/paym/pol/activ/instr/html/index.en.html (Accessed 20.6.19).

Where Article 3 relates to the use of the instruments, Article 4 largely prohibits their production or acquisition. Thus, the person who steals a payment instrument (e.g. a card) or counterfeits it would be within this offence. 'Counterfeits' includes those situations where a card is cloned through, for example, placing a 'skimmer' in the card slot of an ATM. The offence could also be used for online fraud. The wording of Article 4(b) includes the falsification of an instrument, and thus could include those who procure the details of credit cards etc. through hacking or other techniques. The card details constitute a corporeal non-cash payment instrument and remain so even though the card is not physically present. This broadens the scope of the offence.

Article 4(c) criminalises those who possess an instrument, but only where it is to be used for a fraudulent purpose. Again, reference to 'falsified' instrument would capture those who are in possession of a cloned card or card details that have been procured online. The falsification would be that (a) the user has the right to use it, and (b) that the card is physically present when it is not.

Article 4(d) requires all conduct related to the transfer or trading of instruments to be criminalised, so long as it is for the purpose of fraud. From the wording of the paragraph it is clear that it does not matter whether the seller intends to commit the fraud, it is sufficient that she is aware that someone else will use the instrument for fraudulent purposes.

Article 5 then establishes similar offences for non-corporeal instruments. The following conduct is to be criminalised:

(a) the unlawful obtainment of a non-corporeal non-cash payment instrument, at least when this obtainment involves the commission of one of the offences referred to in articles 3 to 6 of Directive 2013/40/EU, or misappropriation of a non-corporeal non-cash payment instrument;
(b) the fraudulent counterfeiting or falsification of an instrument;
(c) the holding of an unlawfully obtained, counterfeit or falsified instrument for fraudulent use, at least if the unlawful origin is known at the time of the holding of the instrument;
(d) the procurement for oneself or another, including the sale, transfer or distribution, or the making available of an instrument for fraudulent use.

Article 5 is more complicated, partly because of the nature of the instruments. However, it is establishing broadly similar offences to Article 4. Paragraph (a) is interesting because it, in essence, has two alternatives. Member States can choose to criminalise 'the unlawful obtainment' of an instrument. Reference to 'unlawful' makes clear that it will not capture those who obtain it legitimately or in a neutral way. The second alternative is to criminalise the unlawful obtainment only when it involves the commission of an offence under Directive 2013/40/EU. This is the Directive on attacks against information systems,[55] which criminalises activity such as access to information systems, system interference, data interference and interceptions.[56] Relating this to the Directive on fraud, the unlawful obtainment of an instrument would be captured where the obtainment is through, for example, hacking.

Because Article 5 relates to non-corporeal instruments it is sometimes more difficult to visualise what is meant. PayPal would be a good example of a non-corporeal instrument. If, for example, D hacked into V's account and caused a payment of €5,000 to be sent from D's account to V's, this would be a good example of liability that should be criminalised under Article 5(a). Article 5(b) criminalises the counterfeiting or falsification of an instrument. This could, for example, cover diversion frauds which are becoming popular. Let us take an example:

> V is due to sell her house for €250,000. She instructed her lawyers to transfer the money into a named bank account. Shortly before the sale, her lawyers receive an email purporting to be from her telling them to send the money to a different account. They do so, but the email was not from her, and the money has been stolen.[57]

This would be a good example of someone counterfeiting a non-corporeal instrument. Derivatives of this are becoming increasingly common, and thus Article 5(b) is to be welcomed. Articles 5(c) and (d) are the equivalent of Article 4(c) and (d) so nothing more will be said on this.

Article 6 criminalises fraud relating to information systems. It requires Member States to criminalise:

---

[55] *Gillespie* [12], pp.44-48.
[56] Directive 2013/40/EU, Articles 3-6.
[57] For a real-life example, see https://www.theguardian.com/money/2017/jan/14/lost-67000-conveyancing-scam-friday-afternoon-fraud-legal-sector-email-hacker (Accessed 22 June 2019).

[the] performing or causing a transfer of money, monetary value or virtual currency and thereby causing an unlawful loss of property for another person in order to make an unlawful gain for the perpetrator or third party…when committed intentionally by:

(a) without right, hindering or interfering with the functioning of an information system;
(b) without right, introducing, altering, deleting, transmitting or suppressing computer data.

This is not dissimilar to Article 5(a) when read in conjunction the Directive on attacks on information systems. However, Article 6 is slightly wider and reflects a more updated understanding of how fraud through interference can occur. An example of when Article 6 could be used would be those instances where malware is used to pollute the DNS of a system, meaning when a user tries to access a legitimate (money-transfer) site, they are directed to a fraudulent site instead.[58] This is interfering with a system and causes the user to suffer property (financial) loss.

4.2.1 Jurisdiction

As is well known, jurisdiction poses considerable challenges for cybercrime.[59] Article 12 of the Directive specifically addresses jurisdiction. Article 12(1) requires member states to establish jurisdiction where either the offence is committed in whole or in part of its territory, or where the offender is one of its nationals. This is then supplemented by Article 12(3) which states that Member States can choose to extend jurisdiction where the offender is habitually resident (rather than a national) of the state, or where the offence is committed for the benefit of a legal person established in its territory. 'Legal person' means a company, and, therefore, the implication is that jurisdiction should be secured if a company procures the fraud identified above.

Allowing states to assert jurisdiction where the offence takes place 'in part' within their territory significantly broadens the reach of the various offences. It would, for example, allow a country to claim jurisdiction in the following instances:

(i) the perpetrator uses ICT in the territory to commit the fraud;
(ii) the victim resides in the territory, particularly where the victim is tricked into undertaking a positive act, such as sending money, card details etc.

[58] *Karlof* [14].
[59] For a discussion see *Gillespie* [12], ch.11.

(iii) the victim's bank is based in the territory;

(iv) the recipient's bank is based in the territory.

In many online frauds this will mean that more than one country will be able to assert jurisdiction. As the Directive sets out a common framework for the offences, there is unlikely to be any issue of dual criminality, which will allow easier cross-border co-operation. However, the Directive is silent as to which country can proceed against the defendant. Let us take an example:

> D, a French national living in Portugal, hacks into the computer of V, a Belgian national, and obtains his credit card details. The credit card is issued from a bank in Luxembourg, and D uses it to purchase goods from an online store in Germany.

In this example France, Portugal, Belgium, Luxembourg and Germany could all potentially claim jurisdiction, as it either involves their nationals or the crime took place, in part, in their territory. Who should go first? Assuming that the Portuguese police arrest him, should they go first as they have custody of the offender? Should it be Germany where the goods are purchased fraudulently, or Luxembourg where the card is issues and where, therefore, the financial loss will be recorded? The absence of any detail within the Directive means that it will be for the states to negotiate with each other. Presumably, the location of the offender, location of relevant evidence and the country where the majority of the fraud was conducted will be relevant considerations.

4.2.2 Does this Directive tackle online fraud?

While the Directive is comprehensive, does it tackle online fraud? The answer would appear to be that it tackles *some* online fraud, but in other instances it does not. The Directive primarily tackles the falsification and forgery of payment methods. To that extent it can be said that it covers most types of the payment frauds identified earlier. Where a person clones, for example, a debit card or credit card, then that will be a criminal offence, as will its sale, procurement and use. Similarly, where a person creates a false money transfer mandate then that will come within the Directive.

What of the other types of online fraud? For example, what of auction fraud? If a person lists an item that is not actually available, does this come within the Directive? It is not obvious from the face of the Directive that it is, but the recital suggests the issue is more complicated. Recital (11) states that 'sending fake invoices to obtain payment credentials should be considered as an attempt

at unlawful appropriation'.[60] The wording of the recital should be noted. It refers to sending fake invoices to obtain the credentials. This could include, for example, card details, bank account details or PayPal instructions. However, the emphasis is on the credentials. So if the credentials are obtained through fake invoices with the intention of then using them later fraudulently, this would constitute an offence under either Article 4(a) or 5(a) of the Directive, because the credentials become an instrument. Where those accrued credentials are used fraudulently, then it becomes an offence under Article 3. What of the situation where the credentials are not accrued, it is the *payment* itself that is accrued? In those circumstances it is not obvious that an offence takes place. Articles 3, 4 and 5 refer to accruing an *instrument* and the payment is not an instrument.

The same position is undoubtedly true of confidence frauds. In those instances, a person will typically send the fraudster some money. The instrument is neither stolen, falsified or counterfeit. The victim intends to send the fraudster some money: they have been tricked into believing that the transfer is legitimate. That is undoubtedly fraud, but it is not within the Directive. The same is true of Advance Fee Frauds ('419 frauds') where, again, the reason for transfer is deliberate but the actual transfer is legitimate.[61] Again, without a stolen, falsified or counterfeit instrument then it does not fall within the Directive.

It is easy to see why the Directive does not cater for such matters, as the Directive was replacing the earlier Framework Decision that also did not include them. However, since 2001 (when the Framework Decision was passed) and 2019 (when the Directive was passed) our understanding of online fraud has become more sophisticated. The Directive could, and should, have been expanded to cover the common forms of online fraud. That would ensure that EU citizens are given a minimal level of protection. By not doing so, there is a risk that some countries will not consider online fraud seriously, leaving citizens vulnerable and, depending on the context, undermining the single market.

5. CONCLUSION

Online fraud continues to be one of the most prolific cybercrimes. It is also a crime that perhaps has the widest scope. A fraud can range from €5 to €500m. Indeed, some suggest that small-amount frauds are the most rewarding because people will not go through the hassle of trying to

[60] OJ L123/19. 10.5.2019.
[61] *Chang* [4].

reclaim a small amount of money. If thousands of people feel the same way, then the small amount multiplied by thousands of people suddenly becomes a large amount.[62]

The transnational nature of online fraud poses challenge for existing legal instruments. Without a common definition of online fraud, it can be difficult to secure the custody of the offender. The Directive will ensure that all countries within the Union have the same basic structure. More than this, the Directive sets out a minimum threshold for the maximum sentence,[63] and it is perhaps no coincidence that the threshold is set at between one- and five-years' imprisonment. This means that the offences will come within the European Arrest Warrant scheme, ensuring that it will be simpler to obtain the custody of someone accused of committing online fraud within the EU.

The Directive is, therefore, to be welcomed in that it sets out a minimum degree of protection across the Union. However, as noted above, it does not include all forms of online fraud, and that is a mistake. Online fraud undermines the single market. This is particularly true of commerce fraud, but it can also be true of confidence frauds, which may make people more sceptical of engaging in e-commerce. There is a need to harmonise the laws relating to this type of fraud too. The Union could, and should, have set out a minimum framework to protect all victims of online fraud from the most common types of online fraud.

Care must be taken to ensure that new laws do not create false hope. The sheer volume of online fraud means that few reports are ever dealt with, and yet this can lead to resentment and frustration by those who are victims.[64] Effectively tackling online fraud requires all parties, including law enforcement, private citizens, business and the financial industry to come together to understand what each person's role is in tackling fraud.[65] The law is only one part of this puzzle, albeit an important part.

References

1. Aniello, S. and Caneppele, S: Selling Stolen Goods on the Online Markets: An Explorative Study. Global Crime. **19**, 42-62 (2018).

[62] *Gillespie* [12], p.314.
[63] Article 9 of the Directive. This follows the usual process whereby States are told that the maximum sentence can be no less than that specified within the Directive. Member States can, of course, decide to set a higher punishment.
[64] *Cross* [6], pp.6-8.
[65] *Cross* [5].

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

3. Button, M., Nicholls, C.M., Kerr, J. and Owen, R. Online frauds: Learning from victims why they fall for these scams. Australian & New Zealand journal of criminology. **47**, 391-408 (2014).

4. Chang, J.J.S.: An analysis of advance fee fraud on the internet. Journal of Financial Crime. **15**, 71-81 (2008).

5. Cross, C. Banks can't fight online credit card fraud alone, and neither can you. The Conversation. Available at: https://theconversation.com/banks-cant-fight-online-credit-card-fraud-alone-and-neither-can-you-82088 (Accessed 1.7.19).

6. Cross, C. Expectations vs reality: Responding to online fraud across the fraud justice network. International Journal of Law, Crime and Justice. **55**, 1-12 (2018).

7. Cross, C., Kelly, R. and Smith, R.G.: The reporting experiences and support needs of victims of online fraud. Trends in issues in criminal justice. **518**, 1-14 (2016).

8. Cross, C.: No Laughing Matter: Blaming the Victim of Online Fraud. International Review of Victimology. **21**, 187-204 (2015).

9. Dean, B. Hard Evidence: How Much Is Cybercrime Really Costing Us?. The Conversation. Available at http://theconversation.com/hard-evidence-how-much-is-cybercrime-really-costing-us-34473. Accessed 9 June 2019.

10. ECB: Fifth Report on Card Fraud. European Central Bank, Brussels (2018).

11. FBI: Internet Crime Report 2018. Department of Justice, Washington DC (2018).

12. Gillespie, A.A.: Cybercrime: Key Issues and Debates (2nd Edn). Routledge, London (2019).

13. Holt, T.J. and Graves, D.C. A Qualitative Analysis of Advance Fee Fraud E-Mail Schemes. International Journal of Cyber Criminology. **1,** 137-154 (2007).

14. Karlof, C., Shanker, U., Tygar, J.D. and Wagner, D.: Dynamic pharming attacks and locked same-origin policies for web browsers. Proceedings of the 14th ACM conference on Computer and communications security. 58-71 (2007).

15. Kieffer, C. and Mottola, G: Understanding and Combating Investment Fraud. In Mitchell, O.S., Brett Hamond, P. and Utkus, S.P. (eds) Financial Decision Making and Retirement Security in an Aging World. Oxford University Press, Oxford (2017).

16. Pratt, T.C., Holtfreter, K. and Reisig, M.D.: Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. Journal of Research in Crime and Delinquency. **47**, 267-296 (2010).

17. Rege, A.: What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud. International Journal of Cyber Criminology. **3**, 494-512.

18. Sandwell, B.: On the Globalisation of Crime: The Internet and New Criminality in Jewkes, Y. and Yar, M. (eds) Handbook of Internet Crime. Routledge, London (2010).

19. Stabek, A., Watters, P. and Layton, R.: The Seven Scam Types: Mapping the Terrain of Cybercrime. Second Cybercrime and Trustworthy Computing Workshop (IEEE 2010).

20. Synder, JM: Online Auction Fraud: Are the Auction Houses Doing All They Should or Could to Stop Online Fraud? Federal Communications Law Journal. **52**, 453-472 (2000).

21. UK Finance: Fraud the Facts 2018. Available at: https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2018 (Accessed 1.7.19).

22. Van Wilsem, J.: 'Bought It, but Never Got It': Assessing Risk Factors for Online Consumer Fraud Victimization. European Sociological Review. **29**, 168-178 (2011).

23. Wall, D.: Cybercrime: The Transformation of Crime in the Information Age. Polity, Cambridge (2007).

24. Whitty, M.T. Anatomy of the Online Dating Romance Scam. Security Journal. **28** 443-455 (2015).

25. Whitty, M.T. and Buchanan, T. The Online Romance Scam: A Serious Cybercrime. CyberPsychology, Behavior and Social Networking. **15**, 181-183 (2012).

26. Whitty, M.T., and Buchanan, T.: The online dating romance scam: The psychological impact on victims–both financial and non-financial. Criminology & Criminal Justice. **16**, 176-194 (2016).

27. Whitty, T.M. Do You Love Me? Psychological Characteristics of Romance Scam Victims. CyberPsychology, Behavior and Social Networking. **21**, 105-109 (2018).

28. Yar, M. and Steinmetz, KF: Cybercrime and Society (3rd Edn). Sage, London (2019).