COPYRIGHT NOTICE

UB ResearchOnline
<http://researchonline.ballarat.edu.au>

Q^} c' A' a ^ A' @ A' @ ^} * ^ • A' A' @ A' ^ * | a a } A' A' ^} c' A' a ^

Published version available at
<http://dx.doi.org/10.1109/E{dgtUge042340846829>:

Copyright 2012 IEEE Personal use of this material is permitted.
Permission from IEEE must be obtained for all other users, including
reprinting/ republishing this material for advertising or promotional
purposes, creating new collective works for resale or redistribution to
servers or lists, or reuse of any copyrighted components of this work in
other works

Identity Crime

The Challenges in the regulation of identity crime

Eric Holm

The Business School, University of Ballarat
PhD Candidate at Bond University
Australia
e.holm@ballarat.edu.au

Abstract— This paper discusses the unique challenges of regulating identity crime. Identity crime involves the use of personal identification information to perpetrate crimes of fraud. As such, the identity crime involves using personal and private information to perpetrate crime. This article considers the two significant issues that obstruct responses to this crime; firstly, the reporting of crime. Secondly the paper considers the issue of jurisdiction. Finally, the paper explores some responses to this crime. The paper then explores some of the current responses to identity crime.

Keywords—identity crime, regulation, online fraud, jurisdiction, personal information.

I. INTRODUCTION

Certain information is worth money whereas other information is quite worthless [1] in terms of a monetary value particularly when it comes to crimes involving identity. The information that is valuable to the identity criminal is that which can be converted into gain, typically by way of frauds [2]. Certain information, particularly personal identification particulars provide opportunity for identity criminals to either obtain credit under false pretences or to impersonate another for similar purposes. Personal identification particulars include; social security details, drivers licence details, passport as well as others [2]. Hence, the crime of stealing identity particulars may be the catalyst for a number of crimes that follow. The offences arising can include fraud, deception, laundering, organised crime and even acts of terrorism [2]. The losses attributable to identity crime can be measured by monetary losses through fraud [3] but as mentioned, there are a number of offences that can be committed once the information is stolen. In Australia it has been suggested that identity crime is one of the most prominently emerging types of fraud [4]. Although one of the challenges of recording crime in Australia is that identity crimes are subsumed into recorded incidence of fraud [5]. The misreporting of crime tends to distort the reliability of data that pertains both to fraud and also identity crime [6].

II. THE DIRECT AND INDIRECT COSTS OF IDENTITY CRIME

The direct costs of identity crime in Australia are estimated at \$5.88 billion per year [7]. The most significant implication of this crime is financial [8]. As far back as 2006, the losses

arising from identity crime in the United Kingdom economy were \$1.7 billion [9]. This latter figure took into account the preventative measures as well as the costs associated with the prosecution of cases. In both instances the losses attributable to identity crime are significant.

In terms of losses arising from this crime, there are also many indirect costs arising from identity crime. These costs involve injury to reputation as well as potential damage to share prices and other hidden costs to business relations [10]. While the direct costs are more easily quantifiable, the indirect losses are more difficult to measure. For instance, a cost scarcely considered in the literature is the indirect and hidden costs to victim's psychology and emotions [11]. Such indirect costs are scarcely measured and difficult to quantify and certainly add to the costs of identity crime.

III. WHO ARE THE VICTIMS?

Identity fraud is reliant upon information [12]. Much of this information is availed from the Internet, particularly through information sales. Further, a study conducted in the United States on identity fraud found that the most common method used for obtaining information was to purchase information over the Internet [13]. However, information is also obtained by other means also like through spams, scams and phishing [14] amongst others.

There is some debate as to whether identity crime is more prominent on Internet [15] or not. Interestingly, some components of this crime may take place offline and others offline [16]. However, an important reason why identity crimes take place on the Internet is that there is a significant amount of personal identification information on the Internet as well as potential targets [17].

While the storage of information itself does not always present vulnerability for identity crime, it is rather the way in which information can be used that can be. The exposure to risk of an individual computer user online is arguably dependent upon the behaviour of the computer user [18]. Furthermore, it is argued that the decision to purchase items on the Internet is associated with exposing oneself to greater risks [19]. However,

conversely there is a latent risk that resides for all computer users connected to the Internet. Indeed, the greater the personal information that resides on the Internet, the greater potential for information misuse. Interestingly, the information that is on the Internet may be provided by the individual, exchanged by corporations as well as transferred by various other means and reasons for information exchange [20]. Therefore it is the exchange of certain information that presents risks such as, passports, birth certificates, immigration documents, driver's licences and social security cards [21]. In regard to the responding to identity crime these are challenged by two key issues. The first issue relates to issues of jurisdiction. The second issue relates to the difficulty in quantifying the cost associated with identity crime. These will now be discussed in turn.

IV. THE ISSUE OF JURISDICTION

It is clear that there is no central body controls information dissemination on the Internet. The Internet itself, as a dispersed body covers various jurisdictions and consequently there are a number of practical difficulties in regard to investigating and convicting identity criminals and many of the practical difficulties are amplified by dispersed nature of the Internet and also the tendency of the Internet to cut across jurisdictions [22].

The responses to identity crime vary due to the various different cultural beliefs and values internationally [23]. These influence the way in which identity crime is viewed, but this is also problematic as identity crimes are mostly dealt with through domestic mechanisms. Therefore, for the response to be effective it requires a regulatory response that appropriate domestic responses to be effective.

Given that mostly responses would be through criminal sanction, the issue around jurisdiction stem from determining the ability of the state to bring an action against this person. Historically, the effects doctrine has been adopted as a way to justify a state taking action against the individual [24]. This doctrine applies where the harm is linked to the state [24]. This approach has been utilised as a justification for which an action to apply criminal sanctions may be taken [25].

The significance of this doctrine is that that this provides for jurisdiction to be exercised by a state outside its physicality and jurisdiction [26]. For identity crime, this would result in a state being able to take action against an offender in another state provided it can be ascertained that such an offender caused an effect upon the domestic territory [27]. The application this effects doctrine has been seen to be effective in past cases in such cases like the Lotus case [28]. While this case was not related to identity crime the case certainly represented a way in which a state may enforce domestic sanctions outside its jurisdiction.

V. THE ISSUE OF RELIABLE DATA

Conservatively there are significant costs associated to identity crime that can be estimated at tens of billions of dollars [29]. However, it is difficult to gather an accurate view of the total cost attributable to identity crime because it is not easily quantified due to the way losses are recorded and many identity crimes are not reported. For instance, in Australia, the Australian Bureau of Statistics (ABS) suggests that 43 per cent of victims of crimes involving credit and bank cards were prepared to report this crime to police [30]. This suggests that there is a significant proportion of identity crime that is not reported to authorities [31]. This non-reporting of crime distorts statistics on the incidence of identity crime.

As there is no central repository of data pertaining to identity crime, the data that is available is through various dispersed sources, including law enforcement as well as government agencies. Therefore it is difficult to obtain an accurate measure of the true incidence of identity crime due the varied approaches to reporting and recording this crime. In this regard, a central repository of information that pertains to victimization would be most useful [32].

The impact of identity crime in relation to indirect costs is scarcely measured and there is limited data available regarding the complete costs of this [33]. The costs associated with the preventative measures [34] need to be considered when measuring the impact of this crime. This has been referred to as the difference between financial cost and other costs. The first of these costs can be easily quantified and the latter not so easily determine [35]. Nonetheless, the implication of incorrect measurements of such costs is incorrect responses to crime. Therefore, ultimately the dispersed nature of reporting as well as the difficult to measure indirect costs makes this an issue in responding to identity crime.

VI. THE RESPONSES TO IDENTITY CRIME

A. Regulatory responses

Regulatory responses to identity crime will always face challenges due to the dispersed nature of the Internet and the challenges with jurisdiction. Therefore, it is difficult to know if greater regulation in regard to identity crime will make any difference. Furthermore, it remains difficult to measure the effectiveness of regulatory responses with such issues pertaining to the reliability of data.

Self-regulation has been adopted within industry as a way to regulate the behaviour that occurs and therefore controls undesirable behaviours through internal sanction [31]. For identity crimes, the two specific types of self-regulation have had an impact relate to self-regulation of the Internet as well as the self-regulation of financial institutions.

While self-regulation has been used in an industry context to regulate behaviour, these industry based initiatives seldom directly apply to identity crimes but rather tend to influence the standards of behaviour which have some relationship to this

crime. Such a relationship is difficult to quantify but proves to be critical for reasons beyond this discussion of identity crime.

B. Technological responses

One of the significant vulnerabilities of Internet transactions is the difficulty of the person transacting to verify the identity of the person with whom you are sharing information. This is particularly evident with electronic payment transactions [36]. However, authentication provides a way of identifying an individual [37]. In terms of a technological response, this approach provides a way of verifying the identity of the person with whom one transacts which is critical for Internet based interaction [38]. Likewise encryption is a technological solution that is worthy of mention here as a way of protecting data transfer [38]. However, as with the most sophisticated responses, these can be circumvented by the most sophisticated techniques [39].

C. Education as a response

There seems to be a lack of knowledge regarding vulnerabilities when it comes to data. It has been suggested that a key weakness in cyber security is the human factor [40]. Furthermore, there are behavioural factors that play an influence in the way in which individuals exchange information on the Internet. Therefore it is important to understand these [41] and to work on enhancing knowledge of the vulnerabilities. However the educative process should not work in isolation as each response to crime is, in part reliant upon the other response to provide an influence on the incidence of identity crime.

VII. CONCLUSION

In reflecting back on the title of this paper, it is clear that there are challenges in responding to identity crime. However it is difficult to determine an appropriate response to this crime with issues such as the non-reporting of crime as well as the reliability of data regarding this crime. These issues are quite separate from those pertaining to jurisdiction that influences any regulatory response to this crime. Nevertheless, the catalyst for change will need to come from an accurate reported incidence of this crime. Without accurate reporting it will remain impossible to determine if the responses in place, as diverse as they might be are actually adequate.

There are a number of practical difficulties in regard to regulating identity crime. Foremost there is the issue of jurisdiction [22]. Thereafter, there are the issues that relate to the accuracy of data both through the reported incidence of this crime as well as through the non-reporting of crime. With regard to responses to crime these must be based on the existence of data and when the data is inaccurate then the responses appropriateness comes into question.

REFERENCE LIST

- [1] Forester, T., Morrison, P.: *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*. MIT Press, Boston MA (1994).
- [2] Saunders, K., Zucker, B.: Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act., *Cornell Journal of Law and Public Policy* 8, 661-666 (1999).
- [3] State of New Jersey Commission of Investigation and the Attorney General of New Jersey <http://csrc.nist.gov/publications/secpubs/computer.pdf>
- [4] Queensland Police Fraud Investigative Group, <http://www.police.qld.gov.au/Resources/Internet/services/reportsPublications/documents/page27.pdf>
- [5] Australian Institute of criminology <http://www.aic.gov.au/publications/current%20series/tandi/381-400/tandi382.aspx>.
- [6] Grabosky, P., Smith, R., Dempsey, G.: *Electronic theft: unlawful acquisition in cyberspace*. Cambridge: Cambridge University Press, United Kingdom (2001).
- [7] Smith, R.: Addressing Identity-related. Trends and Issues in Crime and Criminal Justice (2003)
- [8] Lynch, J.: Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks. *Berkeley Technology Law Journal* 20, 266-67 (2005).
- [9] Home Office Identity Fraud Steering Committee <http://www.identitytheft.org.uk/faqs.asp>
- [10] PriceWaterhouse Coopers, http://www.pwc.com/gx/en/economic-crime-survey/pdf/pwc_2003gecs.pdf
- [11] Black, P.: Phish to fry: responding to the phishing problem. *Journal of Law and Information Science* 73, 73-91 (2005).
- [12] Department of Justice, Office of Community Oriented Policing Services <http://www.cops.usdoj.gov/files/ric/Publications/e05042360.txt>
- [13] Anderson, K.: Who are the victims of identity theft? The effect of demographics *Journal of Public Policy and Marketing* 25, 160-171 (2006).
- [14] Australian Competition and Consumer Commission, <http://www.accc.gov.au/content/item.phtml?itemId=816453&nodeId=ef518e04976145ffed4b13dd0ecda1a6&fn=Little%20Black%20Book%20of%20Scams.pdf>.
- [15] Public Interest Advocacy Centre (2003) <http://www.travel-net.com/~piacca/IDTHEFT.pdf>
- [16] Organisation for Economic Development <http://www.oecd.org/dataoecd/35/24/4064>
- [17] Quirk, P., Forder, J.: *Electronic Commerce and the Law*. John Wiley & Sons Australia, Ltd, Milton, Qld (2003).
- [18] Copes, K., Kerley, K., Huff R., Kane, J.: Differentiating identity theft: An exploratory study of victims using a national victimization survey. *Journal of Criminal Justice* 38, 1045-1052 (2010).
- [19] Bossler, A., Holt, T.: The effect of self-control on victimization in the Cyberworld. *Journal of Criminal Justice* 38, 227-236 (2010).
- [20] Australian Office of the Australian Information Commissioner <http://www.privacy.gov.au/faq/smallbusiness/q2>
- [21] Public Safety Canada, <http://www.publicsafety.gc.ca/prg/le/bs/report-eng.aspx>
- [22] Smith, R.: Examining Legislative and Regulatory Controls on Identity Fraud in Australia. In: *Proc. 2002 Marcus Evans Conferences*, pp.7-12, Sydney (2002).
- [23] Towell, E., & Westphal, H.: *Investigating the future of Internet regulation* 8, 26-31 (1998).
- [24] Coppel, J.: A Hard Look at the Effects Doctrine of Jurisdiction in Public International Law. *Leiden Journal of International Law* 6, 73-90 (1993).
- [25] *United States v. Aluminum Co. of America*, 148 F.2d 416, 444 (2d Cir. 1945).
- [26] *Hartford Fire Insurance Co. v. California*, 113 S. Ct. 2891 (1993)
- [27] *Gencor Ltd v. Commission* [1999] ECR II-753 at paras. 89-92.
- [28] *The Lotus Case (France v Turkey)* PCIJ Rep (1927).
- [29] Willox, N., Regan, T.: Identity fraud: Providing a solution. *Journal of Economic Crime Management* 1, 1-15 (2002).
- [30] Australian Bureau of Statistics, [http://www.ausstats.abs.gov.au/Ausstats/subscriber.nsf/0/866E0EF22EFC4608CA2574740015D234/\\$File/45280_2007.pdf](http://www.ausstats.abs.gov.au/Ausstats/subscriber.nsf/0/866E0EF22EFC4608CA2574740015D234/$File/45280_2007.pdf)
- [31] National Consumer Council http://www.talkingcure.co.uk/articles/ncc_models_self_regulation.pdf
- [32] Organisation for Economic Cooperation and Development, <http://www.oecd.org/dataoecd/49/39/40879136.pdf>
- [33] Australian Institute of Criminology, <http://www.aic.gov.au/documents/A/A/3/%7BAA329573-5D62-46FB-9E6F-4D86A6DDDD9BC%7Dt247.pdf>
- [34] Sullivan, R.: Payments Fraud and Identity Theft?. *Economic Review* 3, 36-37 (2008).

- [35] Lucas, R.: *The FACT Act's hidden costs Credit Card Management* 17, 52. (2004)
- [36] Barker, K., D'Amato, J., Sheridan, P.: Credit card fraud: awareness and prevention. *Journal of Financial Crime* 15, 398-410 (2008).
- [37] Morrison, R.: Commentary: Multi-Factor Identification and Authentication. *Information Systems Management* 24, 331-332 (2007).
- [38] O'Farrell, N., Outllet, E., Outllet, E.: *Hack Proofing your wireless network*. Syngress Publishing, Rockland, MA (2002).
- [39] Broadhurst, R., Grabosky, P.: Computer-related Crime in Asia: Emergent Issues. In: Broadhurst, R., Grabosky, P. (eds) *Cyber-Crime: The Challenge in Asia*, Hong Kong University Press, Hong, pp.1-26. (2005)
- [40] Symantec,
http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf
- [41] Stajano, F.: Understanding Scam Victims: Seven Principles for Systems Security. *Communications of the ACM* 44, 70 (2011).