JOURNAL OF ANTI-CORRUPTION LAW

2018 Volume 2 Number 1 Pages 58—70

IS IT CYBERFRAUD OR GOOD OL' OFFLINE FRAUD? A LOOK AT SECTION 8 OF THE SOUTH AFRICAN CYBERCRIMES BILL

Sagwadi Mabunda*

ABSTRACT

This paper discusses section 8 of the South African Cybercrimes and Cybersecurity Bill, a section which deals with the crime of cyberfraud. It argues that there are certain fraudulent acts which have been presented incorrectly as examples of cyberfraud when they are classified better as ordinary offline fraud. The mere presence of an internet element in the commission of a fraud crime is not enough to elevate the crime to cyberfraud status. Therefore, for an act to be called a cyberfraud crime, it must meet the minimum requirement of being a computer-dependent crime rather than being merely a computer-enabled crime.

1 INTRODUCTION

Fraud in South Africa is big business. The 2017 card fraud statistics report of the South African Banking Risk Information Centre (SABRIC) shows that there has been a consistent increase in gross fraud loss on South African-issued credit cards. For instance, in 2010 the gross fraud loss was R209 million for South African-issued credit cards in all countries. By 2017, the amount had risen to R436.7 million, with 2014 recording the highest gross fraud losses at R463.7 million.[1]

A type of fraud referred to as Card Not Present (CNP) fraud is reportedly the leading contributor to gross fraud loss on South African-issued credit cards. This is a kind of fraud where neither the card nor the cardholder is present during the transaction. It is common in instances where the retailer is unable to check the card

* LLB (Wits) LLM (UWC) PhD Candidate (UWC). E-mail: sagwadi.mabunda@gmail.com.
The author would like to express her gratitude to the National Research Foundation of South Africa for its generous support.

1 South African Banking Risk Information Centre *2017 Card Fraud Booklet* at 11, available at https://www.sabric.co.za/media/1448/2017-card-fraud-booklet.pdf (visited 31 July 2018).

or the identity of the cardholder when the transaction is being completed, as in online shopping or purchases made telephonically.[2] In 2017, CNP fraud accounted for 72.9% of the overall credit card gross fraud loss. The loss to CNP fraud rose from R296.4 million in 2016 to R318.4 million in 2017, that is, a 7.4% increase in a single year.[3] While the figures provided by SABRIC focus on card fraud, they give a sense of the scale of fraud as a whole in South Africa.

Cybercrime also poses a serious challenge to South Africa, with cyberfraud being a cause for major concern.[4] In response, the drafters of the South African Cybercrimes and Cybersecurity Bill of 2017 (Cybercrimes Bill) have dedicated a provision to the criminalisation of cyberfraud. Unfortunately, the explanatory notes to the Cybercrimes Bill do not give any great insights into the reasoning behind the creation of a new crime of cyberfraud when common-law fraud already exists. The notes simply state that the Bill "aims to create the statutory offence of cyber fraud by specifically criminalising fraud by means of data or a computer programme, or through the interference with data or a computer programme".[5] While this declaration might appear compelling at first glance, in reality it is not.

This paper considers the crime of cyberfraud as formulated in the Cybercrimes Bill. It argues that certain offences commonly accepted as cyberfraudulent do not qualify to be classified as true cybercrimes. This is because they do not meet the minimum requirements that would elevate them from ordinary offline fraudulent offences to cyberfraud. It argues, further, that in order for a fraudulent act to be transformed from offline fraud to cyberfraud, it needs to be a computer-dependent act rather than merely a computer-enabled act. The paper also questions whether there is a need for cyberfraud when the common-law crime of fraud is capable of addressing computer-enabled fraud adequately.

2 SABRIC (2017) at 39.

3 SABRIC (2017) at 11.

4 Kilian A (19 September 2017) "Cybercrime Becoming a Major Threat in South Africa" at 1, available at http://engineeringnews.co.za/article/cybercrime-becoming-a-major-threat-in-south-africa-2017-09-19 (visited 31 July 2018).

5 South African Cybercrimes and Cybersecurity Bill, 2017 at 67.

1.1 Cyberfraud and Common-Law Fraud

The Cybercrimes Bill provides for the criminalisation of offences relating to cyberfraud in section 8. It reads as follows:

> Any person who unlawfully and with the intention to defraud, makes a misrepresentation—
> *(a)* by means of data or a computer programme; or
> *(b)* through any interference with data or a computer programme as contemplated in subsection 5(2) or interference with a computer data storage medium or a computer system as contemplated in section 6(2),
> which—
> (i) causes actual prejudice; or
> (ii) is potentially prejudicial,
> to another person, is guilty of the offence of cyber fraud.

This definition may be compared to the common-law definition of fraud, which provides that fraud is the unlawful and intentional making of a misrepresentation which causes actual prejudice or which is potentially prejudicial to another.[6]

The essential elements of cyberfraud and common-law fraud are the same. They are (1) unlawfulness (2) intention (3) misrepresentation and (4) prejudice. The Cybercrimes Bill does not indicate whether these elements must be interpreted differently from the elements of ordinary fraud, and it therefore is unnecessary to delve into the details of all the elements. The exception is the element of misrepresentation. While common-law fraud does not specify the manner in which the fraudulent act must occur, the Cybercrimes Bill does. As is apparent from section 8, it provides that the misrepresentation must be done by means of data or a computer programme; or through any interference with data or a computer programme as contemplated in section 5(2) or a computer storage medium or computer system as contemplated in section 6(2).

Misrepresentation sometimes is expressed as a "perversion or distortion of the truth".[7] It means that A must represent to B as true a fact or a set of facts which is not actually true. In the common law, the manner in which a misrepresentation occurs does not matter. In some cases it may take the form of spoken or written words, but it may also be expressed in conduct, such as a nod of the head signifying consent.[8] The idea is well-established that a misrepresentation can take any form which is deceiving and misleading. This means that when there

6 This definition was confirmed in *Myeza* 1985 (4) SA 30 (T) 31-32; *Ex parte Lebowa Development Corporation Ltd* 1989 (3) SA 71 (T) 101; and *Gardner* 2011 (1) SACR 570 (SCA) para 29.

7 Snyman CR (2014) *Criminal Law* Durban: LexisNexis at 524.

8 Snyman (2014) at 524.

are technological advancements which allow for new forms of misrepresentation, such forms may be considered to resort under the common-law definition of fraud. In other words, new forms of misrepresentation do not add to or remove anything from the accepted elements of fraud. In turn, this means that the creation of a new crime of cyberfraud is unnecessary.

Notwithstanding its complete concordance with common-law fraud, cyberfraud has been discussed as though it is deserving of being considered a new and stand-alone offence. For that reason, it is necessary to consider some of the popular views about cyberfraud. One of the first steps in determining whether an offence may be classified rightly as a cybercrime is to determine whether it is a computer-dependent offence or a computer-enabled offence.

Computer-enabled crimes are those crimes that pre-date the existence of computers, the internet and cyberspace. These are crimes such as fraud, pornography, money laundering and (sexual) harassment. Computer-dependent crimes are the crimes that are inseparable from computers, the internet and cyberspace. They are the crimes that emerged in tandem with the internet and cannot exist without it, such as hacking and malware attacks.[9] The difference between computer-enabled and computer-dependent cybercrimes rests on the role that technology plays in the commission of the crime, that is, whether or not it would have been possible to commit the crime without a computer.

Examples of offences which commonly are referred to as cyberfraud are discussed below. In order to determine whether they are true cases of cyberfraud, they must be classified as either computer-enabled or computer-dependent. If they are computer-dependent offences and cannot be dealt with adequately under the common-law definition of fraud, then they may be raised to the status of cybercrimes.

1.2 Fraudulent Online Sales

Online shopping has become very a popular form of shopping because it is very convenient and cost effective. Many stores offer online sales services which are secure and reliable, adding to the popularity of online shopping. The internet has made it possible also for individuals to transact with one another directly on platforms such as *eBay* and *Gumtree.*

Critics have asserted that although these transactions are beneficial to individuals who wish to sell and buy goods, they can be problematic in that they

9 Furnell S (2002) *Cybercrime: Vandalising the Information Society* London: Addison Wesley at 22.

present a risk to both the seller and the buyer. For example, a seller may not wish to release the goods or services until payment has been secured and the buyer may not want to make payment before the goods or services have been delivered.[10] This makes it difficult because neither party has any guarantee that the transaction will be completed in accordance with the agreed terms and conditions.

There are some instances where a seller may offer for sale a product which does not exist actually or which is considerably different from that which was advertised. In other instances, a buyer may pay for the product via a debit order which she later reverses or cancels, after the seller has delivered the product. And because these are private transactions between private individuals, there usually are limited avenues for recourse outside of claims under contract law. Another manifestation of this type of scam is the advertising of non-existent rental properties online. In these cases, victims may be asked to send the offender information which ordinarily would be confidential, such as bank statements with personal identifying information, supposedly to confirm that the target can afford the rent. Such information is very valuable to a person intending to commit identity theft. In other cases, a victim may be requested to pay the deposit for a rental property which does not exist or is not actually available for rent.[11] The reliance upon the internet in these cases means that the victim is disadvantaged by being deprived of the visual and social clues that would guard against the fraud. The anonymity that is provided by the internet also makes apprehending the offender difficult, if not impossible.

Be that as it may, the perpetration of this crime is by no means computer-dependent. It is merely computer-enabled. Indeed the internet has provided a platform for this fraud to be committed on a larger scale by providing the offender with access to more suitable targets. Although it may have been more tedious and time consuming to perpetrate offline, the same fraud could have been committed by word of mouth, by newspaper advertisements or by posting flyers on a street lamp. It is not enough to assert that because the transaction was completed via an online platform, it is a cybercrime. It would be possible to find the offender guilty under common-law fraud. The existence of the internet makes commission of the crime more efficient, but that is ultimately a secondary consideration. Expedience cannot create a new crime.

10 Clough J (2015) *Principles of Cybercrime* Cambridge: Cambridge University Press at 211.

11 Cross C, Smith RG & Richards K (2014) "Challenges of Responding to Online Fraud Victimisation in Australia" 474 *Trends & Issues in Crime and Criminal Justice* Australian Institute of Criminology at 2.

1.3 Advance Fee Fraud

The advance fee scheme has become one of the more common forms of online fraud. This type of fraud includes lottery fraud, romance scams and inheritance schemes. The methods by which this type of fraud is perpetrated may differ, but what they have in common is a promise of a reciprocated benefit for the requirement of transfer of funds.[12]

A case of advance fee fraud typically would play out in the following way. An offender makes unsolicited contact with an unsuspecting target via spam. He informs her that he is a Nigerian Prince who has inherited a large sum of money from his late father, the king of Nigeria. He can make up an elaborate story about the instability of Nigerian politics which is threatening to dispossess him of his inheritance if he does not move it overseas. He asks the target to help him move this money to an international jurisdiction with the promise that he will share a portion of the inheritance with her.[13] Once the target has shown interest in the scam and has agreed to participate, she is instructed to make a series of miscellaneous payments[14] to the offender which will be used for cutting through the red tape associated with moving large funds. The amounts can increase as the time goes by but, ultimately, the scam concludes with the promised share of the inheritance never materialising. To make matters worse, the victim typically is left with no legal recourse because the premise of the transaction was illegal *ab initio*. What is more, the victim may be intimidated with threats of death or bodily harm or kidnapping should she try to recover her money.[15]

The advance fee fraud is referred to colloquially as the "419 Scam", being named after provision 419 in the Nigerian Criminal Code which criminalises advance fee fraud. Nigeria is notorious for being a hub of this type of fraud. It is a common form of online fraud and it has mushroomed over the years, to include pyramid schemes, get-rich-quick schemes, fraudulent business opportunities, fake educational qualifications, financial advice scams and lottery scams.[16]

The advance fee fraud is also one of the most discussed forms of online fraud, whether in the mainstream media, social media, popular culture or academic writings. One of the more famous scams was the *Banco Noroeste* scam, where a Brazilian banker bought a fake airport for US$242 million from Nigerian

12 Cross, Smith & Richards (2014) at 1.

13 Smith RG, Holmes MN & Kaufman P (1996) "Nigerian Advance Fee Fraud" 121 *Trends and Issues in Crime and Criminal Justice* Australian Institute of Criminology at 4-5.

14 SABRIC "419 Scam", available at https://www.sabric.co.za/stay-safe/419-scam/ (visited 31 July 2018).

15 Smith, Holmes & Kaufman (1996) at 3-5.

16 Clough (2015) at 214.

fraudsters.[17] This story is discussed widely as an example of one of the biggest cyberfraud cases encountered. However, while its sensational facts make for compelling reading, it is by no means a cybercrime.

Those who claim that advance fee fraud and its various manifestations are cybercrimes rely on the assertion that the internet is providing a huge marketplace for potential targets.[18] The increase in commercial and financial transactions conducted online has led to people being less prudent when it comes to sharing information online and responding to e-mails. Also, the convenience of internet transactions has robbed targets of the ability to observe social cues that might speak to the trustworthiness of the people with whom one interacts. Further, the immediacy that comes with internet transactions has given offenders more avenues for committing fraud. Paradoxically, it appears that the lack of traditional authentication tools has spawned a lax attitude to security, creating more trust in the online system instead of healthy suspicion.[19]

Advance fee fraud occurs predominantly via e-mail and the offender tends to find his victim by chance, as he would send millions of spam e-mails and only a handful of people respond positively. This means that he has a reach that defies geographical limitations. Here computers and the internet are crucial. They facilitate prolonged communication at minimal cost to offender, which means that he can engage in multiple simultaneous scams. Still, the computer is not indispensable to the success of this crime. This type of fraud can be perpetrated just as effectively via the telephone or snail-mail or, as was the case in the *Banco Noroeste* scam, via face-to-face meetings. In other words, advance fee fraud is a computer-enabled offence and does not warrant classification as a cybercrime.

1.4 Click Bait

Click bait scams are very common on the internet. The profitability of this scam is derived from exploitation of the way in which advertising on the internet is structured. Many websites and digital platforms depend on advertiser fees to operate and to make a profit. A website would charge advertisers certain fees depending on the amount of internet traffic which that website receives. This is be determined by the number of clicks that a website receives per hour, per day, per

17 BBC News Africa (2004) "Huge Nigeria Scam Trial Collapses", available at http://news.bbc.co.uk/2/hi/africa/3909233.stm (visited 20 January 2017).

18 Clough (2015) at 211.

19 Finch E (2007) "The Problem of Stolen Identity and the Internet" in Jewkes Y (ed) *Crime Online* Abingdon: Willan Publishing at 38.

week and so forth.[20] The more users visit a website, the more it can charge advertisers, thereby increasing its revenue from advertising. Click bait is about luring users into visiting a website.

Click bait should not be confused with a variation of a "malvertising" attack. A malvertising attack is a form of internet advertising which hides malware within advertisements that are hosted on relatively safe websites. The aim of malvertisements is to entice a target to click on a bogus advertisement which would download malware surreptitiously onto the computer system of the target.[21] This type of attack uses a similar concept to click bait but it should not be considered as a form of fraud because the intention of the offender is not to defraud the target but to infect her system with malware so that he can gain some other benefit, for example, access to confidential information such as passwords and financial details.

Click bait relies heavily on the manipulation of the target. It can come in the form of overstating or misrepresenting a news headline to bait people into clicking on a story. It does this by using hyperboles and superlatives that arouse the target's curiosity about an item. Invariably, the content of that item does not warrant such exaggeration.[22] Click bait is common on social networking and social media platforms where one encounters headlines such as: "This girl gave a homeless man her lunch. You won't believe what happened next!" It is very likely that what happened next was that the homeless man thanked her and ate the sandwich, but the objective was to pique the target's curiosity and have her click on the story, much to her disappointment. Unfortunately, as common as these tricks are, they are nothing new and are not exclusive to the internet. A classic example of sensational headlines is the 1983 *New York Post* headline that declared: "Headless body found in topless bar", which is acclaimed for being as witty as it is horrific.[23]

Classifying click bait as a form of cyberfraud is quite a stretch of the imagination. In fact, click bait hardly can be classified even as regular fraud. If we recall the elements of fraud, we note that there is indeed an intentional misrepresentation on the part of the offender, but it is not clear where the actual

20 Clough J (2015) at 216.

21 Techopedia (2018) "Malvertising", available at https://www.techopedia.com/definition/4016/malvertising (visited 25 July 2018).

22 Gardner B (2015) "You'll Be Outraged by How Easy it Was to Get You to Click on This Headline", available at https://www.wired.com/2015/12/psychology-of-clickbait/ (visited 19 December 2017).

23 *New York Post* (9 June 2015) "The Genius behind 'Headless Body Found in Topless Bar' Headline Dies at Age 74", available at http://nypost.com/2015/06/09/new-york-post-editor-and-film-critic-vincent-musetto-dies-at-74/ (visited 12 December 2017).

or potential prejudice lies. At worst, a "victim" suffers disappointment that her expectation of being shocked by what happened between the homeless man and the girl is dashed. Sensationalism is hardly a crime. In any case, even if this were to be argued successfully as a case of offline fraud, the computer and the internet are simply enablers of the offence. All that has happened is that the offence has moved from the pages of sensationalist newspapers and magazines to an internet website.

1.5 Fraudulent Investments

The ease with which one can generate an impressive website that solicits investments and promises high returns has made fraudulent investment schemes very popular. This offence involves the rapid dissemination over the internet of fraudulent and misleading information regarding investment opportunities. It usually is done with the intention of influencing share prices of companies. These schemes are called "pump and dump" or "trash and cash" schemes. Their tactics include releasing false news reports about certain shares and talking them up in online platforms.[24]

In August 2013, the Federal Bureau of Investigation (FBI) announced in a press release that it had arrested six men in the US and had indicted them on charges of engaging in a "pump and dump" scheme and committing advance fee fraud. It was alleged that they bought a large number of worthless shares in eleven publicly traded companies which in fact were shell companies. They then used fraudulent advertising campaigns to inflate the worth of the shares, which they in turn sold at a profit in excess of $120 million. It was alleged that in the advance fee scheme, they convinced targets to pay an advance fee which would enable them to sell their shares to other investors, or that they could join lawsuits that would enable them to recover their losses. The scheme allegedly involved targets in approximately 34 countries across North America, Europe and Asia.[25]

This type of fraud can have devastating effects on victims and the ease with which it can be perpetrated is cause for concern. Be that as it may, upon closer inspection, this crime is not a true case of cyberfraud. Taking the FBI case discussed above as an example, the press release highlights the fact that most of the

24 Morris S (2004) "The Future of Netcrime Now: Part 1 – Threats and Challenges" *Home Office Online Report* 62/04 at 17.

25 Federal Bureau of Investigation (2013) "Nine individuals Indicted in One of the Largest International Penny Stock Frauds and Advance Fee Schemes in History" Press Release, available at https://archives.fbi.gov/archives/newyork/press-releases/2013/nine-individuals-indicted-in-one-of-the-largest-international-penny-stock-frauds-and-advance-fee-schemes-in-history (visited 9 April 2018).

fraudulent activities made use of telephones and disposable cellular phones.[26] The internet may have provided a bigger and better platform to trick targets but the scam was not dependent on the presence of a computer to be successful. It is a computer-enabled crime if the advertisements that helped inflate the value of the shares were run predominantly over the internet. Should that be the case, the computer or internet merely enabled the offenders to gain a wider platform to reach more victims. It might be tempting to label the fraud a cybercrime because of the enormous financial reward that the offenders gained. However, this type of crime can be (and evidently has been) committed without resorting to cyberspace. Undoubtedly, it is a very sophisticated scheme which has the potential of taking full advantage of technological advancements, but currently it remains computer-enabled. One can see a future in which fraudsters use botnets or artificial intelligence to perpetrate this type of offence, making it computer-dependent. In that case, it may be a cybercrime, but it would likely be a case of cyberforgery and uttering, where the offender creates false data or computer programmes. In any case, fraudulent investment schemes can be dealt adequately with under the common law at this juncture.

1.6 Identity Theft

The terms "identity theft", "identity fraud" and ''identity crime" usually are used interchangeably because there is no generally accepted definition of the crime. The Australasian Centre for Policing Research has produced the following classification:

> 1. *Identity crime* is a generic term used to refer to offences where the defendant uses a false identity to perpetrate the crime. This may include such offences as money laundering, drug trafficking, tax evasion, illegal immigration or terrorism. It may also include lesser offences such as minors using false identification to buy alcohol.
> 2. *Identity fraud* is a more specific form of identity crime where a false identity is used to gain money, goods, benefits or services.
> 3. *Identity theft* is the assumption of pre-existing identity.[27]

Identity crime is by no means a new form of criminality but the advent of the internet has expanded its scope and provided new opportunities for offenders to acquire the targeted identity information.[28] The portability and transferability of digital data increases the desirability of the target while reducing the potential for detection.

---

26 FBI Press Release (2013).

27 Australasian Centre for Policing Research (2006) *Standardisation of Definitions of Identity Crime Terms: A Step Towards Consistency* Report Series No 145.3 at 9-10.

28 Clough (2015) at 219.

Before the convenience of the internet, identity fraudsters used to rely on "dumpster diving". This is the practice of rummaging through physical trash cans to find identification information from discarded documents, such as financial statements, confidential business letters and memoranda. Today, dumpster diving is not limited to physical trash but includes poorly sanitised and discarded hard drives which are flush with files containing sensitive information.

The fears around identity fraud are exacerbated by the continuous stream of reports of massive data leaks that appear every other day. In these data breaches, such as the one at American credit reporting agency Equifax in late 2017, there is always a concern as to the use to which the sensitive information can be put by hackers. However, once one wades through the sensationalism and the media frenzies, one realises that the fraud being perpetrated is the same as ordinary fraud. Users of sensitive personal information to commit credit card fraud, for example, have not changed since the traditional dumpster divers of yesteryear. Granted, they possess better skill sets but they are conventional fraudsters all the same. They use the information they obtain in the same way as before. When one considers identity theft, one must differentiate between the hacking offences that may occur when the offender seeks to gain the confidential information and the fraudster who uses that information to defraud the target. The fraudster can be dealt with adequately under the common law.

2 WHY DOES THIS MATTER?

It is accepted that laws heavily influence the perception of society about what acts are right or wrong, socially acceptable or morally reprehensible. This is the reason why crimes are set out clearly in legislation. But in order for any law to be effective in combating crime, its parameters must be defined clearly. In this regard, it is necessary to have minimum requirements or characteristics which identify what should qualify as a cybercrime and what should not.

Firstly, how can one combat something if one does not know how to define it? It has been established that cybercrime grows at an exponential rate, and perhaps this made legislators anxious to criminalise everything dubbed "cyber" without a proper evaluation of its cybercriminological veracity. The examples discussed in §1 above are evidence of that legislative anxiety.

Secondly, the complexity of cybercrime requires a phenomenal amount of resources to be allocated to combating it. Many law enforcement agencies, such as the FBI and Interpol, have dedicated investigative units that deal specifically with cyber-related crimes. In Chapter 10 of the Cybercrimes Bill provision is made for

the establishment of "Structures to Deal with Cybersecurity". These include a Cyber Response Committee,[29] and nodal points and private sector computer security incident response teams.[30] These specialised units and the special units within the police services and the prosecuting authority need to have a clear mandate about the kinds of crimes which fall within their remit. For example, if a team within the police services were to be made responsible solely for the cybercrimes contained in the Cybercrimes Bill, the novelty of cybercrime almost guarantees an understaffed and/or under-skilled team with very limited resources.

Say a victim is hit over the head with a computer and she dies, will that be called cybermurder? Of course not. The definition of murder under the common law is the unlawful and intentional killing of a person. The way that the person is killed is inconsequential in the determination of whether a murder was committed. The victim could have been killed as easily with a brick or hammer or a knife. The common-law crime of murder can address this case adequately. It obviously would not be the responsibility of any cybercrimes unit.

Take a second example. A target is sent an e-mail telling her that she has won a prize of R50 000 and she would have to deposit R5 000 into the bank account of the sender as transactional fees. The victim complies but the R50 000 does not materialise. Is this a cybercrime and should a special cybercrimes unit be investigating it? Undoubtedly, this is a case of fraud but it does not qualify as a cybercrime. The crime may have been enabled by a computer but it is definitely not computer-dependent.

The distinction between computer-enabled and computer-dependent crimes is important in these cases because it helps with the distribution of resources. Many computer-enabled crimes, such as advanced fee frauds, are just high-tech manifestation of offline crimes, which mean that the work of the fraudster is made easier and more efficient by a computer. She can reach more people, more places and in less time than if she had to defraud one person at a time. However, the inclusion of the e-mail as a medium is not enough to elevate this crime to the status of a cybercrime and, therefore, the case may be referred to an ordinary crimes unit which deals with conventional fraud cases. The problem described above applies not only to the police services but also to the prosecuting authorities, as well as to cybercrime and cybersecurity researchers. The difficulty is that so much of cybercrime is becoming so mythologised that cases which can be dispensed with easily are being over-complicated nowadays and not resolved at all.

29 Section 53 of the Cybercrimes Bill.
30 Section 55 of the Cybercrimes Bill.

3 CONCLUSION

The crime of fraud has evolved over the decades but it has done so only in respect of the manner in which the fraudster perpetrates the crime. The essential elements of fraud have not changed in any significant way. There is a need to be vigilant when determining which offences are categorised as cybercrimes by observing minimum characteristics of the offence, such as whether it is computer-enabled or computer-dependent. In many cases an offence can be dealt with adequately in terms of the existing common law of fraud. The creation of a new crime of cyberfraud is unnecessary and will increase the burden on law enforcement agencies and the rest of the criminal justice system. It also will divert resources from detecting, combating and defeating true cybercrimes.

The crimes discussed above may have devastating effects on their victims, but they should not be re-classified arbitrarily as cybercrimes. It is important to allow the South African Cybercrimes Bill to be effective by not saddling it with an overly broad mandate. Section 8 of the Cybercrimes Bill ought not to be enacted until such time as its contents have been differentiated clearly from the common-law version of fraud, and its provisions have been made applicable only to computer-dependent offences.