IDENTITY THEFT AND TAX CRIME: Has technology made it easier to defraud the revenue?

Mathew Leighton-Daly

Abstract

The modern phenomena of online applications and processes mean that there is greater opportunity to defraud both the revenue and others, based on identity theft, than ever before. 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 application and other online processes are such that fraudsters can coordinate entire schemes without ever showing their faces in the traditional sense. This creates new opportunities for fraud both directly upon the ATO but also using taxpayer information to obtain a financial advantage from others based on that information.

This paper focuses on a significant financial crime investigation and subsequent prosecution (Strike Force Apia - the largest NSW Strike Force in relation to mortgage fraud based on inter alia alleged false income tax returns) to identify some financial crime typologies relating to the revenue and taxpayer information. Once the context and risks have been identified and analysed the work moves into an analysis of evidence and procedure and offence analysis to consider how effectively existing processes can facilitate detection and investigation and prosecution in this dynamic technology-enabled space.

It is concluded that while technology has in some respects created new opportunities to defraud the revenue, detection and investigations technology coupled with existing law surrounding the proof of data, means that appropriately resourced regulatory agencies, including the ATO, can counter even the more sophisticated attempts to defraud the revenue and third parties based on taxpayer information.

1 BPol, JD (Hon I), LLM (Syd), PhD Scholar (Atax, UNSW); School of Law, Faculty of Law, Humanities & the Arts, University of Wollongong.
1. **Introduction**

The modern phenomena of online applications and processes mean that there is greater opportunity to defraud both the revenue and others, based on identity theft, than ever before. 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 application and other online processes are such that fraudsters can coordinate entire schemes without ever showing their faces in the traditional sense. This creates new opportunities for fraud both directly upon the ATO but also using taxpayer information to obtain a financial advantage from others based on that information.

This paper focuses on a significant financial crime investigation and subsequent prosecution (Strike Force Apia - the largest NSW Strike Force in relation to mortgage fraud based on inter alia alleged false income tax returns) to identify some financial crime typologies relating to the revenue and taxpayer information. Once the context and risks have been identified and analysed the work moves into an analysis of evidence and procedure and offence analysis to consider how effectively existing legislation can facilitate detection and investigation and prosecution in this dynamic technology-enabled space.

2. **Understanding Financial Crime**

Attempting to explain financial crime is not new. 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. This ultimately led to the development of the ‘fraud triangle’, not by Sutherland himself, but rather by one of his students, Donald Cressy.

---

\(^2\) E Hardin Sutherland and D Cressy, *Criminology* (Lippincott, 1978):

- Criminal behaviour is learned; it’s not inherited, and the person who isn’t already trained in crime doesn't invent criminal behaviour.
- Criminal behaviour is learned through interaction with other people through the processes of verbal communication and example.
- The principle learning of criminal behaviour occurs with intimate personal groups.
- The learning of crime includes learning the techniques of committing the crime and the motives, drives, rationalizations and attitudes that accompany it.
- A person becomes delinquent because of an excess of definitions (or personal reactions) favorable to the violation of the law.
Both in an article and his book, Cressey defined the fraud problem as a ‘violation of a position of financial trust’ that the person originally took in good faith. Thus, the fraud triangle and its three stages (categorised by the effect on the individual) of (1) pressure, (2) opportunity and (3) rationalisation was born. The fraud triangle has been the subject of a great deal of discussion since its conception. Notably, Wolfe and Hermanson suggest that the fraud triangle could be improved by considering a fourth element, capability. This means the personal traits and abilities that play a major role in whether fraud might actually occur even with the presence of the other three elements. Cressey’s fraud triangle has been the subject of analysis, notably also by Free. In his article, ‘Looking through the fraud triangle: A review and call for new directions’ Free reviews popular frameworks used to examine fraud (including the fraud triangle) and earmarks three areas where there is considerable scope for academic research to guide and inform important debates within organisations and regulatory bodies. Three under-researched issues are identified: rationalisation of fraudulent behaviours by offenders, the nature of collusion in fraud and regulatory attempts to promote whistle blowing.

2.1 Case study – strike force apia

Like popular fraud examination frameworks, in trying to understand financial crime, case studies may be helpful too. 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. As for understanding the methods and extent of technology-enabled financial crime however, 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 reliability of facts adduced in criminal

---


4 D Cressey, Other People’s Money, A Study in the Social Psychology of Embezzlement (Patterson Smith, 1953) 973.

5 Ibid:


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. 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.

Obtaining reliable data in relation to financial crime can be difficult. Further to the comments made immediately 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 (Strike Force Apia was an investigation led by the NSW Police Fraud Squad State Crime Command into organised mortgage fraud in Australia). The facts reproduced below are taken from the document titled ‘Agreed Statement of Facts’, which was contained on the NSW District Court file.

2.2 Modus operandi

Court documents reveal that the following modus operandi was utilised:

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

---


[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.

10 This point is to be distinguished from Tappan’s argument that existing criminal law ought to establish boundaries to criminological study (P Tappan, “Who is the criminal?” (1947) 12 AM Soc Rev 96 at 99-100), which was dismissed angrily by Hart (HM Hart, “The aims of the criminal law” (1958) 23 Law & Contemp Problems 404).

11 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. Certain documents relating to the agents, 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, purportedly on behalf of the agents, via brokers (presumably to avoid any face-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 dissipation of the monies.

5. When the agents defaulted in respect of the facilities, the persons whose identities were used by the offenders (not being in possession of the relevant money or other property) would deny any knowledge of the fraud.

Many of the frauds involved companies. In this case, the offenders would record the names of agents as directors and shareholders who in fact had nothing to do with the scheme (or at least were only complicit to the extent of providing their personal information. Like in relation to the applications themselves, the deployment of agents in the scheme here appears to have been an essential component of the scheme and may have delayed its detection. Importantly, the agents helped the scheme withstand desktop checking or investigations. 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 agents. 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. 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 agents in the scheme helped it survive desktop investigation here 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.

2.4 Detection

Just as technology creates opportunities for criminals, it also creates opportunities for crime control. The systematic computational analysis of data or statistics (analytics) and processes or sets of rules to be followed in calculations by computers (algorithms) is not particularly new. In this regard, Phua et al\textsuperscript{13} surveyed the existing research on all technical and review articles on automated fraud detection 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). Nowadays, 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\textsuperscript{14} and thus law enforcement.

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 it can reliably detect financial crime automatically (or even reliably detect red flags automatically). By reference to the scheme used in Strike Force Apia, the principal offenders essentially de-sophisticated their communications to ensure that their involvement would survive 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 agents and the principal offenders themselves. Again, in Strike Force Apia, it was the use of modern surveillance technologies rather than data mining which obtained the apparently necessary relationships and 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 (e.g. dark web) and de-sophisticated relationship mining (to the extent that such relationships create data that will then be capable of being mined).

\textsuperscript{13} C Phua et al, A Comprehensive Survey of Data Mining-based Fraud Detection Research, Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference

2.5 Investigation

Officer from Strike Force Apia ultimately charged offenders with offences under the *Crimes Act 1900* (NSW). Again, 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

The investigation of any criminal law is to an extent prescribed by the criminal law and moreover the law of evidence. The law of evidence in most Australian jurisdictions is now largely codified via the so called uniform evidence law.\(^{15}\) These Acts, however, are not quite a code and not quite uniform. Moreover, the operation of the *Constitution* s 80, ss 68 and 79 of the *Judiciary Act 1903* (Cth) (and 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.\(^{16}\) Because this paper is being delivered in New South Wales and uses a NSW strike force operation as its case study, references to evidence law hereinafter are references to the *Evidence Act 1995* (NSW).

---

\(^{15}\) *Evidence Act 1995* (Cth), *Evidence Act 1995* (NSW), *Evidence Act 2008* (Vic); *Evidence Act 2011* (ACT)

\(^{16}\) There are exceptions where the Commonwealth has specifically provided otherwise such as with regard to the sentencing, imprisonment and release of federal offenders — see pt IB of the *Crimes Act*.  

291
The Evidence Act’s drafters were insightful. 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, s 48 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,

(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 Evidence Act deals with the former whereas the latter is governed by the provisions in Chapter 3 Evidence Act. Key admissibility provisions include the rules around relevance, admissions, hearsay and opinion.

Pursuant to s 55(1) 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. 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

---

17 NAB v Rusu [1999] NSWSC 539, [19].
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.\(^{18}\) There is also a provision, s 50 Evidence Act, which explicitly provides for ‘Proof of voluminous or complex 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.

### 2.6 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), which has formed the basis of the property offences enacted by many Australian jurisdictions. 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.\(^{19}\) As will be shown however even if the NSW 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.’\(^{20}\) As will be shown, this appears to be true.

Post-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).’\(^{21}\)

---

\(^{18}\) Aqua-Marine Marketing Pty Ltd v Pacific Reef Fisheries (Australia) Pty Ltd (No 4) [2011] FCA 578, [10].

\(^{19}\) 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.

\(^{20}\) S Bronitt and B McSherry, Principles of Criminal Law (3rd ed, 2010), 42.

\(^{21}\) Revised Explanatory Memorandum at 89.
Section 135.1 Criminal Code creates an offence of obtaining a gain or causing a loss. Section 135.1(1) Criminal Code 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 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) 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 ss 135.1(1) and 135.1(3) Criminal Code, 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 ss 135.1(5) Criminal Code makes it clear that it is simply not necessary to prove the accused knew.

Section 135.1(5) Criminal Code makes it clear that there need only be an intention to cause loss, thus incorporating the old economic imperilment doctrine. In addition to various other species of fraud, ss 135.1(1) Criminal Code 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 & Ors22 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), found23 the situation was one where the sentencing judge was entitled to take into account the maximum penalty prescribed by Crimes Act s 29D, 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 Criminal Code is of general and broad application. It is broader than its NSW equivalent, which inter alia requires deception. Section 192E 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.”

22 (2006) 161 A Crim R 300, [71].
23 R v Ronen & Ors (2006) 161 A Crim R 300, [76].
Section 193E *Crimes Act* has more in common with the Commonwealth’s more serious fraud offence, ‘*obtaining a financial advantage by deception*’ than the offence of ‘general dishonesty’. Here s 134.2 of the *Criminal Code* provides:

> “(1) A person is guilty of an offence if:
> (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 s 134.1(1) *Criminal Code* or s 129E *Crimes Act* are (1) deception and (2) dishonesty. In relation to the former, lies, mistruths and misleading statements are the classic indicia of dishonesty. 24 In *Re London and Globe Finance Corporation Limited*, 25 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*. 26 Like s 192B of the *Crimes Act 1900* (NSW), s 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 *Criminal Code* s 130.3 and s 4B *Crimes Act* 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.

---


26 [2000] HCA 43; 201 CLR 603; 173 ALR 529; 74 ALJR 1263.
Steel argues that the concept of a ‘financial advantage’ in criminal fraud generally is a concept of unclear meaning. 27 In the context of tax-crime, the situation becomes even more opaque. In relation to s 135.2 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. (emphasis added)” 28

Although under the Crimes Act, there is a definition of ‘Obtaining a financial advantage of causing a financial disadvantage’ in s 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. 29 Conversely, in Director of Public Prosecutions v Turner, 30 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. 31 The position was complicated where interest was payable on an outstanding amount. Miles CJ in Fisher v Bennett 32 observed that delaying payment, where penalties and interest are provided for, might tend to worsen (as opposed to advance) a defendant’s position. 33 This point may have been put to rest however by the Court of Criminal Appeal – at least in tax cases. In Pratten v R 34 (dismissing an appeal on this point), the Court held: 35

“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.”

28 At 199.
29 Tilley v Official Receiver in Bankruptcy (1960) 103 CLR 529.
33 Steel, above n 27.
34 [2014] NSWCCA 117.
35 Pratten v R [2014] NSWCCA 117, [92].
In *Pratten v R*, the Court goes on to conclude that the expression ‘financial advantage’ in s 134.2(1) *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 work is on whether existing financial crime offences facilitate the investigation and prosecution of technology-enabled crimes. Pausing here to discuss the application of s 134.2 *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 (i.e. tax-related liabilities would continue to accrue with interest and penalties irrespective of taxpayer misrepresentations in relation to them (this 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 conduct with one carrying 5 years’ gaol and the other 10. The broad, general approach to drafting modern fraud offences does give them continuing relevance and application despite exploitation of technology by criminals.

As a NSW-based investigation and prosecution, the charges preferred against offenders in Strike Force Apia were *Crimes* Act offences. These included various fraud offences, money laundering offences, and forgery offences. General fraud offences may be distinguished from forgery offences. Investigators and prosecutors appear to have focussed on the latter with many of the counts on the indictments being for ‘using a false document’ under s 254(b)(ii) *Crimes Act*. One might speculate that the charge of ‘using’ as opposed to ‘making’ 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*, 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 *Crimes Act* (and s 143.2 *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*:

---

36 *Pratten v R* [2014] NSWCCA 117, [92]
37 S 135 *Criminal Code*.
38 See Part 4AA *Crimes Act 1900* (NSW).
39 See Part 4AC *Crimes Act*.
40 See Part 5 *Crimes Act*.
41 s 253 *Crimes Act 1900*.
“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.” 43 ‘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
(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 NSW fraud and false document charges. Had the matter been investigated and prosecuted by reference to Commonwealth offences, noting the tension with s 134.2 Criminal Code discussed above, the existing regime would have also been plainly caught by Commonwealth offences.

3. FINANCIAL CRIME PREVENTION

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, 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 diamond) 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 important – very important – from a preventative perspective in controlling financial crime, the triangle is really subordinate or perhaps, more accurately, complimentary 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 Commonwealth level this is imposed by s 10 of the *Public Governance, Performance and Accountability Rule 2014* (Cth)). Although private organisations on the other hand may not, 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. Treatment of fraud and corruption risks by private organisations such as financial institutions may involve a cost benefit analysis but this ought to include both tangible (including financial risk) and non-tangible (including operational and reputational risks) outcomes.

The Commonwealth’s Fraud Control Framework\(^44\) 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.’ AS 8001-2008 Fraud and Corruption Control\(^45\) proposes (at 1.4) an approach to controlling fraud and corruption through a process of:

- establishing an entity’s fraud and corruption control objectives and values;
- setting an entity’s anti-fraud and anti-corruption policies;
- developing, implementing, promulgating and maintaining an holistic integrity framework;
- fraud and corruption control planning;
- risk management including all aspects of identification, analysis, evaluation, treatment, implementation, communication and monitoring and reporting;
- implementation of treatment strategies for fraud and corruption risks with a particular focus on intolerable risk;
- ongoing monitoring and improvement;

\(^44\) Attorney-General’s Department, *Commonwealth Fraud Control Framework*, iii accessed online on 18 March 2018 <https://www.ag.gov.au/CrimeAndCorruption/FraudControl/Pages/FraudControlFramework.aspx>

• awareness training;
• establishing clear reporting policies and procedures;
• setting guidelines for the recovery of the proceeds of fraud or corruption; and
• implementing other relevant strategies.

AS 8001-2008 (at 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). 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. Specifically in relation to prevention efforts, this requires 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 may need to be improved by way of incorporating both sophisticated and de-sophisticated relationship analytics (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. Existing 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 fraud. Of course, the concept of capability differs from capacity and although capability may exist, agencies must ensure that they are adequately resourced. Thus while technology has no doubt created new opportunities to defraud the revenue, detection and investigations technology coupled with existing law surrounding the proof of data means that appropriately resourced regulatory agencies, including the ATO, can counter even the more sophisticated attempts to defraud the revenue and third parties based on taxpayer information.
5. REFERENCES/BIBLIOGRAPHY

5.1 Primary materials

5.1.1 Legislation

Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)
Constitution of Australia Act 1900 (UK)
Crimes Act 1914 (Cth)
Crimes Act 1900 (NSW)
Crimes Amendment (Fraud, Identity and Forgery Offences) Act 2009 (NSW)
Criminal Code Act 1995 (Cth)
Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000 (Cth)
Evidence Act 2011 (ACT)
Evidence Act 1995 (Cth)
Evidence Act 1995 (NSW)
Evidence Act 2008 (Vic)
Judiciary Act 1903 (Cth)
Public Governance, Performance and Accountability Rule 2014 (Cth)
Theft Act 1968 (UK)

5.1.2 Cases

Aqua-Marine Marketing Pty Ltd v Pacific Reef Fisheries (Australia) Pty Ltd (No 4) [2011] FCA 578
Attorney-General's Reference (No. 1 of 2000) [2001] 1 WLR 331
Director of Public Prosecutions v Turner [1974] AC 357
Ex parte Windsor (1869) LR 1 CCR 200
Fisher v Bennett (1987) 85 FLR 469
NAB v Rusu [1999] NSWSC 539
Pratten v R [2014] NSWCCA 117
R v Ceylan [2002] VSCA 53
R v Moore [1987] 1 WLR 1585
R v Roberts [1886] VicLawRp 33; (1886) 12 VLR 135
R v Ronen & Ors (2006) 161 A Crim R 300
5.2 Secondary materials

Attorney-General’s Department, *Commonwealth Fraud Control Framework* accessed online on 18 March 2018 <https://www.ag.gov.au/CrimeAndCorruption/FraudControl/Pages/FraudControlFramework.aspx>


Cressey, D, ‘Why Do Trusted Persons Commit Fraud? A Social-Psychological Study of Defalcators’ (1951) 92 *Journal of Accountancy* 576

Cressey, D, *Other People’s Money, A Study in the Social Psychology of Embezzlement* (Patterson Smith, 1953)


Free, C, ‘Looking through the fraud triangle: a review and call for new directions’ (2015) 23(2) *Meditari Accountancy Research* 175

Free, C and P Murphy, ‘The Ties that Bind: The Decision to Co-offend in Co-offend in Fraud’ (2014) 32(1) *Contemporary Accounting Research* 18


Murphy, P, and C Free, ‘Broadening the Fraud Triangle: Instrumental Climate and Fraud’ (2015) 28(2) Behavioral Research in Accounting 41