eJournal of Tax Research vol. 16, no. 3, pp. 578-593

Identity theft and tax crime: has technology made it easier to defraud the revenue?

Mathew Leighton-Daly*

Abstract

The modern phenomenon of online applications and processes mean that there is greater opportunity than ever before to defraud both the revenue and others, based on identity theft. This article focuses on Strike Force Apia, a significant financial crime investigation and subsequent prosecution to identify financial crime typologies relating to the revenue and taxpayer information. The article analyses the detection of financial crime, including by technology-enabled processes, and considers how effectively existing procedural law and criminal offence legislation can facilitate detection, investigation and prosecution. The article concludes that while technology has created new opportunities to defraud the revenue, detection and investigations technology coupled with existing law surrounding the proof of data, means that appropriately resourced organisations, including the Australian Taxation Office, can counter even the more sophisticated attempts to defraud the revenue and third parties based on taxpayer information.

Key words: tax administration, tax evasion, crime, identity fraud

* School of Law, University of Wollongong.

1. INTRODUCTION

The modern phenomenon of online applications and processes mean that there is greater opportunity than ever before to defraud both the revenue and others, based on identity theft. Criminals have always exploited technology. The modern technology-enabled environment, however, facilitates fraudsters not only stealing taxpayer information but also using such information to obtain a financial advantage from other persons (including financial institutions) in ways that were previously not possible. Modern applications and other online processes are such that fraudsters can coordinate schemes without ever showing their faces in the traditional sense. This creates new opportunities for fraud both directly upon the Australian Taxation Office (ATO) and also using taxpayer information to obtain a financial advantage from others based on that information.

This article focuses on a significant financial crime investigation and subsequent prosecution (Strike Force Apia - the largest New South Wales Strike Force in relation to mortgage fraud based on *inter alia* alleged false income tax returns)[1] to identify some financial crime typologies relating to the revenue and taxpayer information. The article focuses on the detection of financial crime including by technology-enabled processes in light of the case study. By reference to the current procedural law and criminal offence regime the article then considers how effectively existing legislation can facilitate detection and investigation and prosecution in the context of dynamic developments in technology.

2. UNDERSTANDING FINANCIAL CRIME

Sutherland, who was famous for coining the concept of 'white-collar crime' also developed the 'differential association' theory,[2] which introduced the concepts of rationalisations and opportunities in an attempt to explain criminal behaviour:

1. Criminal behaviour is learned; it is not inherited, and the person who is not already trained in crime does not invent criminal behaviour.
2. Criminal behaviour is learned through interaction with other people through the processes of verbal communication and example.
3. The principal learning of criminal behaviour occurs with intimate personal groups.
4. The learning of crime includes learning the techniques of committing the crime and the motives, drives, rationalisations and attitudes that accompany it.

A person becomes delinquent when they satisfy more of the definitions (or personal reactions) favourable to the violation of the law than to abide by the law.

This theory ultimately led to the development of the 'fraud triangle', by Cressey, a student of Sutherland.Cressey defined the fraud problem as a 'violation of a position of

[1] New South Wales Police Force, 'Field Operations: Police Officer of the Year', *Police Monthly* (November 2014) 22. *R v Terrence Reddy Adam Eli Meyer* (2011/00220791; 2011/00249266), Reddy Statement of Agreed Facts (unsigned). It is noted that the writer appeared for one of the accused persons (Terrence Reddy) in relation to some of his charges. This analysis is limited to documents on the Court file.
[2] Edwin H Sutherland and Donald R Cressey, *Criminology* (Lippincott, 1978).

financial trust' that the fraudster originally took in good faith.[3] He went on to argue that trusted persons become trust violators when they conceive of themselves as having a financial problem that is non-sharable, are aware that this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their contacts in that situation verbalisations which enable them to adjust their conceptions of themselves as users of the entrusted funds or property. (In other words, theyare able to rationalise their dishonest actions, and so they are not – in their minds – acting inconsistently with their personal codes of conduct.)

The fraud triangle is a framework designed to explain the reasoning behind a fraudster's decision to commit fraud. It has three stages (categorised by the effect on the individual) of: (1) pressure; (2) opportunity, and (3) rationalisation. Pressure may stem from financial issues, health issues, blackmail, psychological issues, lifestyle dependency or greed. Opportunity is present when the fraudster identifies and takes advantage of circumstances in order to obtain personal gain. Rationalisation is used to placate the fraudster's feelings of guilt or criminality. The fraud triangle has been the subject of a great deal of discussion since its conception.

Notably, Wolfe and Hermanson[4] suggest that the fraud triangle could be improved (and thus expanded and explained as a fraud 'diamond') by considering a fourth element, capability. This means, in explaining whether a fraud might occur, the personal traits and abilities of the fraudster coincide with the other three elements of pressure, opportunity and rationalisation. Cressey's fraud triangle has also been the subject of analysis, notably, by Free,[5] who has reviewed popular frameworks used to examine fraud (including the fraud triangle) and earmarked three areas where there is considerable scope for academic research to guide and inform important debates within organisations and regulatory bodies: (i) rationalisation of fraudulent behaviours by offenders; (ii) the nature of collusion in fraud, and (iii) regulatory attempts to promote whistle blowing.[6]

The fraud triangle and fraud diamond are applied below to support the analysis of the effectiveness of existing legislation.

2.1 Case study – Strike Force Apia

Case studies are useful in understanding financial crime. In its compliance guide, AUSTRAC encourages reporting entities to read its published case studies to assist them understand their reporting obligations and thus counter financial crime.[7] However, in analysing the methods and extent of technology-enabled financial crime, non-conviction-related data may need to be treated more carefully than data obtained following a criminal trial (noting the rules of evidence and procedures relating to the

[3] Donald Cressey, 'Why Do Trusted Persons Commit Fraud? A Social-Psychological Study of Defalcators' (1951) 92(5) *Journal of Accountancy* 576; Donald Cressey, *Other People's Money, A Study in the Social Psychology of Embezzlement* (Patterson Smith, 1953) 973.

[4] David Wolfe and Dana Hermanson, 'The Fraud Diamond: Considering the Four Elements of Fraud' (2004) 74(12) *CPA Journal* 38.

[5] Clinton Free, 'Looking Through the Fraud Triangle: A Review and Call for New Directions' (2015) 23(2) *Meditari Accountancy Research* 175; Clinton Free and Pamela Murphy, 'The Ties that Bind: The Decision to Co-Offend in Fraud' (2015) 32(1) *Contemporary Accounting Research* 18.

[6] Free, 'Looking Through the Fraud Triangle', above n 5.

[7] AUSTRAC, *Compliance Guide*, available at: http://www.austrac.gov.au/book/export/html/462 (accessed 11 January 2019).

reliability of facts adduced in criminal proceedings and the criminal standard of proof being beyond a reasonable doubt). By the same token, where a jury has found an accused person guilty in a financial crime case, one might query the jury's ability to deal with complex financial products and transactions.[8] In other words, in trying to understand the extent of and typologies used in financial crime cases, both conviction and non-conviction data may need to be treated with care.[9]

Obtaining reliable data in relation to financial crime can be difficult. Further to the comments above, most indictable prosecutions are dealt with in intermediate courts, which often do not report their decisions. Information relating to such criminal proceedings including transcripts, documents tendered in any trial or on sentence as well as any facts agreed between the parties may only be obtained from the court registry.

The following is a discussion and analysis of some of the information tendered in the prosecution of certain persons arising from Strike Force Apia, an investigation led by the New South Wales Police Fraud Squad State Crime Command into organised mortgage fraud in Australia.[10] The facts reproduced below are taken from the document titled 'Agreed Statement of Facts', which was contained on the New South Wales District Court file.[11]

2.2 Offenders' method of operation

Court documents[12] reveal that the following *modus operandi* was utilised:

1. The offenders would obtain copies of identification documents and other identification information from taxpayers with good credit histories ('taxpayers') (whether these taxpayers were complicit to any extent in the scheme was not settled).

2. Certain documents relating to the taxpayers, including income tax returns, were falsified to show a higher taxable income. This was typically done with PDF editing programs.

3. The principal offenders applied for finance, in the name of the taxpayers and purportedly on the taxpayers' behalves, via brokers (presumably to avoid any face-

---

[8] See Roderick Munday, 'The Roskill Report on Fraud Trials' (1986) 45(2) *Cambridge Law Journal* 175; Michael Levi, 'The Roskill Fraud Commission Revisited: An Assessment' (2004) 11(1) *Journal of Financial Crime* 38. See also Simon Bronitt and Bernadette McSherry, *Principles of Criminal Law* (Thomson Reuters, 3rd ed 2010) ch 12 (reproduced in Hugh McDermott (ed) *Fraud, Financial Crime and Money Laundering* (Thomson Reuters 2013) 41):

> [T]he complexity of modern commercial transactions raises concern that the trial procedures for dealing with 'serious commercial fraud' are inadequate. It has been argued that non-expert jurors may be less capable of evaluating financial impropriety, thereby increasing the costs and delays in prosecution, as well as the risk of unwarranted acquittals. It is noted that, in Australia, federal (as opposed to state and territory) criminal prosecutions must be tried by jury pursuant to the *Constitution* s 80.

[9] This point is to be distinguished from Tappan's argument that existing criminal law ought to establish boundaries to criminological study (Paul Tappan, 'Who is the Criminal?' (1947) 12(1) *American Sociological Review* 96, 99-100); for a contrary view on this argument, see Henry M Hart Jr, 'The Aims of the Criminal Law' (1958) 23(3) *Law and Contemporary Problems* 401.

[10] See n 1, above.

[11] *R v Terrence Reddy Adam Eli Meyer* (2011/00220791; 2011/00249266), Reddy Statement of Agreed Facts (unsigned).

[12] Ibid.

to-face contact between the applicant and persons employed by the finance company).

4. The offenders caused the money or property obtained pursuant to the finance to be made available to them. This involved the offenders using the property obtained or dissipating the monies.

5. When the taxpayers defaulted in respect of the facilities and enforcement proceedings were commenced against them, the taxpayers would deny any knowledge of having applied for finance in the first place and contend that they had been the victim of an identity fraud.

Many of the frauds involved companies. Where companies were used, the offenders would record the names of taxpayers as directors and shareholders on the company register of the Australian Securities and Investments Commission (ASIC). These taxpayers in fact had no involvement with the companies (or at least were only complicit to the extent of providing their personal information). As for the applications themselves, the deployment of taxpayers in the scheme here appears to have been an essential component of the scheme and may have delayed its detection.

The offenders communicated between themselves and with the taxpayers in person or via mobile phone. This combined with using the taxpayers as applicants for the facilities, and as company directors and shareholders, helped the scheme withstand desktop checking or investigations by the financial institutions. Moreover, in this case, the confidentiality of taxpayer information was perhaps used to the offenders' advantage.

2.3 Frauds against whom

First and obviously the schemes involved a fraud against the financial institutions which provided the facilities purportedly to the taxpayers. Secondly, they were frauds against the ATO. This was in two different ways. It was a fraud against the ATO because the fraudsters were the beneficiaries of the money or other property that was obtained from the scheme and, obviously, this was not reported as income. It was also a fraud on the ATO because the fraudsters were altering (technically falsifying) ATO documents – particularly tax returns – as part of a package of documents to obtain finance. This second fraud might be better described as a forgery in that the alterations resulted in ATO documents telling lies about themselves.[13] The ATO is a victim of the forgery in such a situation because it affects the ATO's integrity. Finally, they were also frauds against ASIC because to the extent companies were involved the fraudsters were falsifying the information contained on the ASIC register.

Again, the scheme appears to have exploited the confidentiality of taxpayer information in conjunction with good faith finance application principles. The incorporation of taxpayers in the scheme helped it survive desktop investigation particularly because the persons whose details were recorded on the applications for finance and company registers were apparently persons with no criminal associations and of good credit.

[13] *R v Moore* [1987] 1 WLR 1585.

2.4 Detection

Just as technology creates opportunities for criminals, it also creates opportunities for crime control. Wang[14] surveyed the existing research on all technical and review articles on automated fraud detection (including systematic computational analysis of data or statistics (analytics) and processes or sets of rules to be followed in calculations by computers (algorithms)) between 2000 and 2010. Analytics and algorithms can now be used to examine large pre-existing databases in order to generate new information (data mining). Algorithms are at the point where analyses of large volumes of data can predict what people will read, watch and buy let alone contribute to national security[15] and thus law enforcement and crime prevention.

Although data mining is playing increasingly important roles in relation to the detection of financial crime – and will perhaps have an increasingly important role as technology continues to improve – it does not appear to be at the point where data mining or desktop investigative processes can be relied upon solely to detect financial crime (or even reliably detect the red flags of financial crime). By reference to the scheme used in Strike Force Apia, the offenders used the taxpayers' details for applications for finance and as directors and shareholders on the ASIC register. Furthermore, communications between the offenders themselves and the offenders and the taxpayers were in person or via telephone. The digital footprint therefore discoverable by data mining would have related to the taxpayers and not the offenders (and thus appeared legitimate).

Although the scheme exploited technology, the principal offenders essentially reduced their reliance on technology-enabled communications (or 'de-sophisticated' their communications) to ensure that their involvement would evade a desktop or automated analysis. It was apparently the mobile telephone intercepts that allowed investigators and prosecutors to identify links between the principal offenders and the taxpayers and the principal offenders themselves. As is shown below, in Strike Force Apia, it was the use of modern surveillance technologies rather than data mining which obtained the necessary relationships between the offenders and associated admissions to convict the principal offenders of the scheme.

Both the sophistication of clandestine communications (for example via the use of the dark web and/or untraceable telecommunications) and de-sophistication of communications (for example, engaging in communications which do not result in the creation of data capable of mining) present a challenge to data mining applications. It is suggested then here for data mining applications to reach their full potential in relation to financial crime detection they may need to improve their identification and incorporation of both sophisticated (eg, dark web) and de-sophisticated relationship mining (to the extent that such relationships create data that will then be capable of being mined).

---

[14] Shiguo Wang, 'A Comprehensive Survey of Data Mining-based Fraud Detection Research', Intelligent Computation Technology and Automation (ICICTA), (2010) CoRR, abs/1009, 6119.

[15] Lyria Bennett Moses and Louis de Koker, 'Open Secrets: Balancing Operational Secrecy and Transparency in the Collection and Use of Data by National Security and Law Enforcement Agencies' (2017) 41(2) *Melbourne University Law Review* 530.

2.5 Investigation

Officers from Strike Force Apia ultimately charged offenders with offences under the *Crimes Act 1900* (NSW). The offenders were detected, investigated and prosecuted not by red flags following desktop audit or data mining processes but by the use of modern surveillance equipment and techniques including:

- Telecommunications interception;
- Aural surveillance devices (including listening devices worn on certain persons as well as installed at fixed locations); and
- Visual surveillance devices.

Despite offenders using mobile telephone numbers obtained in false names and regularly changing these numbers, it was the telecommunications interception in particular that captured admissions between the principal offenders, which in turn formed a substantial and persuasive component of the evidence relied upon by investigating police in deciding to charge and the prosecutor during the trial and sentence proceedings.

2.5.1 Existing evidence law prescriptions

In addition to operational investigations methods such as those above, the investigation of any alleged criminality is prescribed by the criminal law and the law of evidence. The law of evidence in most Australian jurisdictions is now largely codified via the so-called uniform evidence law[16] (although these Acts are not in fact a Code and not quite uniform). Moreover, the operation of section 80 of the federal *Constitution* and sections 68 and 79 of the *Judiciary Act 1903* (Cth) (together with s 109 of the *Constitution*) means that the relevant evidence Act in a tax crime prosecution is usually not the Commonwealth Act. This is because the *Constitution* and *Judiciary Act* create a system of surrogate Commonwealth law, derived as a form of legislative shorthand, by picking up and applying the State law of practice, procedure and evidence to federal offences. Thus, rules of practice, procedure and evidence in a prosecution for federal criminal offences are, except where otherwise provided for, those of the relevant State or Territory where the offence was committed.[17] Because this article uses a New South Wales strike force operation as its case study, references below to evidence law are references to the *Evidence Act 1995* (NSW).

The *Evidence Act's* drafters were insightful. Despite being drafted before 1995, it facilitates the adducing and admissibility of modern, technology-enabled evidence. The definition of 'document' means 'any record of information' and includes '(b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them'. Moreover, section 48 of the *Evidence Act* facilitates '*Proof of contents of documents*' via a variety of means other than via tender including:

> (a) adducing evidence of an admission made by another party to the proceeding as to the contents of the document in question,

[16] *Evidence Act 1995* (Cth), *Evidence Act 1995* (NSW), *Evidence Act 2008* (Vic); *Evidence Act 2011* (ACT).
[17] There are exceptions where the Commonwealth has specifically provided otherwise such as with regard to the sentencing, imprisonment and release of federal offenders — see *Crimes Act 1914*, Pt IB.

(b) tendering a document that:

(i) is or purports to be a copy of the document in question, and

(ii) has been produced, or purports to have been produced, by a device that reproduces the contents of documents,

(c) if the document in question is an article or thing by which words are recorded in such a way as to be capable of being reproduced as sound, or in which words are recorded in a code (including shorthand writing)--tendering a document that is or purports to be a transcript of the words,

(d) if the document in question is an article or thing on or in which information is stored in such a way that it cannot be used by the court unless a device is used to retrieve, produce or collate it--tendering a document that was or purports to have been produced by use of the device,

(e) tendering a document that:

(i) forms part of the records of or kept by a business (whether or not the business is still in existence), and

(ii) is or purports to be a copy of, or an extract from or a summary of, the document in question, or is or purports to be a copy of such an extract or summary…

Fundamentally, the *Evidence Act* assumes a distinction between adducing evidence including in relation to documents and the admissibility of evidence so adduced. Section 48 of the *Evidence Act* deals with the former whereas the latter is governed by the provisions in Chapter 3 of that Act. Key admissibility provisions include the rules governing relevance, admissions, hearsay and opinion.

Pursuant to section 55(1) of the *Evidence Act*, evidence is relevant if it could rationally affect the assessment of the probability of the existence of a fact in issue in the proceedings. In order for evidence to be relevant it must first be authenticated, which can probably not be done from the face of the document itself.[18] In the case of documents extracted from a smart device (for example), it may be that the metadata around the document (say in the case of a digital photograph or SMS message) may contribute to the authentication of the primary data itself.

'*Admission*' is defined very broadly in the Dictionary to the *Evidence Act* to mean, relevantly, a previous representation that is 'adverse to a person's interest in the outcome of the proceeding'. An admission is an exception to both the hearsay and opinion rules. Section 69 excepts 'business records' from the hearsay rule. This is a very broad exception and can include electronic mail communications.[19] There is also a provision (section 50) which explicitly provides for 'Proof of voluminous or complex

[18] *National Australia Bank Ltd v Rusu* [1999] NSWSC 539 [19].
[19] *Aqua-Marine Marketing Pty Ltd v Pacific Reef Fisheries (Australia) Pty Ltd (No 4)* [2011] FCA 578 [10].

documents'. This section not only facilitates the adducing of a summary but also excepts any summary adduced from the general prohibition against opinion evidence.

The definition of '*document*' in the *Evidence Act* plainly facilitates proof of data and other forms of digital evidence that might be relevant in relation to a technology-enabled crime. In Strike Force Apia, although the law of evidence contributed to the quality and reliability of the evidence adduced in the trial, it does not appear to have impacted adversely on either investigative and/or prosecutorial stages. Thus by reference to the above analysis, the existing provisions of the *Evidence Act* appear to facilitate the investigation and prosecution of technology-enabled financial crime.

2.6 Financial crime offences

Having considered whether the law of evidence effectively facilitates the investigation and prosecution of technology-enabled financial crime, this article will now consider whether the current financial crime offences are appropriate, particularly in the context of Strike Force Apia. While complex, it is critical to understand them as a whole in order to assess the comprehensiveness of their application to technology-focused financial crime.

Australia has followed the United Kingdom's lead in relation to financial crime offences. In the 1960s, the Criminal Law Revision Committee in the United Kingdom recommended that larceny and related offences should be replaced with a comprehensive code dealing with property offences. This model was enacted via the *Theft Act 1968* (UK). The Commonwealth enacted a *Theft Act*-like regime via the *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000* (Cth). New South Wales on the other hand does not appear to have adopted the *Theft Act* per se. Rather, the law relating to offences of dishonest acquisition involving deception was reformed in 2010 by the *Crimes Amendment (Fraud, Identity and Forgery Offences) Act 2009*.[20] Commonwealth offences are relevant when the fraud victim is a Commonwealth entity, such as the ATO. Where the victim is a person (natural or corporate), state offences are relevant.

As will be shown, however, even if the New South Wales provisions are not quite based on the *Theft Act* model, there is consistency between them. The general fraud offences created by the *Fraud Act* (and other like regimes) have been argued to offer 'the prospect of greater certainty, consistency and predictability in the criminal law'.[21]

After 24 May 2001, indictable Commonwealth fraud offences are contained in div 133 of the Schedule to the *Criminal Code Act 1995* (Cth) ('*Criminal Code*'). Section 135.1 of the *Criminal Code* 'contains a codified equivalent to *s 29D Crimes Act 1914 (Cth)*'.[22]

Section 135.1 of the *Criminal Code* creates an offence of obtaining a gain or causing a loss. Section 135.1(1) states that a person is guilty of an offence if the person does anything with the intention of dishonestly obtaining a gain from a Commonwealth

---

[20] The *Crimes Amendment (Fraud, Identity and Forgery Offences) Act 2009* (repealed) amended the *Crimes Act 1914* (Cth) by repealing a number of provisions relating to fraud and forgery, replacing them with new fraud and forgery provisions, and inserting offences concerning identity crime. It commenced on 22 February 2010.

[21] Bronitt and McSherry, above n 8, 42.

[22] Revised Explanatory Memorandum to the Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill 1999 (Cth) 89.

entity. Subsection (2) states that it is not necessary to prove that the accused knew that the other person was a Commonwealth entity. Section 135.1(3) creates another offence for causing a loss. Here, a person is guilty if the person does anything with the intention of dishonestly causing a loss to a Commonwealth entity. Again, it is not necessary to prove that the other person is a Commonwealth entity.

Section 135.1(5) of the *Criminal Code* creates an offence where a person dishonestly causes a loss, or dishonestly causes a risk of loss, to a Commonwealth entity. Similar to sections 135.1(1) and 135.1(3), it is not necessary to prove that the accused knew that the other person is a Commonwealth entity. In other words, absolute liability can be said to apply instead of strict liability because the latter affords the accused the defence of honest and reasonable mistake of fact and section 135.1(5) of the *Criminal Code* makes it clear that it is simply not necessary to prove the accused knew.

Section 135.1(5) makes it clear that there need only be an intention to cause loss, thus incorporating the common law economic imperilment doctrine. In other words, section 135.1(5) confirms that a person commits an offence if the person does anything with the intention of dishonestly causes a risk of loss to another person. In addition to various other species of fraud, section 135.1(1) would plainly catch tax-related fraud. Consider the situation where a fraud has been committed over a number of years or there have been a number of frauds over a number of years including the changeover period from the *Crimes Act 1914* (Cth) to the *Criminal Code*. Howie J in *R v Ronen & Ors*[23] adopted the Explanatory Memorandum's observation that the maximum penalty under the *Crimes Act 1914* (Cth) was 'far too high'. Here his Honour (with whom Spigelman CJ and Kirby J agreed), found[24] the situation was one where the sentencing judge was entitled to take into account the maximum penalty prescribed by section 29D of the *Crimes Act,* but that it was no longer an appropriate yardstick to the sentence to be imposed and had little relevance as a guide to the seriousness of the appellant's conduct.

Section 135.1 of the *Criminal Code* is of general and broad application. It is broader than its New South Wales equivalent, which *inter alia* requires deception. Section 192E of the *Crimes Act 1900* (NSW) states:

> (1) A person who, by any deception, dishonestly:
>
> (a) obtains property belonging to another, or
>
> (b) obtains any financial advantage or causes any financial disadvantage,
>
> is guilty of the offence of fraud.
>
> Maximum penalty: Imprisonment for 10 years.

Section 192E of the *Crimes Act 1900* has more in common with the Commonwealth's more serious fraud offence, '[o]btaining a financial advantage by deception' than the offence of 'general dishonesty'. Here section 134.2 of the *Criminal Code* provides:

> (1) A person is guilty of an offence if:

[23] (2006) 161 A Crim R 300 [71].
[24] Ibid [76].

> (a) the person, by a deception, dishonestly obtains a financial advantage from another person; and
>
> (b) the other person is a Commonwealth entity.
>
> Penalty: Imprisonment for 10 years.
>
> (2) Absolute liability applies to the paragraph (1)(b) element of the offence.

Two liminal elements requiring satisfaction in a prosecution under section 134.1(1) of the *Criminal Code* or s 192E of the *Crimes Act 1900* are (1) deception and (2) dishonesty. In relation to the former, lies, mistruths and misleading statements are the classic indicia.[25] In *Re London and Globe Finance Corporation Limited*,[26] Buckley J defined deception as follows: 'To deceive is, I apprehend, to induce a man to believe that a thing is true which is false, and which the person practising the deceit knows or believes to be false'. This passage was approved of by the High Court in *Spies v The Queen*.[27] Like section 192B of the *Crimes Act 1900* (NSW), section 133.1 of the *Criminal Code* expressly defines 'deception' to include:

- a deception as to the intentions of the person using the deception or any other person; and
- conduct by a person that causes a computer, a machine or an electronic device to make a response that the person is not authorised to cause it to do.

Curiously, a deception under the Commonwealth offence need only be reckless whereas dishonesty (which is defined in section 130.3 of the *Criminal Code* and section 4B of the *Crimes Act 1900* and is the subject of detailed discussion below) requires actual knowledge on the part of the accused. This means that the prosecution must prove the fault element of dishonesty; however, in relation to the deception, this only requires the fault element of recklessness, that is, to recklessly deceive dishonestly.

Steel argues that the concept of a 'financial advantage' in criminal fraud generally is a concept of unclear meaning.[28] As will be shown, in the context of tax crime, the situation becomes even more opaque. In relation to section 135.2 of the *Criminal Code* (which creates a less serious offence for obtaining financial advantage), the *Revised Explanatory Memorandum* states:

> The Gibbs Committee considered that the offence would be too broad if it extended to any advantage. They recommended that it be limited to knowingly obtaining a pension, benefit, bounty or grant from the Commonwealth to which the person is not entitled. [29]

---

[25] *Scott v Metropolitan Police Commissioner* [1975] AC 819.
[26] [1903] 1 Ch 728, 732-733.
[27] [2000] HCA 43; 201 CLR 603; 173 ALR 529; 74 ALJR 1263.
[28] Alex Steel, 'Money for Nothing, Cheques for Free? The Meaning of "Financial Advantage" in Fraud Offences' (2007) 31(1) *Melbourne University Law Review* 201.
[29] Revised Explanatory Memorandum to the Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill 1999 (Cth) 199.

This quote would suggest that the concept of financial advantage for the *Criminal Code* may not have been intended to extend to evaded taxes.

Although under the *Crimes Act 1900*, there is a definition of 'Obtaining a financial advantage or causing a financial disadvantage' in section 192D which explicitly includes temporary financial advantages, the term is not defined in the *Criminal Code*. At common law, it is by no means clear whether evasion of payment of a debt can amount to a financial advantage. For example, the High Court held that the passing of a valueless cheque was in fact a conditional payment of the debt, which was later rejected by the paying bank. Thus, no credit was asked for by such an action. There was a fraud, but not a fraud to obtain a financial advantage.[30] Conversely, in *Director of Public Prosecutions v Turner*,[31] the House of Lords found that presentation of a valueless cheque amounted to a financial advantage because it afforded the accused further time in which to make payment.[32] The position was complicated where interest was payable on an outstanding amount. Miles CJ in *Fisher v Bennett* [33] observed that delaying payment, where penalties and interest are provided for, might tend to worsen (as opposed to advance) a defendant's position.[34] This point may have been put to rest however by the Court of Criminal Appeal – at least in tax cases. In *Pratten v R*[35] (dismissing an appeal on this point), the Court held: [36]

> The position argued for by the appellant ignores the fact that upon the lodgement of the return, assuming a lower liability to pay tax than would otherwise have been the case, the taxpayer was subject to a lesser liability. The fact of that lesser liability was itself a financial advantage. That was so notwithstanding that at some time in the future that position might change.

In *Pratten v R*,[37] the Court went on to conclude that the expression 'financial advantage' in section 134.2(1) of the *Criminal Code* is broad enough to include being subject to a lesser liability as a result of the lodging of a false, or presumably no, return.

It is noted in passing that the emphasis of this part of the article is on whether existing financial crime offences facilitate the investigation and prosecution of technology-enabled crimes. Pausing here to discuss the application of section 134.2 of the *Criminal Code* in particular as a response to tax crime, it is submitted that there are at least two problems with its use in the case of dishonest misrepresentations about a taxpayer's taxable income. The first is in relation to its apparent irreconcilability with the objective theory of taxation (ie, tax-related liabilities would continue to accrue with interest and penalties irrespective of taxpayer misrepresentations in relation to them, which was the argument ventilated but rejected in *Pratten v R*). Secondly, the Court of Criminal Appeal's interpretation of financial advantage in the *Criminal Code* has meant that the Crown has an apparently unqualified choice of two offences in relation to the same

---

[30] *Tilley v Official Receiver in Bankruptcy* (1960) 103 CLR 529.
[31] [1974] AC 357.
[32] See also *R v Locker* [1971] 2 QB 321; *R v Page* [1971] 2 QB 330; *R v Fazackerley* [1973] 2 All ER 819; *R v Turner* [1973] 2 All ER 828.
[33] (1987) 85 FLR 469, 473.
[34] Steel, above n 28.
[35] *Pratten v R* [2014] NSWCCA 117.
[36] Ibid [92].
[37] Ibid.

conduct, with one carrying five years' imprisonment[38] and the other ten years'. The broad, general approach to drafting modern fraud offences does give them continuing relevance and application despite exploitation of technology by criminals.

As a New South Wales-based investigation and prosecution, the charges proffered against offenders in Strike Force Apia were *Crimes Act* offences. These included various fraud offences,[39] money laundering offences,[40] and forgery offences.[41] General fraud offences may be distinguished from forgery offences. Investigators and prosecutors appear to have focused on the latter with many of the counts on the indictments being for 'using a false document' under section 254(b)(ii) of the *Crimes Act 1900*. One might speculate that the charge of 'using' as opposed to 'making'[42] a false document was preferred to avoid the prosecution having to prove the creation of the false documents, which would have been more difficult than charging that the documents were, at minimum, used in the scheme.

Part 5 of the *Crimes Act 1900*, which deals with forgery, contains both interpretative provisions as well as offence provisions. The *Criminal Code* contains similar provisions in Part 7.7, Division 143. Section 250 of the *Crimes Act* (and section 143.2 of the *Criminal Code*) define false document. That definition was taken from the *Forgery and Counterfeiting Act 1981* (UK). As Lord Ackner said in *R v Moore*:[43]

> It is common ground that the consistent use of the word 'purports' in each of the paragraphs (a) to (h) inclusive of s.9(1) of the Act imports a requirement that for an instrument to be false, it must tell a lie about itself, in the sense that it purports to be made by a person who did not make it (or altered by a person who did not alter it) or otherwise purports to be made or altered in circumstances in which it was not made or altered.

The use of false document offences, then, 'requires more than simply making or altering a document so that it contains known falsehoods. The relevant falsity goes to the character of the document itself, in the sense that it purports to be something which it is not'. [44] 'Document' is defined in the *Interpretation Act 1987* (NSW) in similar, but not identical, terms to the *Evidence Act*:

> 'document' means any record of information, and includes:
>
> (a) anything on which there is writing, or
>
> (b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them, or

[38] *Criminal Code* s 135.
[39] See *Crimes Act 1900* (NSW) Part 4AA.
[40] Ibid Part 4AC.
[41] Ibid Part 5.
[42] Ibid s 253.
[43] [1987] 1 WLR 1585. See also *Attorney-General's Reference (No1 of 2000)* [2001] 1 WLR 331, 336 (Lord Woolf, CJ).
[44] *R v Ceylan* [2002] VSCA 53 [22] (Winneke P with whom Batt JA and O'Bryan AJA agreed) citing *Brott v R* [1992] HCA 5; (1992) 173 CLR 426, 430 per Brennan J; *Ex parte Windsor* (1869) LR 1 CCR 200, 204 per Blackburn J; *R v Roberts* [1886] VicLawRp 33; (1886) 12 VLR 135, 142.

(c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else, or

(d) a map, plan, drawing or photograph.

The *Criminal Code*'s definition of 'document' mirrors (a) – (c) but does not include (d).

As stated above, the offenders in Strike Force Apia utilised PDF editing software with the edited, or more correctly false, documents being plainly caught by both the definition of 'document' and the offence of 'using a false document'. Again, the *modus operandi* deployed was plainly caught by existing New South Wales fraud and false document charges. Had the matter been investigated and prosecuted by reference to Commonwealth offences, noting the tension with section 134.2 of the *Criminal Code* discussed above, the existing regime would have also been plainly caught by Commonwealth offences.

3. FINANCIAL CRIME CONTROL

The Commonwealth's Fraud Control Framework[45] in the context of fraud against the Commonwealth, notes:

> Fraud threats are becoming increasingly complex. Not only are entities at risk of fraud from external parties and internal officials, but increased provision of online services and exposure to overseas markets has created new threats from overseas criminals.'

The theory of financial crime and the analysis of case studies help in understanding financial crime in relation to detection, investigation, prosecution and prevention. Focusing for the moment on prevention, whether the fraudster ought to be explained by reference the triangle (or diamond) is not to the point. What is relevant, however, is that both conceptions incorporate an element of opportunity. Furthermore, the question of whether the fraud triangle is descriptive or predictive is perhaps of greater relevance. The fraud triangle (or as Wolfe and Hermanson conceive it, a diamond)[46] discussed above and its contribution or relevance to financial crime control is perhaps its contribution to the both criminological theory as well as the description of a fraudster. Although context is very important from a preventative perspective in controlling financial crime, the triangle is really subordinate or perhaps, more accurately, complementary to a risk-based financial crime control protocol.

Like reporting entities under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth), government organisations have a positive obligation to control fraud (at the Commonwealth level this is imposed by section 10 of the Public Governance, Performance and Accountability Rule 2014 (Cth)). Although not all private organisations are subject to the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, all organisations and the persons associated with them are subject to criminal fraud prohibitions and the associated law of corporate criminal responsibility and the law of complicity.

---

[45] Attorney-General's Department, *Commonwealth* '*Fraud Control Framework* (2017) iii, https://www.ag.gov.au/Integrity/FraudControl/Documents/CommonwealthFraudControlFramework2017.PDF (accessed 11 January 2019).
[46] Wolfe and Hermanson, above n 4.

Some private organisations, including financial institutions, may manage fraud and corruption risks via a cost-benefit analysis in terms of the cost of financial crime control (including investigation and litigation) to an organisation versus that organisation's measurable loss as a result of financial crime. Losses (or costs) however must be considered in terms of both tangible (including financial risk) and non-tangible (including operational and reputational risks) outcomes. A cost-benefit analysis by reference to tangible loss only therefore is an inadequate response to financial crime control. Australian Standard 'AS 8001-2008 Fraud and Corruption Control'[47] proposes (in section 1.4) an approach to controlling fraud and corruption. AS 8001-2008 counsels a combined process of establishing an organisation's fraud control objectives and values, which are then set in policy. In addition, it recommends a risk-based approach to the identification, analysis, evaluation, treatment, implementation, communication and monitoring and reporting of fraud. Clear reporting policies and procedures and ongoing awareness training, monitoring and improvement are also prescribed.

AS 8001-2008 (in section 1.9) adopts the three key themes suggested for fraud and corruption control by KPMG Forensic Fraud Risk Management in their Whitepaper issued in November 2005 (prevention, detection and response).[48] The descriptive fraud triangle (or diamond) assists in understanding the typical fraudster. Case study analysis also assists in understanding emerging typologies. Both of these matters assist in the detection, investigation and prosecution of financial crime. The analysis above reinforces the sufficiency and comprehensiveness of the Commonwealth and State (using the example of New South Wales in the context of the case study) legislation in doing so.

Therefore, specifically in relation to prevention efforts, risk-based financial crime control protocols assist in prevention or control efforts. With the exception of data mining, detection, investigation, prosecution and prevention of financial crime all appear to be dependent on sufficient allocation of resources rather than procedural or legal reform of existing processes.

4. CONCLUSION

Although data mining applications are yet to reach their full potential insofar as incorporating both sophisticated and de-sophisticated relationship analytics is concerned (to the extent that this is possible particularly in relation to the latter), an analysis of the above case study by reference to current processes suggests that existing detection, investigation, prosecution and prevention processes are adequate in countering financial crime.

The extensive analysis of the relevant legislation identifies that, in the current context, the legislation is sufficient. In addition, existing forensic processes (including the law of evidence and offence regimes) appear to provide the capability to detect, investigate and prosecute even the more sophisticated species of financial crime. Of course, the concept of capability differs from capacity and although capability may exist, agencies must be adequately resourced. Thus while technology has no doubt created new opportunities to defraud the revenue, detection and investigations technology coupled

[47] Standards Australia, *AS 8001-2008: Fraud and Corruption Control* (2008) section 1.4, https://www.saiglobal.com/PDFTemp/Previews/OSH/AS/AS8000/8000/8001-2008.pdf.
[48] Ibid.

with existing law surrounding the proof of data means that appropriately resourced regulatory agencies, including the ATO, appear to have the capability to counter even the more sophisticated attempts to defraud the revenue and third parties based on taxpayer information.