Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Addressing identity crime in crime management information systems: Definitions, classification, and empirics

Rodger Jamieson [a], *Lesley Pek Wee Land* [a], *Donald Winchester* [a], *Greg Stephens* [a], *Alex Steel* [b], *Alana Maurushat* [b], *Rick Sarre* [c]

[a] *The Australian School of Business, School of Information Systems, Technology and Management, University of New South Wales, Australia*
[b] *Faculty of Law, University of New South Wales, Australia*
[c] *School of Commerce, the University of South Australia, Australia*

Keywords:
Identity crime
Identity fraud
Identity theft
Identity deception
Computer crime
Internet
Information systems security (ISS)
Taxonomy
Personnel identifying information (PII)
Crime management information systems

ABSTRACT

Identity fraud as a term and concept in its formative stages was often presumed to be identity theft and visa versa. However, identity theft is caused by the identities (or tokens) of individuals or organisations being stolen is an enabling precursor to identity fraud. The boundaries of identity fraud and identity theft are now better defined. The absence of specific identity crime legislation could be a cause of perpetrators not classified as breaching identity crimes but under other specific entrenched law such as benefit fraud, or credit card fraud. This metrics overlap can cause bias in crime management information systems. This study uses a multi-method approach where data was collected in both a quantitative and qualitative manner. These approaches are used as a lens for defining different classes of online identity crimes in a crime management (IS) security context. In doing so, we contribute to a deeper understanding of identity crime by specifically examining its hierarchical classes and definitions; to aid clearer structure in crime management IS. We seek to answer the questions: should current law around identity fraud continue to be reinforced and measures introduced to prevent identity crime; should laws be amended; or should new identity crime laws be constructed? We conclude and recommend a solution incorporating elements of all three.

1. Introduction

The illegal online use or trade in identities of individuals and organizations is recognized to have a substantial influence on other crimes such as frauds and money laundering; seriously impacting the real economy.[1] The global economic cost of these identity crimes was estimated to be "US$2 trillion in 2005".[2] In the United States the annual estimated cost of identity crime alone in 2009 was "US$54 billion".[3] These survey figures may not reflect the actual figures if real cases were to be analysed.[4] A major concern with the costing of identity crimes is the potential bias, error, and lack of

[1] Goode, S., and Lacey, D. 2010 "Detecting Complex Account Fraud in the Enterprise: The Role of Technical and Non-Technical Controls", Decision Support Systems. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., and Sun, X. 2011. "The Application of Data Mining Techniques in Financial Fraud Detection: A Classification Framework and an Academic Review of Literature", Decision Support Systems (50:4) or (50), pp. 559–569.
[2] Hurley, J., and Veytsel, A. 2003. "Identity Theft: A $2 Trillion Criminal Industry in 2005", The Aberdeen Group 13 May, p. 1.
[3] Miceli, D., and Kim, R. 2010. "2010 Identity Fraud Survey Report: Consumer Version", Javelin Strategy & Research February, p. 5.
[4] For example, the Uniform Crime Reports have different statistics than the National Crime Victimisation Surveys in the US. See Chen, H., Schroeder, J., Hauck, R. V., Ridgeway, L., Atabakhsh, H., Gupta, H., Boarman, C., Rasmussen, K., and Clements, A. W. (2002). "COPLINK Connect: Information and Knowledge management for Law Enforcement", Decision Support Systems (34), pp. 271–285.

0267-3649/$ – see front matter © 2012 Rodger Jamieson, Lesley Pek Wee Land, Donald Winchester, Alex Steel, Alana Maurushat, Greg Stephens, and Rick Sarre. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2012.03.013

consistency in how they are defined and classified.[5] As crime management information systems (IS) transition from paper-based to digital systems to ease storage and aid retrieval (often remotely for law enforcement), there is an emergent need to classify the fields accurately.[6]

The US leads the way in criminalizing identity crime and data breaches.[7] (IS) security research focuses on computer abuse, computer crime, and computer-related crimes. Computer crimes include "crimes whereby the computer is the target or the mechanism for committing the crime or the computer user is the target. It also includes crimes committed over the Internet or where the Internet plays a role in the commission of the crime" (see Table 6).[8] Online identity crimes are linked to computer abuse, computer crime and computer-related crime in IS security, because they are enabled by computers and/or the Internet. A difference is that identity crime involves social engineering of people and technology.

The ubiquity of information technology; computers, the Internet, mobile devices, and their interconnectedness in a digital economy enables the increase of identity crime methods, such as phishing, not previously accounted for by computer crime and abuse in IS research.[9] Internet users reached the 2 billion mark in January 2011.[10] Smart perpetrators are devising increasingly sophisticated ways of committing identity crimes. Therefore classes of IS-enabled abuse, such as identity crime, continue to evolve often ahead of IS security innovations.[11]

The remainder of this paper is structured as follows. The next section discusses the methodology.[12] Then we identify the various definitions of identity crime and discuss our results. The final sections discuss the contributions, implications, limitations, conclusion and future research in this area.

2. Methodology

We use a multi-method research design consisting of qualitative methods and quantitative methods via secondary data to investigate how identity crime terms are defined and how the categories shape organizational actions for measuring and improving IS security to reduce identity crimes.[13] We collected qualitative data from Australia via 10 face-to-face interviews and two by teleconference in 2002. In 2002 Australia had no legislation that specifically targeted identity crime and this was a unique out-of-sample setting to study identity crimes as other jurisdictions such as the United States had enacted identity crime legislation. We also gathered data from communications with Attorney Generals and Crime Collection agencies until 2010 from many countries. All qualitative data has been continuously updated from secondary sources. From our interview transcripts, we derived themes using NVivo qualitative software.[14] The data was collected from Attorney General's departments and Government Statistics Agencies from Australia (Federal and States), Canada, European Union, Ireland, Netherland, United Nations, United Kingdom, and the US (Federal and States). The data was based on questions of identity crime definitions and their crime classification systems in use. We also obtained conditional access to the ABS Personal Fraud data collection to reclassify their identity crime data[15] for our empirical quantitative identity crime data testing, using our definitions and classification.

Interviewees were drawn from diverse industries such as banks, retailers, telecommunications, utilities, State Government licensing authorities, Federal Government agencies (welfare, immigration), and a US academic/criminologist for insights from the US. The organizations selected for interviewing represented those most targeted by identity crime perpetrators. Their credibility can be attested by the senior positions they held for instance in fraud, fraud management, compliance, and/or internal auditing. Some of the interviewees were previously employed in law enforcement or the legal profession. The interview instrument contained mainly 13 questions. Each interview lasted approximately one and a half hours. Interviewee recordings were professionally transcribed, checked for reliability and accuracy, and corroborated by members of the research team. The rich data and information gathered via email correspondence and/or telephone

[5] Romanosky, S., Telang, R., and Acquisti, A. 2008. "Do Data Breach Disclosure Laws Reduce Identity Theft?", Carnegie Mellon University pp. 1–30.

[6] Chen, above note 4. See also Orlikowski, W. J., and Iacono, C. S. 2001. "Research Commentary: Desperately Seeking the "IT" in IT Research – A Call to Theorizing in the IT Artifact", Information Systems Research (12:2), pp. 121–134, and Sproule, S., and Archer, N. 2007. "Defining Identity Theft", IEEE Computer Society, Eighth World Congress on the Management of eBusiness pp. 1–11.

[7] Romanosky, above note 5. See also Maurushat, A., "Data Breach Notification Law Across the World from California to Australia" Privacy Law and Business International, April, 2009.

[8] Douglas, J. E., Burgess, A. W., Burgess, A. G., and Ressler, R. K. (Eds. 2nd edition). 2006. Crime Classification Manual, San Francisco, CA, Jossey-Bass. Parker, D. B. 1976. Crime by Computer. New York, Charles Scribner's Sons.

[9] Bryant, R. (Ed.) 2008. Investigating Digital Crime. England, John Wiley & Sons Ltd.

[10] Statement of ITU Secretary General, Dr. Hamadoun Toure, January 26, 2011 available at http://www.who.int/topics/millennium_development_goals/accountability_commission/ITU_SG_statement_26Jan2011.pdf.

[11] Biegelman, M. T. (ed.) 2009. Identity Theft Handbook: Detection, Prevention, and Security. John Wiley & Sons, Inc. *See also* Berg, S. 2008. "Preventing Identity Theft Through Information Technology", in Perspectives on Identity Theft, M. M. McNally, and G. R. Newman (Eds.), Crime Prevention Studies, (23), pp. 151–167. Monsey, NY, U.S.A., Criminal Justice Press.

[12] McKelvey, B. 1982. Organizational Systematics: Taxonomy, Evolution, Classification. Berkeley, CA. University of California Press. *See also* Stuessy, T. F. (2nd edition) 2009. Plant Taxonomy: The Systematic Evaluation of Comparative Data. New York, Columbia University Press.

[13] Ashakkori, A., and Teddlie, C. 1998. Mixed Methodology: Combining Qualitative and Quantitative Approaches. Thousand Oaks, CA, Sage Publications. Corbin, J., and Strauss, A. 1990. "Grounded Theory Research: Procedures, Canons, and Evaluative Criteria", *Qualitative Sociology* (13:1), pp. 3–21. Glaser, B. G., and Strauss, A. L. 1967. The Discovery of Grounded Theory. Chicago: Aldine.

[14] QSR NVivo. 2008. Version 2.0. Melbourne, Australia, QSR International Pty. Ltd.

[15] Australian Bureau of Statistics. 2008a. 4528.0 Personal Fraud 2007. Australian Bureau of Statistics, June, pp. 1–40.