JICLT
Journal of International Commercial Law and Technology
Vol.9, No.2 (2014)

The Criminalisation of Identity Theft under the Saudi Anti-Cybercrime Law 2007

Suhail Almerdas[1]

PhD Researcher at the Centre for Criminal Justice Studies,
School of Law
University of Leeds, UK,
lwsia@leeds.ac.uk

Abstract. This article examines the extent to which legal measures enacted in Saudi Arabia are able to tackle the problem of widespread cybercrime, namely identity theft. It examines to what extent the Saudi Anti-Cybercrime Law 2007 is capable of encompassing possible methods for obtaining the financial information of others, including phishing, pharming, using malware and hacking, which appear to be the most common methods of obtaining the personal information of others online. It also questions whether the Saudi Anti-Cybercrime Law should take action and criminalise identity theft that involves non-financial motivations in a way similar to the criminalisation of identity theft that does involve financial motivations, an activity which has already been criminalised under the Anti-Cybercrime Law. Furthermore, the paper highlights how it is important to criminalise the transferring and possession of materials (data and programs) for the purpose of identity theft in order to strengthen the legal response to this type of cybercrime in Saudi Arabia.

1. Introduction

Identity theft is not a new phenomenon. Typically, this activity is committed through physical means, such as stealing a wallet or going through the rubbish bin of someone to find discarded documents that contain an individual's personal information, such as name, date of birth, address, phone number and credit card information.[2] The development of information and communication technologies and the proliferation of the Internet, however, have provided criminals with even more opportunities to acquire personal and confidential information through various methods, such as phishing, pharming, using malware and hacking.[3] In addition, the Internet extends the reach of criminals to a global level. In cyberspace, as Internet World State shows, approximately 2.5 billion people use the Internet from all of the world's regions.[4] Certainly, any of these people can be targets for identity thieves. After confidential financial account details are obtained, committing fraud is only a few keystrokes away.[5] Various types of fraud can be committed using the identity-related information of individuals, such as purchasing goods or registering for services using the victims' personal information, and transferring money online from the victims' accounts to another account.[6] Non-financial consequences can also take place. Identify thieves

[1] LLB, LLM, PhD Researcher at the Centre for Criminal Justice Studies, School of Law, University of Leeds, UK, Email: lwsia@leeds.ac.uk; Lecturer in Law, Faculty of Law, King Abdulaziz University, Jeddah, Saudi Arabia, Email: salmrdas@kau.edu.sa.

[2] Fujun Lai, Dahui Li and Chang-Tseh Hsieh, 'Fighting Identity Theft: The Coping Perspective' (2012) 52 Decision Support Systems 353, 354.

[3] Marco Gercke, 'Legal Approaches to Criminalize Identity Theft' in United Nations Office on Drugs and Crime, *Handbook on Identity-Related Crime* (United Nations 2011) 17-18.

[4] Internet World State, 'Internet Usage Statistics' (30 June 2012) <http://www.internetworldstats.com/stats.htm> accessed 10 May 2013.

[5] Samuel C McQuade (ed), *Encyclopedia of Cybercrime* (Greenwood Press 2009) 75.

[6] See International Telecommunication Union, 'ITU Global Cybersecurity Agenda, High-Level Experts Group, Global Strategic Report' (2008) 39

may acquire the identity-related information of others to impersonate them in order to tarnish their reputations.[7]

Identity theft attacks seem to be one of the most common and widespread cybercrimes in the world. It was estimated in 2007 that there is one phishing attack among every 87 emails, which is only one method of committing identity theft.[8] This means that millions of phishing attacks are carried out each year against Internet users throughout the world.[9] Most recently, the Anti-Phishing Working Group (APWG) revealed that it received 53,081 reports of phishing attacks and identified 119,101 unique phishing sites during the second quarter of 2013,[10] which seems to be a huge number. With the expansion of databases, one successful identity theft attack could put millions of people's identity-related information at risk. A good example to illustrate this is the hacking of Sony's PlayStation Network in April 2011, in which hackers gained access to 77 million accounts on the PlayStation Network.[11] Forensic testing revealed that the data of 77 million users, including usernames, passwords, security answers, credit card details, purchase history and addresses were believed to have been acquired by hackers.[12] According to Alan Paller, research director of the SysAdmin, Audit, Network, Security (SANS) Institute, the value of the identity-related information of PlayStation users, if sold on the online black market for credit cards and personal information, could reach tens of millions of dollars.[13]

What the above examples, and indeed many other similar examples, show is that identity theft attacks have reached a high level of sophistication and are expanding, putting huge amounts of people's identity-related information at risk. Thus, various measures must be taken to reduce the effects of attacks, such as technical measures and improved awareness of Internet users. Among these measures is the need for effective legislation that is able to tackle this type of cybercrime and eliminate safe havens for identity thieves who can launch their attacks from any place in the world.

During the past decade, many countries have passed legislation to impose criminal sanctions on identify theft. Among these countries is Saudi Arabia, which enacted the Anti-Cybercrime Law in 2007 to handle various harmful activities that occur in cyberspace, including identity theft. However, the Saudi Anti-Cybercrime Law 2007 seems to have received little attention from researchers who sorely need to examine whether or not this law is able to tackle cybercrimes (including identity theft) and determine whether further legal responses are required. This article attempts to contribute to such an important examination through examining whether the Saudi Anti-Cybercrime Law is capable of tackling identity theft or whether further legal responses are needed. It begins by providing an overview of the term 'identity theft', which is by itself a controversial term, and how this term will be used throughout the paper. Then, an examination of the extent to which the Anti-Cybercrime Law is able to tackle the problem of identity theft that occurs in cyberspace will be provided. This examination will take place across three sections: 1) the offence of identity theft under the Anti-Cybercrime Law 2007; 2) identity theft and financial/non-financial motivations; and 3) transferring and possessing materials (data and programs) for the purpose of identity theft.

<http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/global_strategic_report.pdf> accessed 26 October 2013.

[7] Chuck Easttom and Det J Taylor, *Computer Crime, Investigation, and the Law* (Course Technology 2011) 5.

[8] Samuel C McQuade (ed), *Encyclopedia of Cybercrime* (Greenwood Press 2009) 140.

[9] Ibid.

[10] Anti-Phishing Working Group, 'Phishing Activity Trends Report: 2nd Quarter 2013' (2013) 3 <http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf> accessed 9 November 2013.

[11] BBC, 'Sony Insurer Seeks PlayStation Network Hack Opt-Out' (22 July 2011) <http://www.bbc.co.uk/news/technology-14247883> accessed 3 October 2013.

[12] Keith Stuart and Charles Arthur, 'PlayStation Network Hack: Why It Took Sony Seven Days to Tell the World' *The Guardian* (London, 27 April 2011) <http://www.theguardian.com/technology/gamesblog/2011/apr/27/playstation-network-hack-sony> accessed 6 October 2013.

[13] Ibid.

2. The term 'identity theft'

The term 'identity theft' is widely used today among law enforcement agencies, organisations and scholars. However, the term 'identity theft' has two main problems. The first one is that this term is not consistently used – as is the case for many widely used terms. Some use the term 'identity theft' to refer to using the personal identifying information of others for unlawful purposes, such as to acquire goods and services. In this approach, Hoffman and McGinley define identity theft as 'the use of an individual's personal identifying information without his or her knowledge and with the intent to aid or abet in any unlawful activity such as the fraudulent obtaining of services, merchandise, money, and/or credit'.[14] In a similar vein to Hoffman and McGinley, McQuade considers the use of the personal identifying information of the victim for unlawful purposes as a core component in defining identity theft. McQuade states that

> Identity theft, also referred to as *identity fraud*, is a criminal act where one individual misrepresents himself by pretending to be someone else. This is typically done by illegally using the victim's personal information to open new financial accounts, use existing financial accounts, or do some combination of the two.[15]

Obviously, according to the above definitions, obtaining the personal information of someone does not constitute identity theft by itself; the term refers to the misuse of this information that follows from the obtaining of the information. The Identity Fraud Survey Report issued by Javelin Strategy and Research does not agree with the above definitions. Instead, the *Javelin Report* views those activities as 'identity fraud' rather than 'identity theft'. The *Javelin Report* argues that

> Identity fraud is the actual misuse of information for financial gain and occurs when criminals use illegally obtained personal information to make purchases or withdrawals, create false accounts or modify existing ones and/or attempt to obtain services such as employment or health care.[16]

As for identity theft, the *Javelin Report* contends that 'True identity theft occurs after the exposure of personal information; typically someone's personal information is taken by another individual without explicit permission'.[17] In the same vein as the *Javelin Report*, Vacca considers the appropriation of the personal identifying information of others as a core component of the identity theft definition, stating that 'identity theft is the appropriation of an individual's personal information to impersonate that person in a legal sense'.[18]

The inconsistent using of the various terms in relation to identity crimes was recognised by the Australian Centre for Policing Research (ACPR), which has developed a number of definitions, including identity theft and identity fraud, and suggested that they be used at least within Australasian law enforcement and revenue protection agencies. Consistent with the *Javelin Report*, the ACPR distinguished between 'appropriation' of another person's identity and 'use' of someone's identity to commit fraud. The ACPR recommended that '"Identity Fraud" be used to describe the gaining of money, goods, services other benefits or the avoidance of obligations through the use of a fabricated identity; a manipulated identity; or a stolen/assumed identity',[19] and that '"Identity Theft" be used to describe the

---

[14] Sandra K Hoffman and Tracy G McGinley, *Identity Theft: A Reference Handbook* (Greenwood Publishing Group 2010) 2.
[15] Samuel C McQuade (ed), *Encyclopedia of Cybercrime* (Greenwood Press 2009) 91.
[16] Javelin Strategy and Research, '2011 Identity Fraud Survey Report: Consumer Version' (2011) 6 <https://www.javelinstrategy.com/brochure/207> accessed 8 May 2013.
[17] Ibid.
[18] John R Vacca, *Identity Theft* (Pearson 2003) 4.
[19] Australian Centre for Policing Research, 'Standardisation of Definitions of Identity Crime Terms: A Step towards Consistency' (2006) 15 <http://pdf.aminer.org/000/246/496/electronic_commerce_fraud_towards_an_understanding_of_the_phenomenon.pdf> accessed 2 November 2013.

theft or assumption of a pre-existing identity (or significant part thereof), with or without consent, and, whether, in the case of an individual, the person is living or deceased'.[20]

With these definitions of the *Javelin Report*, Vacca, and the ACPR, identity theft is committed once an individual appropriates personal information of someone, irrespective of whether that identity-related information is used for committing other offences or not. This article will adopt this approach when talking about identity theft. More precisely, when the term identity theft is used in this article it basically refers to the 'appropriation' of the personal information of someone without lawful cause rather than 'using' the personal information of someone to commit fraud. The approach of McQuade, Hoffman, and McGinley is to be avoided because they tend to use the terms 'identity theft' and 'identity fraud' interchangeably. In this way, McQuade, Hoffman, and McGinley link their definition to fraud; thus, by adopting their approach, it would be difficult to distinguish between 'appropriation' and 'use' of another person's identity, which are clearly distinct acts.

The second problem with using the term 'identity theft', as Clough noted, is the involvement of the word 'theft'. According to Clough, the problem is that the term 'theft' is not used in its literal meaning because the identity of an individual is not 'stolen'. Instead, information about the identity of an individual is appropriated for the purpose of committing a further offence.[21] It seems that this problem caused some countries to avoid using the term 'theft'. An example is Norway, which used the term 'identity infringement' in the Penal Code 2009 section 202, instead of 'identity theft',[22] which seems more precise than the term 'identity theft'. Other terms, seemingly more accurate than 'identity theft', such as 'identity appropriation' and 'identity assumption', might be also suggested. However, while some phrases admittedly seem more accurate than the phrase 'identity theft', avoiding using the term 'identity theft' does not seem necessary or practical as it is widely used and accepted today, regardless of its accuracy.

3. The offence of identity theft under the Anti-Cybercrime Law 2007

Until 2007, neither identity theft that is committed through physical means nor that which is committed through a computer was offences under any Saudi law. While this omission remained for identity theft committed through physical means, it did not do so for the identity theft carried out via computers because that format became an offence with the enactment of the Anti-Cybercrime Law 2007.

The offence of identity theft was provided within the Anti-Cybercrime Law at article 4 as follows:

> Any person who commits one of the following cybercrimes shall be subject to imprisonment for a period not exceeding three years and a fine not exceeding two million riyals, or to either punishment:
>
> …
>
> (2) Attaining - without lawful cause - to bank or credit data, or data pertaining to ownership of securities to obtain data, information, funds or services offered.

Commission of the offence under article 4(2) requires the *actus reus* of 'attaining' to 'bank or credit data, or data pertaining to ownership of securities'. As for the term 'attaining', it is indeed an extremely broad term and seems to be intended to operate broadly and include any method that may be used to acquire identity-related information. Thus, this should make article 4(2) capable of encompassing all possible methods of obtaining the personal information of others, including phishing, pharming, using malware and hacking, which appear to be the most common methods of obtaining the personal information of others online.[23] In addition, article 4(2) requires specific *mens rea* for criminal liability to

[20] Ibid.
[21] Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press 2010) 209.
[22] See Stein Schjolberg and Solange Ghernaouti-Helie, *A Global Treaty on Cybersecurity and Cybercrime* (2nd edn, Stein Schjolberg and Solange Ghernaouti-Helie 2011) 43-44.
[23] See David S Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity 2007) 71-79; James Graham and others (eds), *Cyber Fraud: Tactics, Techniques, and Procedures* (Taylor and Francis Group 2009);

be attached, by proving that the offender who attained bank or credit data, or data pertaining to ownership of securities intended 'to obtain data, information, funds or services offered'. A further condition is required by article 4(2), which is that the offence be committed 'without lawful cause'. As Alboqami noted, this condition clearly excludes those who are authorised by law to deal with other people's identities from falling within the boundary of article 4(2),[24] which therefore should include businesses, police organisations and governmental departments that deal with people's identities. Subject to these exceptions, it could be said that article 4(2) was designed to be applied to people who, without lawful cause, attain the financial information of others in order to obtain data, information, funds or services offered irrespective of whether they use it for further crimes or not.

However, it should be noted that in order to attain bank or credit data, or data pertaining to ownership of securities, an offender may commit an article 4(2) offence though committing other offences, such as unauthorised access (which is an offence under article 93(1) of the Regulation of Telecommunications Law 2002) or data interference (which is an offence under article 5(2) of the Anti-Cybercrime Law 2007). Moreover, those who violate article 4(2) may commit further offences once they attain the confidential financial data, such as by gaining money or services through using the victim's personal information (which is an offence under article 4(1) of the Anti-Cybercrime Law 2007). This means that committing the offence of identity theft under article 4(2) would overlap with other offences and that may cause some confusion when establishing the offence under article 4(2). Accordingly, in order to get a clear picture of how article 4(2) may apply and would overlap with other offences, it is helpful to discuss them by considering the main possible methods that may be used by offenders to commit identity theft, namely phishing, pharming, using malware and hacking. Certainly, discussing these methods also serves as way of highlighting weaknesses or possible difficulties that may arise when dealing with this type of cybercrime under Saudi law.

The first method to discuss is phishing, which is one of the main methods used to acquire confidential information about others in cyberspace.[25] It is a type of social engineering that is used by criminals who attempt to deceive potential victims and get them to provide their private information, such as usernames, passwords and bank account numbers.[26] A clear and comprehensive explanation of a typical scenario of phishing is provided by Graham and others as follows:

> This well-known tactic typically involves setting up a fraudulent Web site designed to look like the legitimate Web site of a bank or other financial institution, and then spamming out e-mails that appear to be sent from that legitimate institution. These e-mails urge recipients to click on the link to the fraudulent Web site (for example, by stating that the institution will cancel their account if they do not visit the Web site and "update their account information"). The fraudulent Web site records information entered by the victim (such as his or her login and password) and sends it back to the attacker, who either uses the information to access the victim's account or sells the information to other criminals.[27]

In this scenario, once the victims enter their confidential information, the fisher undoubtedly attains financial data, and by doing so, it could be said that the attacker would be liable for prosecution under article 4(2) regardless of whether that obtained information is used for committing other offences or not. Nonetheless, if the fisher went beyond that point, which seems more likely to happen, and used the financial data of the victim, such as using credit cards details for purchasing goods, then, as already noted, the offender would be liable for committing another distinct offence under article 4(1) of the Anti-

---

Marco Gercke, 'Legal Approaches to Criminalize Identity Theft' in United Nations Office on Drugs and Crime, *Handbook on Identity-Related Crime* (United Nations 2011) 16-18.

[24] Nasser Alboqami, *Cybercrime and Combatting it in the Kingdom of Saudi Arabia* (Alhumaithy 2009) 256.

[25] International Telecommunication Union, 'ITU Global Cybersecurity Agenda, High-Level Experts Group, Global Strategic Report' (2008) 40
<http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/global_strategic_report.pdf> accessed 26 October 2013.

[26] Samuel C McQuade (ed), *Encyclopedia of Cybercrime* (Greenwood Press 2009) 139.

[27] James Graham and others (eds), *Cyber Fraud: Tactics, Techniques, and Procedures* (Taylor and Francis Group 2009) 27.

Cybercrime Law 2007 which is acquisition for oneself or others of movable property (which includes money) through fraud.

Alternatively, as highlighted by Graham and others, a phisher may choose to sell the obtained financial data to other criminals rather than to use them personally.[28] If this happened, would the phisher be liable for committing another offence, namely transferring or selling other people's financial data without lawful cause? Surprisingly, the answer is no. This is simply because neither article 4(2), nor any other provision under the Anti-Cybercrime Law 2007 seems to make transferring or selling the financial data of others without lawful cause an offence, which is a notable weakness that will be returned to later. How about the criminal liability of person who bought these illegally obtained data online? While there is no express criminalisation for buying other people's financial data, it is argued that the buyer has committed the *actus reus* of the offence of article 4(2) by attaining financial data without lawful cause. What if the phisher has transferred or sold the obtained information to another person through physical means (hand to hand), is the buyer in this situation liable for committing an offence in the same way as one who bought that financial data online? Interestingly, the answer is no. This is because identity theft that is committed through physical means is not an offence under Saudi law, as addressed previously, and buying financial data of others in the above example cannot fall within the scope of article 4(2) because it is only related to activities that take place online. While this situation relating to physical means is also another obvious weakness in dealing with the identity theft in Saudi Arabia, it is beyond the scope of this article and thus will not be discussed further. However, it leads to consideration of the further situation of where this buyer keeps this purchased confidential financial data in electronic form, perhaps in preparation to sell it online – would s/he be subject to committing any offence, namely possessing other people identity without lawful cause? Unfortunately, the answer is no, which indeed constitutes another weakness in dealing with this type of cybercrime, a topic that will be returned to later.

The second method of identity theft to be discussed relates to a more sophisticated way of acquiring other peoples' identities, which is known as 'pharming',[29] and sometimes 'domain name server (DNS) poisoning', DNS spoofing, or 'cache poisoning'.[30] The same as phishing, the pharming attack is accomplished through setting up a fake website that is designed to appear to belong to a legitimate institution to extract personal information from potential victims.[31] However, pharming is different from phishing in that in a pharming attack, an offender does not employ social engineering to trick a potential victim to visit the false website; instead, the offender reroutes the victim from a valid website that a victim intended to visit to a false one.[32] Pharmers usually accomplish their attacks using two methods. The first is that a pharmer may choose to hack into a DNS and change the address of a targeted website, such as the website of a financial institution, to redirect a potential victim to a fake website. The second method a pharmer may select is to send a virus by email to alter local host files on the victim's computer of a targeted website, to redirect the victim to a fake website. In either method, when users enter the address of the website that they intended to visit, they are automatically redirected to a fraudulent website without their knowledge, which automatically captures their account usernames and passwords when they enter them.[33]

In contrast to the phishing method, for an attacker to accomplish the attack (attaining victim financial data) via pharming, s/he needs first to hack into a DNS and change the address of a targeted website or send a virus by email to alter local host files on the victim's computer. If the attacker adopted the first approach, then by securing the unauthorised access, s/he is liable for prosecution under article 93(1) of

---

[28] Ibid.
[29] Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press 2010) 194.
[30] David S Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity 2007) 77.
[31] James Graham and others (eds), *Cyber Fraud: Tactics, Techniques, and Procedures* (Taylor and Francis Group 2009) 47.
[32] See David S Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity 2007) 77; Neil Daswani, Christoph Kern and Anita Kesavan, *Foundations of Security: What Every Programmer Needs to Know* (Apress 2007) 28; James Graham and others (eds), *Cyber Fraud: Tactics, Techniques, and Procedures* (Taylor and Francis Group 2009) 47.
[33] See James Graham and others (eds), *Cyber Fraud: Tactics, Techniques, and Procedures* (Taylor and Francis Group 2009) 47-48; Shannon Belew and Joel Elad, *Starting an Online Business All-in-One for Dummies* (2nd edn, Wiley Publishing 2009) 337; Deborah Morley and Charles S Parker, *Understanding Computers: Today and Tomorrow, Introductory* (13th edn, Course Technology 2011) 375.

the Regulation of Telecommunications Law 2002, which made mere unauthorised access illegal in itself regardless of the purpose. If the attacker then changed the address of a targeted website, s/he is committing another offence under article 5(2), which is altering of the data of the website. On the other hand, if the attacker adopted the second approach, then by changing the local host files on the victim's computer of a targeted website, s/he would be liable for prosecution under article 5(2), which is altering the data on the victim's computer. If the attacker, in either way (hacking or sending a virus), was successful in receiving financial data from potential victims, then it could be said that the offence under article 4(2) would be established, which is attaining financial data without lawful cause.

Using malware to acquire personal information is the third method of identity theft to be discussed. With this method, an attacker adopts the same approach of phishing in terms of sending emails to potential victims. However, this method differs from a phishing attack in that while the attacker in phishing needs his or her potential victims to visit the fake website and enter their personal information, in using malware, an attacker embeds a link in a message or an attachment file, which once clicked causes malicious software, such as Trojans or key loggers, to be downloaded onto the victim's computer.[34] Installing key loggers on the victim's computer would then enable the attacker to capture keystroke information that could include credit card details or other personal information from the victim's keystrokes.[35]

In this method, if the potential victim clicked on the attached file (which contain malicious software) then the attacker committed an offence under article 5(2) of the Anti-Cybercrime Law, namely, altering a computer program. If the victim then entered personal financial information, then it could be said that the attacker is committing an offence under article 4(2), which is attaining financial data. However, it appears that the task would be harder for the prosecutor in terms of proving this offence under article 4(2) in comparison with phishing and pharming. This difficulty resides in proving the required specific *mens rea*, which is to 'obtain data, information, funds or services offered'. In phishing and pharming, it seems convincing to say that a phisher or pharmer who sets up a fake website that is designed to appear to belong to a legitimate institution and tries to extract personal information from potential victims is more likely intending to attain financial data, funds, or services. The same cannot be said for those who install Trojans or key loggers into victims' computers to capture confidential data. This is because the objective behind the malicious software might not be to capture financial detail but to capture, for instance, a password for the victim's email for other purposes, such as blackmail, even if, unforeseen, the victim entered bank details that then came into the hands of the attacker.

The fourth type of identity theft to discuss here relates to using hacking to obtain personal information. A case that happened in 2011 in Saudi Arabia,[36] which involved hacking along with attaining financial data, is a good example to use to discuss this type of identity theft. In this case, Ziad Alriqaiti, a media spokesperson for the Eastern Region Police, stated that a company that specialised in information technology at Ahsa city filed a complaint claiming that the official email of the company has been hacked. The company alleged that the emails contained confidential information sent to the company, including passwords and other sensitive information for a number of the company's accounts. The hacker, according to the company allegation, managed to exploit the company's email and also hacked the sites of three other companies. The company further alleged that the hacker then sent threatening letters to those companies and their customers. As a result, according to Alriqaiti, the Department for Combating Cybercrime, which is part of the Criminal Search and Investigation Department in Ahsa, managed to track down the hacker and finally arrested him.[37]

Clearly, as mentioned earlier, by securing unauthorised access, the attacker is liable for prosecution under article 93(1) of the Regulation of Telecommunications Law 2002, which made mere unauthorised

---

[34] See Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press 2010) 193.

[35] Sherly Abraham, InduShobha Chengalur-Smith, 'An Overview of Social Engineering Malware: Trends, Tactics, and Implications' [2010] Technology in Society 183, 199.

[36] Saleh Almohaisen and Saleem Alqatan, 'Police of Ahsa Foil [Hackers] Who Hacked Four [Technology] Companies' *Alriyadh Newspaper* (Riyadh, 14 December 2011) <http://www.alriyadh.com/2011/12/14/article691612.html> accessed 17 June 2013.

[37] This case was published in a newspaper, as indicated above, without information concerning what was the punishment and what offence was actually used. It is even difficult to find details of the case because cases are not officially made available to the public in Saudi Arabia, with the exception of few cases that are officially published by the Ministry of Justice in relation to traditional crimes. There does not appear to be any case concerning identity theft among them, including the case in this example.

access illegal in itself regardless of the purpose. However, if the prosecutor proved that the intentions of the hacker were threatening, which seems possible given the context of the case, then it is more likely that the attacker would be prosecuted under article 3(2) of the Anti-Cybercrime Law (instead of article 93(1)), which criminalises unauthorised access to threaten a person and it is a more serious offence than article 93(1)). As for attaining financial data, while it is clear that the attacker attained bank data of the company without lawful reason, it would seem difficult to prove that the attacker intended to obtain this financial data. From the context of the case, it does not seem that the attacker intended to obtain data, information, funds or services offered from the bank account details that he attained, rather he seems most likely to have intended to threaten the company and reaching the financial data appears to have been accidental. However, if the prosecutor proved that the offender's intention for attaining the bank data of the company was to obtain data, information, funds or services offered, then certainly the offender was liable for committing an offence under article 4(2) of the Anti-Cybercrime Law.

To sum up, article 4(2) seems to cover any method that may be used to obtain individuals' financial information, including phishing, pharming, using malware and hacking. With any of these methods, once the perpetrator attains the financial information of the victims without lawful cause, s/he would be liable for committing an offence under article 4(2) irrespective of whether s/he uses it for further crimes or not. Furthermore, the broad meaning of 'attaining' in article 4(2) seems to cover any way that might be created in the future to acquire the confidential information of people. However, article 4(2) clearly limits the criminalisation to only attaining information that relates to 'bank or credit data, or data pertaining to ownership of securities'. By this condition, the Anti-Cybercrime Law limits the application of article 4(2) to identity theft that is related to financial matters.[38] It follows that acquiring the identity-related information of others for non-financial motivations, such as impersonating another person in order to tarnish his or her reputation, is not an offence under the Anti-Cybercrime Law. This limit gives rise to an important question of whether identity theft that causes non-financial harm is less important than that which does cause financial harms and thus needs not be criminalised. The next section will be devoted to discussing this issue. Another concern with article 4(2) is that it appears to have failed to criminalise transferring and possessing the confidential data of others. Thus, the Anti-Cybercrime Law would not be able to deal with those who transfer or sell, for instance, the credit card details of individuals, or with those who, for example, possess other people's identity-related information, such as criminal organisations, which is a clear weakness in combating identity theft under Saudi law, an issue that will be discussed after the following section.

4. Identity theft and financial/non-financial motivations

As emphasised earlier, article 4(2) limits criminalisation to only identity theft that involves financial motivations. Accordingly, acquiring the identity-related information of others for non-financial motivations, such as to impersonate another person in order to tarnish his or her reputation, is not an offence under the Anti-Cybercrime Law. This limit, as already stated, gives rise to an important question of whether identity theft that causes non-financial harm is less important than that which causes financial harm and thus needs not be criminalised. According to Thorpe, non-financial harm, in particular social harm, can be no less disastrous than financial harm. He argued that, by acquiring an online forum's member password and impersonating that person in a place where people know him or her, the impersonator may quickly tarnish the victim's reputation and even make him or her lose his or her account or become liable for defamation or offences, depending on the words that the offender has typed. Thorpe also added that email is not immune from being used to tarnish the reputation of the email owner, providing that sending bulk emails using the victim's address would make the victim receive complaints and gain a reputation as a spammer.[39] Based on Thorpe's view, further harmful methods exist that were probably not widespread at the time of Thorpe's writing in 2006 and perhaps cause more calamities in comparison with forums and emails. These ways in particular include the popular social networking

[38] See Nasser Alboqami, *Cybercrime and Combatting it in the Kingdom of Saudi Arabia* (Alhumaithy 2009) 256.

[39] Stephen W Thorpe, 'Extranets: Applications, Development, Security, and Privacy' in Hossein Bidgoli (ed), *Handbook Of Information Security: Information Warfare; social, Legal, and International Issues; and Security Foundations*, vol 2 (Wiley 2006) 225.

services Facebook (which was launched in 2004);[40] and Twitter (which was launched in 2006).[41] Both Facebook and Twitter, as well as many other social network services, seem to have a greater audience and spread to a wider extent in comparison with forums and emails, which would make it a greater disadvantage when it comes to tarnishing the reputation of someone.

However, the possible non-financial consequences that Thorpe assumes seem unlikely to occur in the majority of cases. It seems clear for those who are using these services, including forums and emails and even Facebook and Twitter, that recipients of emails and followers of forums, Facebook and Twitter would quickly recognise if the account had been taken over by someone by noticing sent or posted things that are not typically sent by the real owner of the account, which would undermine the possible harmful consequences to the reputation of the real owner of the account. Alternatively, and more cautiously, some victims of impersonated accounts would quickly correct the misleading impression through their other accounts, their friends' accounts or newspapers, especially if they are well known figures or governmental or business institutions, and warn others that their email, forum, Twitter or Facebook accounts are being impersonated. An example is Abdulaziz Altarifi, a famous Islamic scholar, who warned his followers on Facebook that both his email account and Twitter account were impersonated.[42] Likewise, the Health Affairs at Jeddah city warned people through the official website of the Saudi Ministry of Health that its Twitter account was impersonated. The Health Affairs asserted that anything published by the impersonated account was completely false and should be ignored by the account followers.[43]

In contrast to Thorp, Easttom and Taylor have a different perspective. While they maintain that identity thefts that involve financial motivations and non-financial motivations could cause harm to the victims, they seem to view the former as more dangerous than the latter. However, unlike Thorp, they view it not on the basis of potential damage to the victim, but rather from the perspective of its widespread impact. They view identity theft that involves financial matters as more dangerous than the non-financial kind on the basis that 'most incidents of identity theft involve economic motivations'.[44] They supported this argument by providing the findings of the US Federal Trade Commission in 2005, which showed that while millions of people 'were the victims of some form of identity theft'[45], '[t]he majority of these identity-theft incidents were financial in nature…'.[46] While Easttom and Taylor admitted that in each of these cases the approximate amount that a victim lost is under $5,000, which they viewed as relatively small in scale, they emphasised that this 'still amount to billions of dollars annually in losses…' which is a significant problem according to them.[47]

The findings of US Federal Trade Commission in 2005 are consistent with numerous reports and statistics that show that identity thefts that involve financial motivations are affecting a large number of victims and causing huge losses around the world. Most recently, the National Fraud Authority Report in 2013 estimated that identity thefts that involve financial motivations cost the UK economy about 3.3 billion British pounds during 2012. It was also estimated by the same report that around 4.3 million people in the UK fall victim to identity fraud, with 2.7 million individuals actually losing on average 1,203 British pounds each in 2012.[48] In the same year, 2013, the Javelin Strategy and Research Report estimated that the number of identity fraud victims in the US reached 12.6 million persons in 2012. It also

[40] Facebook, 'About' <https://www.facebook.com/facebook/info> accessed 3 November 2013.
[41] Twitter, 'Milestones' <https://about.twitter.com/milestones> accessed 3 November 2013.
[42] The Official Page of Abdulaziz Altarifi at Facebook <https://ar-ar.facebook.com/A.Tarifi.1/posts/394781227219836> accessed 2 November 2013.
[43] Ministry of Health, '"Health Affairs at Jeddah" our "Twitter" Account has been Hacked and we Demand not to Communicate with it' <hemohj.gov.sa/index.php/8-معه-التواصل-بعدم-ونطالب-اختراقه-تم-تويتر-في-حسابنا-جدة-صحة-202/أخبار> accessed 2 November 2013.
[44] Chuck Easttom and Det J Taylor, *Computer Crime, Investigation, and the Law* (Course Technology 2011) 5.
[45] Ibid.
[46] Ibid.
[47] Ibid.
[48] National Fraud Authority, 'Annual Fraud Indicator' (2013) 30 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf> accessed 6 November 2013.

estimated that the total losses by identity fraud were 20.9 billion US dollars for the same year.[49] Like the UK and the US, Saudi Arabia experienced huge losses that resulted from identity theft as it has been estimated that identity thefts that involve financial motivations cost the Saudi economy more than 1.9 billion Saudi Riyal a year.[50]

The argument of Easttom and Taylor, together with the above estimations of huge losses resulting from identity theft that involve financial motivations, highlight two important points that seem to indicate that identity theft involving financial motivations is more dangerous than the non-financial kind. The first point is that identity theft that involves financial motivations is more widespread than the kind that involves non-financial motivations. The second point, and more importantly, is that the consequences of identity theft that involve financial motivations not only cause harm to the victim but also may threaten the economy as whole. Given these features, it could be said that identity theft that does not involve financial motivations seems minor in comparison with that which does involve financial motivations. Thus, it would be reasonable to argue that while both identity theft of financial data and identity theft of non-financial data could lead to harmful consequences for victims, taking the whole picture of the problem into account, the first seems to be more dangerous. On this ground, it seems understandable that the Saudi legislator focused on the first type and makes it as an offence through article 4(2) of the Anti-Cybercrime Law.

5. Transferring and possession materials (data and programs) for the purpose of identity theft

As previously mentioned, although article 4(2) seems to have successfully criminalised obtaining the financial identity-related information of others, it appears that it has failed to criminalise other important acts related to identity theft, in particular, transferring and possessing financial data of others without lawful cause. It is believed that transferring and possessing other people's financial identities without lawful cause involves as much risk to the victim as obtaining the financial details of people. Either way, they lead to the same consequences of abusing the victim's information. As for transferring identity-related information, as has been shown earlier, some offenders who obtain the confidential information of victims may transfer or sell it to other offenders who would then commit unlawful activities using the victims' personal information. As Graham and others have pointed out, such information can be transferred via a website or a closed web forum. Graham and others observed that there are numerous forums where offenders meet to buy and sell confidential financial information. They also remarked that some forums include thousands of members,[51] which is a big number. As for the average price for the illegally obtained financial information, as Graham and others have noted, it ranges from $8 to $100.[52] Ciampa observed that the price of selling credit card details ranges from as little as $2 to $700 per card.[53] As for possessing identity-related information, this includes those who possess other people's personal data in electronic form, and encompasses offenders who obtain the data either through physical means or through using computers.

Some would argue that article 4(2) already covers those who transfer or possess financial identity-related information because they already obtained this information without lawful cause, which is covered by article 4(2) of the Anti-Cybercrime Law. This is true for those who acquire the financial identity-related information of others online, but not for those who acquire this information through physical means. Obtaining financial identity-related information without lawful cause through physical means, as mentioned earlier, is not an offence under the Anti-Cybercrime Law or under any Saudi law. Thus, if

[49] Javelin Strategy and Research, 'How Consumers can Protect against Identity Fraudsters in 2013' (2013) 4 <https://www.javelinstrategy.com/uploads/web_brochure/1303.R_2013IdentityFraudConsumerReport.pdf> accessed 6 November 2013.

[50] Aleqtisadiah Newspaper, 'Increasing Losses of Electronic Crimes' (Riyadh, 10 October 2013) <http://www.aleqt.com/2013/10/10/article_792015.html> accessed 6 November 2013.

[51] James Graham and others (eds), *Cyber Fraud: Tactics, Techniques, and Procedures* (Taylor and Francis Group 2009) 28.

[52] Ibid 34.

[53] Mark Ciampa, *Security + Guide to Network Security Fundamentals* (4th edn, Course Technology 2012) 17.

someone obtains such information through physical means, then sells this information over the Internet, it cannot be said that this act is considered an offence under the Anti-Cybercrime Law. Equally, if someone collects credit card details through physical means and then keeps them in electronic form for the purpose of fraud or to transfer them to others to commit fraud, it cannot be said that s/he has committed an offence under the Anti-Cybercrime Law.

The Anti-Cybercrime Law not only failed to criminalise transferring and possessing financial information of others, but also seems to have failed to criminalise transferring and possessing data and programs that may be used in committing the offence of identity theft, such as a phishing draft or software that may be used for the commission of identity theft. This means that transferring and possessing materials (including data and computer programs) with the intention of using them to commit identity theft is not an offence under Saudi law.

A number of countries have recognised the problem of transferring and possessing both data and programs that may be used for committing an offence and have therefore embedded provisions that criminalise these activities. For example, the UK Fraud Act 2006, section 6, makes it an offence to possess an article for use in the course of or in connection with fraud. In addition, section 7 makes it an offence to make, adapt, supply or offer to supply an article knowing that it is designed or adapted for use in the course of or in connection with fraud, or it is intended to be used to commit or assist in the commission of fraud. Section 8 makes it clear that 'article' includes 'any program or data held in electronic form'. Methods of committing the offence as suggested by Crown Prosecution Service (CPS) include lists of credit card numbers, draft emails for use in advance fee frauds, phishing emails, pharming and use of a Trojan.[54] The Explanatory Notes to the Fraud Act also states that

> Examples of cases where electronic programs or data could be used in fraud are: a computer program can generate credit card numbers; computer templates can be used for producing blank utility bills; computer files can contain lists of other peoples' credit card details or draft letters in connection with 'advance fee' frauds.[55]

It seems clear from the definition of 'article' in section 8 of the Fraud Act 2006, together with the examples provided by CPS and the Explanatory Notes, that the offences of sections 6 and 7 can be applied in a very wide scope and encompass any person who possesses or transfers data or program for the purpose of fraud.

Giving this coverage, the important question to arise is how effective are the offences in practice? This answer is found in a Memorandum to the Justice Select Committee entitled 'Post-Legislative Assessment of the Fraud Act 2006', which mentioned feedback received from the CPS on how the new offences of sections 6 and 7 have been used. As for section 6 (possession of articles for use in frauds), the CPS claimed that this section was useful in bringing more than 2,000 charges of possessing article for use in frauds in 2010 (which is an impressive number). The CPS contended that this offence was particularly useful with criminals who did not dispose the hard drives of computers that contained the fraudulent data in relation to credit cards, mobile phones and SIM cards. The CPS asserted that section 6 was helpful in prosecuting those criminals who possess such types of data on their computers. As for section 7 (making or supplying articles for use in frauds), the CPS alleged that it was able to bring 284 charges under this section in 2010. While the CPS admitted that the 284 charges might be a small number (perhaps in comparison with the charges brought under section 6), it maintained that this was significant on the basis that section 7 had been used in serious credit card fraud cases. The CPS also added that section 7 is also helpful in dealing with cases where hard drives contain preparatory documents and where the victim is unable to provide the required assistance in the investigation.[56]

From the highlighted weaknesses of the legal responses to identity theft in Saudi Arabia as presented above and supported with an example that showed how legal measures adopted in the UK were helpful for the UK prosecutors in handling transferring and possessing articles for use in frauds, it would be

---

[54] The Crown Prosecution Service, 'Possession of Articles for Use in Fraud' <http://www.cps.gov.uk/legal/s_to_u/sentencing_manual/possession_of_articles_for_use_in_a_fraud/index.html> accessed 30 October 2013.

[55] Explanatory Notes to the Fraud Act 2006, 5.

[56] Ministry of Justice, *Post-Legislative Assessment of the Fraud Act 2006: Memorandum to the Justice Select Committee entitled* (June 2012) 7.

reasonable to recommend that the Saudi law needs to be strengthened in order to combat the offence of identity theft, by criminalising transferring and possessing materials (data and programs) for the purpose of identity theft.

However, it should also be noted that such efforts to criminalise this form of identity theft would need to overcome a number of challenges. The first important challenge to mention here relates to the 'dual use' nature of the materials (data and programs) that may be used for identity theft purposes. Dual-use materials can be used for legitimate ends or for criminal purposes. Thus, there must be a restriction on the offence of transferring and possessing materials (data and programs) to avoid over-criminalisation. Section 6 of the UK Fraud Act 2006, as an example to illustrates this, provides that 'A person is guilty of an offence if he has in his possession or under his control any article for use in the course of or in connection with any fraud'. Bainbridge argued that the offence of section 6 includes 'article' that may be used for legitimate and non-legitimate purposes. An example, as illustrated by Bainbridge, is decryption software, which can be used for both legitimate and non-legitimate purposes. While this software may be used for research purposes, it can also be used to decrypt the passwords of bank accounts. However, Bainbridge asserted that the offence of possession can only be applied if the accused intended for the 'article' (in this example the software) to be used in the course of or in connection with a fraud,[57] which seems to exclude legitimate usage of articles.

Another concern relates to the meaning of 'possession', which could raise various challenges when it comes to application. Such challenges emerged in the UK Fraud Act 2006, section 6. Ormerod, when discussing the term 'possession' in section 6, raised several possible challenges in this regard. The first relates to personal possession. Ormerod wondered if it were possible for possession to be committed through an intermediary. He asked, would a person be liable for committing possession if the software is held on his teenage son's computer, or does the employer possesses software if it is located on his employee's computer? While Ormerod noted that such questions may be thought to be related to 'control' by the accused if it is to be considered within the offence at all, he emphasised that section 6 does not stipulate that the possession is exclusively for personal possession and not through an intermediary.[58]

Another possible challenge raised by Ormerod in relation to 'possession' under section 6 of the UK Fraud Act relates to jurisdiction. Ormerod wondered whether an accused possesses data if those data are only stored in the server of another jurisdiction and can be accessed through the Internet.[59]

Perhaps the most notable possible challenge raised by Ormerod regarding possession under section 6 of the UK Fraud Act relates to the situation where the accused claims that s/he has deleted the related data or software in question, and thus it is no longer under his or her possession although it can be retrieved by an expert.[60] A very good example which presents this challenge is the UK case of *R v Porter*[61] where the defendant had deleted indecent images of children from his computers. In this case, the defence claimed that none of the deleted images were in his possession because he had done all that he could do to divest himself of possession by placing them in the recycle bin, which he had then emptied. While the deleted images were recoverable by experts, the court accepted the defendant claim and expressed the view that in the special case of deleted images from a computer, a person no longer has custody or control if s/he cannot retrieve or gain access to these images. The court argued that once a person has deleted images, s/he has put them beyond his or her reach in a similar way to a person who destroys or gets rid of a hard copy photograph. On this ground, the court decided that it cannot be said that a person who cannot retrieve an image from a hard disk drive is in possession of the image just because the hard disk drive and the computer are in his possession.

The questions that Ormerod raised in relation to section 6 of the UK Fraud Act 2006, together with the case of *Porter*, reflect the fact that criminalising possession of electronic material is not an easy task. Therefore, the Saudi legislator needs to pay particularly close attention when criminalising possession of materials in relation to identity theft, if it is to be criminalised at all, to ensure the minimising of possible

---

[57] David Bainbridge, 'Criminal Law Tackles Computer Fraud and Misuse' [2007] Computer Law and Security Report 276, p.278. See also Jacqueline Martin and Tony Storey, *Unlocking Criminal Law* (3rd edn, Routledge 2013) 433.

[58] David Ormerod, *Smith and Hogan's Criminal Law* (13th edn, Oxford University Press 2011) 915.

[59] Ibid.

[60] Ibid 917.

[61] *R v Ross Warwick Porter* [2006] EWCA Crim 560 (UK). See also David Ormerod, *Smith and Hogan's Criminal Law* (13th edn, Oxford University Press 2011) 917.

legal challenges that would emerge from the way the offence of possession is drafted. The most important thing to be clearly addressed relates to deleted materials. This is because almost all computer users practice deleting materials on regular basis, and thus any computer that is brought in for criminal investigation most likely includes deleted materials, which could be linked in one way or another to the offence in question or even other offences. This means that the challenge of deleted materials might emerge in the majority of cases. Several important points need to be clear for the drafter in this regard to minimise possible legal challenges. Among them is the issue of whether the deleted the materials emptied from the recycle bin would still be considered in the possession of the accused on the grounds that he possesses the material on hard disk drive and the material is retrievable? If yes, would this also include the materials that cannot be retrieved by the accused but can be retrieved by an expert? If the accused is an expert and has the skills to retrieve the material, but he does have the required specialist software or the software is unavailable to the public would that be possession?

The final point to mention in this article relates to the Council of Europe Convention on Cybercrime, 2001. One might wonder how such an offence (identity theft), which this paper claims to be a serious offence, is not covered by the Cybercrime Convention, which has been argued to be the most comprehensive international instrument yet to combat cybercrimes.[62] It only covers computer-assisted fraud that causes a loss of property to another person.[63] However, this limit should not be surprising. Schjolberg and Ghernaouti-Helie explained that the 2001 Cybercrime Convention is based on cyber acts that were carried out in the late 1990s. This means that newer, post-2001 methods of committing cybercrime, such as phishing and pharming, are not mentioned in the Convention.[64] This is consistent with the study by Owen, who observed that the first known phishing attack was conducted in 2001 and became widespread in 2004,[65] and Milhorn who observed that one of the first known pharming attacks was carried out in 2005.[66] However, as Gercke remarked, the challenges posed by identity related crimes have later been recognised at the European Union level, in particular by the Commission of the European Union, as a significant issue.[67] The need for legal action is argued by the Commission of the European Union as follows 'It is often easier to prove the crime of identity theft than that of fraud, so that EU law enforcement cooperation would be better served were identity theft criminalised in all Member States',[68] which reflects the recognition of the importance of combating identity-related crimes at the European Union level.

6. Conclusion

There is no doubt that the development of information and communication technologies and the proliferation of the Internet provide criminals with more opportunities to acquire the personal and confidential information of persons, extending the reach of criminals to a global level, putting huge amounts of people's identity-related information at risk. As a legal response, many countries enacted legislation to impose criminal sanctions on identify theft. Among these countries is Saudi Arabia, which enacted the Anti-Cybercrime Law 2007 to handle various harmful activities that occur in cyberspace, including identity theft.

---

[62] Ales Zavrsnik, 'Cybercrime Definitional Challenges and Criminological Particularities' (2008) 2 Masaryk University Journal of Law and Technology 1, 7; Samuel C McQuade (ed), *Encyclopedia of Cybercrime* (Greenwood Press 2009) 35.

[63] Council of Europe Convention on Cybercrime (2001) ETS 185, art 8.

[64] Stein Schjolberg and Solange Ghernaouti-Helie, *A Global Protocol on Cybersecurity and Cybercrime: An Initiative for Peace and Security in Cyberspace* (Stein Schjolberg and Solange Ghernaouti-Helie 2009) 44-45.

[65] Wesley W Owen, *Examining the Effectiveness and Techniques of the Anti-phishing Technology in Leading Web Browsers and Security* (UMI 2008) 2.

[66] H. Thomas Milhor, *Cybercrime: How to Avoid Becoming a Victim* (Universal Publishers 2007)167.

[67] Marco Gercke, 'Legal Approaches to Criminalize Identity Theft' in United Nations Office on Drugs and Crime, *Handbook on Identity-Related Crime* (United Nations 2011) 40.

[68] Commission of the European Communities, 'Communication from the Commission to the European Parliament, the Council and the Committee of the Regions: Towards a General Policy on the Fight against Cyber Crime' COM (2007) 267 final, 8.

It seems clear that article 4(2) of the 2007 Law is capable of encompassing all possible methods of obtaining the personal information of others including phishing, pharming, using malware and hacking. With any of these methods, once the perpetrator attains the financial information of the victims without lawful cause, s/he would be liable for committing an offence under article 4(2), irrespective of whether s/he uses it for further crimes or not. Moreover, the broad meaning of 'attaining' in article 4(2) seems able to encompass any method that might be created in the future to acquire the confidential information of people. However, article 4(2) clearly limits the criminalisation to only attaining information that relates to 'bank or credit data, or data pertaining to ownership of securities'. By this condition, the Anti-Cybercrime Law limits the application of article 4(2) to only identity theft related to financial matters. This means that acquiring the identity-related information of others for non-financial motivations – such as to impersonate another person in order to tarnish his or her reputation – is not an offence under the Anti-Cybercrime Law. However, this paper argued that because the former is more widespread than the later and the former not only causes harm to the victim but also may threaten the economy as whole, it seems understandable that the Saudi legislator focused on the first type and makes it an offence through article 4(2) of the Anti-Cybercrime Law.

The notable weakness in dealing with identity theft under Saudi law is that the Anti-Cybercrime Law has failed to criminalise two other acts related to identity theft, namely transferring and possessing materials (data and programs) for the purpose of identity theft. Thus, the Anti-Cybercrime Law would not be able to deal with those who transfer or sell, for instance, the credit card details of individuals or with those who, for example, possess other people's identity-related information, a clear weakness in combating identity theft under Saudi law. Thus, the Anti-Cybercrime Law needs to criminalise the identity theft of transferring and possessing materials to fill the gap in the existing law, which would strengthen the legal response against this form of cybercrime.

Acknowledgements

The author expresses his gratitude to Professor Clive Walker and Dr. Stefan Fafinski of the Centre for Criminal Justice Studies in the School of Law at the University of Leeds in the United Kingdom for their invaluable feedback and comments.

* * * *

© 2014 Suhail Almerdas This work is licensed under a Creative Commons Attribution-Noncommercial-No Derivative Works.

Cite as: Almerdas, Suhail.The Criminalisation of Identity Theft under the Saudi Anti-Cybercrime Law 2007.*Journal of International Commercial Law and Technology*, Vol.9 Issue 2 (April, 2014)