FROM PAPER TO ELECTRONIC: EXPLORING THE FRAUD RISKS STEMMING FROM THE USE OF TECHNOLOGY TO AUTOMATE THE AUSTRALIAN TORRENS SYSTEM

ROUHSHI LOW*

I Introduction

In recent years, improvements in information technology have caused various industries to incorporate technology into their manual systems.[1] Technology is usually said to provide business sectors with greater ability to store and exchange information, improve document management, streamline processes so as to enable faster processing leading to a reduction in costs. However technological advances have also provided criminals with new ways of perpetrating crime. This paper will explore the fraud risks stemming from the use of technology to automate the Australian Torrens system. Given the fraud potential afforded to criminals by technology, an understanding of these fraud risks is vital in developing fraud minimization measures. The approach taken by this paper is as follows: first, a brief overview of the methods of fraud perpetration will be provided so as to identify factors in conveyancing processes that enable these frauds; secondly, a comparison of

* Lecturer, School of Accountancy, Queensland University of Technology. Email: r.low@qut.edu.au . The author would like to thank Mark Burdon and Warren Moyes, Senior Advisor to the Registrar-General of Land, Land Information New Zealand, for their helpful comments. The author would also like to thank Professor Michael Weir for the opportunity to participate in the 2008 Torrens Title Workshop at Bond University and to all workshop participants for their informed and helpful feedback.

1 For example, the Australian Government's eHealth program uses technology to electronically manage health information. It is said that this will help deliver safer, more efficient, better quality healthcare. See the Australian Government Department of Health and Aging, *eHealth* (2008) <http://www.health.gov.au/internet/main/publishing.nsf/Content/eHealth> at 4 November 2008. The courts are also increasingly integrating technology into their systems as an aid to courtroom litigation and to improve the management of justice sector data. See for example: Sheryl Jackson, 'New Challenges for Litigation in the Electronic Age' (2007) 12 (1) *Deakin Law Review* 81.

the electronic systems[2] in New Zealand and Canada[3] and the systems proposed in Australia (the Victorian EC System[4] and the National Electronic Conveyancing System or NECS[5]) will be undertaken in order to identify their common and differing characteristics. This comparative analysis will be divided according to the fraud enabling factors identified previously; finally, the implications of these common and differing features from a fraud risk perspective will then be explored and where appropriate, areas for further research will be flagged.

II Fraud in the Torrens System[6]

The most prevalent method of fraud perpetration is forgery of the victim's signature on the mortgage or transfer instrument followed by impersonation of the victim or identity fraud[7] and misleading the victim into signing relevant documentation. It

---

2 For the purposes of this article, electronic systems are systems that allow for a completely paperless transaction, from the preparation of land title documents to the lodgement of such documents for registration. This article will use the term 'electronic registration system' to denote this type of land registration system and 'paper registration system' to denote land registration systems where the registration system has not been automated.

3 These systems are used in this paper because they are fully operational electronic registration systems, as identified in Rouhshi Low, 'Maintaining the Integrity of the Torrens System in a Digital Environment: A Comparative Overview of the Safeguards Used Within the Electronic Land Systems in Canada, New Zealand, United Kingdom and Singapore' (2005) 11(2) *Australian Property Law Journal* 155.

4 In 2002, the Victorian Government started its Land Exchange program to enable the exchange of land related information and the conduct of transactions via the Internet. One of the projects developed by Land Exchange is the Electronic Conveyancing (EC) project which enables electronic settlement and lodgement of title transfers and of discharges and registration of mortgages. The website for the Victorian EC project is: <http://www.landexchange.vic.gov.au/ec/>.

5 Unlike the Victorian EC, which is specific to the State of Victoria, NECS is an Australian-wide initiative. The website for NECS is: <http://www.necs.gov.au/>. Articles on the NECS include Andrew Perry, 'Building the Home Page' (2005) (262) *Lawyers Weekly* 16, Alan Davidson, 'The National Electronic Conveyancing System' (2006) 26(1) *Proctor* 33 and Shaun Drummond, 'Victorian E-Conveyance Should Go National' (2005) (267) *Lawyers Weekly* 10.

6 Information in this section is based on Rouhshi Low, 'Opportunities for Fraud in the Proposed Australian National Electronic Conveyancing System: Fact or Fiction?' (2006) 13(2) *Murdoch University Electronic Journal of Law* 225.

7 It is noted that there is an overlap between forgery and impersonation. In impersonation cases, the fraudulent person impersonating the victim would still be required to sign as the victim on the land title instrument and in that sense the victim's signature is forged. It could also be said that in forging a person's signature, the fraudulent is impersonating that

may also be possible to perpetrate fraud by altering a land title instrument after the instrument had been executed.[8]

These methods of fraud perpetration are linked to certain conveyancing processes and practices, namely:

(i) Processes related to execution and witnessing.

(ii) The current practice that instruments that create or transfer an interest must be executed by the person creating or transferring the interest, and that the most usual method of execution for individuals is the placing of a signature on the instrument, means that fraud may be perpetrated by forging the signature of the person entitled to create or transfer the interest. For companies, the usual method of execution is to affix the company's seal to the instrument. The fact that this affixing of the seal is witnessed by two directors, or by a director and secretary, means that fraud may be perpetrated by affixing the seal without the company's authority and purporting to witness its affixing. Further, since it is possible for an attorney to execute an instrument on behalf of the grantor of the power of attorney, fraud may be perpetrated by falsifying that power of attorney.

(iii) Witnessing requirements are said to act as a safeguard against fraud, but the fraudulent person can circumvent these by forging the signature of the witness (which can be of a genuine or fictitious person) or when the witness attests to the signatures even though there were not signed in his/her presence.[9]

(iv) Processes related to access, preparation, lodgement and examination of land title instruments.

---

person. For the purposes of this paper, impersonation is restricted to the situation where the fraudulent person uses identity documents (including certificate of title) which may be genuine or false to impersonate the victim for the purposes of perpetrating the fraud. Hence the main method of perpetrating the fraud is the use of the victim's identity documents, the forgery of the signature is incidental. Forgery is restricted to the situation where the fraudulent person simply forges the victim's signature.

8 Max Locke, Registrar of Titles Queensland Max.Locke@nrm.qld.gov.au email (14 March 2007). The Registrar noted that the case was resolved by the parties concerned.

9 See Rouhshi Low, 'Opportunities for Fraud in the Proposed Australian National Electronic Conveyancing System: Fact or Fiction?' (2006) 13(2) *Murdoch University Electronic Journal of Law* 225.

(v) As there are currently no restrictions about who may prepare and lodge land title documents, this means that fraud may be perpetrated by fraudulently altering these documents. Anyone with access to these documents that have been prepared and executed may perpetrate this fraud. It also means that fraud may be perpetrated if a fraudulent person prepares the necessary forms, or obtains them from someone else who has prepared them, and misleads or induces the victim to execute them, and they are then lodged for registration.

(vi) Use of the certificate of title.

(vii) Finally, the use of the certificate of title, indicating a right to deal with the land, means that fraud may be perpetrated when the fraudulent person is able to produce the certificate of title and it is assumed that he or she is the person named on the certificate of title and therefore has a right to deal with the land – identity fraud.

III Comparative analysis of salient features of electronic systems

Given that methods of fraud perpetration are linked to access, preparation, lodgement, examination, registration, and execution and use of the paper certificate of title, the following analysis will be divided into these categories.

A *Access*

1 *Restricted access or open access*

In all the electronic registration systems access to the system is controlled – only those who have established their credentials with the system may use the system.[10]

2 *Method of controlling access*

An electronic system's method of controlling access may be divided into two parts: the registration or identification process and the authentication process. The registration process refers to the process that prospective applicants must undergo in

[10] For the New Zealand and Canadian systems, see Rouhshi Low, 'Maintaining the Integrity of the Torrens System in a Digital Environment: A Comparative Overview of the Safeguards Used Within the Electronic Land Systems in Canada, New Zealand, United Kingdom and Singapore' (2005) 11(2) *Australian Property Law Journal* 155. For the NECS and Victorian EC System, see National Electronic Conveyancing Office, 'Draft Operations Description for a National Electronic Conveyancing System V.6' (National Electronic Conveyancing Office, 2007), [7.3]; Department of Sustainability and Environment, *Fact Sheets – What is Electronic Conveyancing (*2008) <http://www.landexchange.vic.gov.au/ec/s_factsheets.html> at 25 November 2008.

order to be registered as an authorised user of the system. Once the application is approved, the user is then able to access the system by logging on to the system. The subsequent process after registration is the authentication process. The registration process involves a 'claim or statement of identity'[11] whereas the 'aim of authentication is to validate a person's identity',[12] to verify that claim so as to ensure that the user who is seeking access to the system is the same one who originally applied to be registered. It is during the registration process that a prospective user must provide the system with identification to enable his or her identity to be established.[13]

There are various authentication techniques but they are generally classed into three broad categories[14]:

- something you have (token-based) such as a smartcard;
- something you know (knowledge-based) such as a password or PIN or an account number; and
- something you are (biometrics) such as facial image or retinal scan.

3 *Authentication methods*

In Ontario and New Zealand, the authentication method in both systems is a combination of 'something you have' and 'something you know' - access is controlled by public key cryptography which requires a token and a password.[15] In Ontario, the token is called the personal security package (PSP),[16] consisting of a

---

11 Office of the Privacy Commissioner of Canada, *Guidelines for Identification and Authentication* (2006) <http://www.privcom.gc.ca/information/guide/auth_061013_e.asp> at 1 November 2006.

12 Stephen Mason, 'Validating Identity for the Electronic Environment' (2004) 20(3) *Computer Law and Security Report* 164, 166.

13 See Geoff Main and Brett Robson, 'Scoping Identity Fraud' (Attorney General's Department, 2001).

14 See: Office of the Privacy Commissioner of Canada, *Guidelines for Identification and Authentication* (2006) <http://www.privcom.gc.ca/information/guide/auth_061013_e.asp> at 22 January 2009.

15 For these systems, public key cryptography is also the technology used to replace handwritten signatures. This is discussed further below. For the purposes of this paper, users who are authorised to use the system are termed 'authorised users'.

16 See Teranet Inc, *Personal Security Package* <http://www.teraview.ca/ereg/ereg_PSP.html> at 22 January 2009.

personal security profile with an encrypted digital identity and pass phrase, and in New Zealand it is the Digital Certificate.[17]

In contrast to this, British Columbia uses a 'something you know' authentication mechanism – access is controlled via unique user identifications (usernames) and passwords. At the time of writing, it appears that the NECS and Victorian EC System will follow the British Columbia pattern.[18]

4 *Registration process*

Whilst all electronic registration systems require its prospective users to undergo a form of registration process to obtain access, the process itself differs from system to system.

In both Ontario[19] and New Zealand[20], each prospective user must undergo a registration process where the prospective user's identity is checked, before access is granted.

However in the British Columbian system and NECS, a type of nomination registration process is/will be used. Under this process, an individual authorised by

---

17 Land Information New Zealand, *Landonline Security* <http://www.landonline.govt.nz/content/general/security.asp> at 22 January 2009.

18 See National Electronic Conveyancing Office, 'Draft Operations Description for a National Electronic Conveyancing System V.6' (National Electronic Conveyancing Office, 2007), [7.4]; Department of Sustainability and Environment, *EC System Rules Release 3* (2008) 29 <http://www.landexchange.vic.gov.au/ec/r_regdocs.html> at 25 November 2008.

19 Each user must complete a personal security licence (PSL) application form and appear before a designated representative (who may be lawyers, notaries, designated land Registry Office representatives, designated Teranet representatives and financial institution signing officers) whose role is to validate the applicant's identity. Upon receiving the PSL application form, Teranet verifies the application before issuing the applicant with a PSL, upon which the applicant can then use the PORTAS website to initialise his/her PSP. See: Teranet Inc, *Securing Your Information* <http://www.teraview.ca/ereg/security_brochure.html> at 20 April 2006 and Teranet Inc. Teranet Authorized Group Services Form 300 (2006) <http://www.teraview.ca/purchase/downloads/Form200.pdf> at 22 January 2009.

20 To obtain a digital certificate to use Landonline, the applicant must complete a proof of identity form, providing current proof of identity. The proof of identity form must be certified and mailed to LINZ who will verify identity before digital certificates can be issued. See Land Information New Zealand, *How to Sign-Up* <http://www.landonline.govt.nz/content/general/how-to-sign-up.asp> at 22 January 2009 and Land Information New Zealand, *Sign-Up Checklist* <http://www.landonline.govt.nz/content/signup/what-you-need.asp> at 22January 2008.

an organisation (such as a law firm) wanting to use the system applies for access. Once the application is successful, the authorised officer may then nominate other individuals employed or contracted by the organisation to be users of the system. Using this method, no identity checks are made on each individual prospective user. So for example, in the NECS, users are categorised into three broad categories: subscribers, users and certifiers[21]. To become registered as a subscriber, the practitioner, or an officer of a business entity authorised to make the application (termed authorised officer), must complete an online application form and sign it with his/her digital signature certificate[22]. The authorised user can then nominate others to be users of the system.[23]

B *Preparation, lodgement, examination and registration*

In all systems, land title instruments are prepared and lodged electronically.[24]

---

[21] Subscribers are corporations, partnerships, associations, government agencies and natural persons meeting the minimum requirements for representing clients in using the NECS. Subscribers are represented by an authorised officer. The term 'client' means registered proprietors, vendors, purchasers, caveators, mortgagees, mortgagors and others with interests in land or parties to a transaction in land. Users are employees or contractors authorised by a subscriber to prepare transaction workspaces under supervision. Certifiers are industry practitioners employed by or contracted to a subscriber and authorized by that subscriber to certify and sign instruments. See National Electronic Conveyancing Office, 'Draft Operations Description for a National Electronic Conveyancing System V.6' (National Electronic Conveyancing Office, 2007), [4.4].

[22] The manner in which the digital signature certificate may be obtained is discussed further below.

[23] For more on the registration process, see National Electronic Conveyancing Office, 'Draft Operations Description for a National Electronic Conveyancing System V.6' (National Electronic Conveyancing Office, 2007), [9.1.2.1] – [9.1.2.5]. For the purposes of this paper, these individuals who are entitled to nominate other users will be called 'nominating officers'.

[24] For a general overview of the preparation and lodgement process for New Zealand, Ontario and British Columbian system, see Rouhshi Low, 'Maintaining the Integrity of the Torrens System in a Digital Environment: A Comparative Overview of the Safeguards Used Within the Electronic Land Systems in Canada, New Zealand, United Kingdom and Singapore' (2005) 11(2) *Australian Property Law Journal* 155. It is likely that the NECS will be similar to the New Zealand system: National Electronic Conveyancing Office, 'Draft Operations Description for a National Electronic Conveyancing System V.6' (National Electronic Conveyancing Office, 2007), [9.25] – [9.26]. In the Victorian system, the electronic workspace is called the Electronic Lodgement File (ELF): Department of Sustainability and

In terms of examination and registration of instruments that have been lodged at the Land Titles Office, it appears that both Canadian systems as well as the NECS and Victorian EC system[25] are/will be limited to the electronic submission of documents and do not make provision for any automatic updates of the register. Manual intervention by staff of the Land Titles Office in examining and processing the electronic document is still required.[26]

This is in contrast to the system in New Zealand where it is possible, depending on the category of e-dealing, that upon lodgement of the e-dealing, it is registered immediately and the titles register automatically updated without manual intervention by LINZ.[27]

C *Execution and witnessing of land title instruments*

In the systems in New Zealand and Ontario, clients[28] no longer physically sign land title instruments for lodgement and registration. Rather it is the authorised user with

---

Environment, *Fact Sheets – Online Lodgement and Settlement* (2008) <http://www.landexchange.vic.gov.au/ec/s_factsheets.html> at 25 November 2008.

25 For NECS, see: National Electronic Conveyancing System, *How NECS Will Work* (2005) <http://www.necs.gov.au/default.aspx?ArticleID=50#WHAT%20NECS%20DOES%20NOT%20COVER> at 5 June 2007. For the Victorian EC System, see Department of Sustainability and Environment, *Fact Sheets – Online Lodgement and Settlement* (2008) <http://www.landexchange.vic.gov.au/ec/s_factsheets.html> at 25 November 2008.

26 Rouhshi Low, 'Maintaining the Integrity of the Torrens System in a Digital Environment: A Comparative Overview of the Safeguards Used Within the Electronic Land Systems in Canada, New Zealand, United Kingdom and Singapore' (2005) 11(2) *Australian Property Law Journal* 155, 176.

27 New Zealand Law Society, *EDealing Guidelines (for Electronic Registration)* (2008) < http://www.lawsociety.org.nz/home/for_lawyers/resources> at 22 January 2009. The categories of e-dealing are (1) AUTO REG – automatically registrable e-dealing which is automatically registered on submission without manual intervention from LINZ (2) LODGE WITH TEMPLATE – lodged e-dealing is manually processed before being registered in Landonline and (3) LODGE WITH IMAGE – scanned or attached electronic file to a lodged e-dealing is manually processed by LINZ before being registered in Landonline.

28 The term 'client' will be used in this paper to denote those who wish to deal with property. It would include registered proprietors, purchasers, mortgagees, mortgagors and any other person with an interest in land or a party to a transaction in land. It would also include attorneys acting on behalf of the donor of the power of attorney.

signing privileges[29] who will sign the relevant instruments electronically lodged for registration. This signature by the authorised user with signing privileges is a digital signature and is not witnessed.

To authorise the user to digitally sign the electronic instrument, all electronic systems require some evidence of client authorisation. Usually this is evidenced by the client signing (handwritten signature) on a client authorisation form and this signature is witnessed (also a handwritten signature).[30]

1 *Authorised user's digital signature*

In all the electronic registration systems public key cryptography administered via a public key infrastructure (PKI)[31] system is the technology used for digitally signing electronic instruments.[32] In Ontario, it is called the PSP, in New Zealand, the 'Digital

---

[29] The term 'signing privileges' refer to authorised users who are able to digitally sign instruments.

[30] In New Zealand, for example, evidence of client authorisation may be provided using a form produced by the New Zealand Law Society, called the Authority and Instruction (A&I) Form, available from the New Zealand Law Society website at: http://www.lawsociety.org.nz/home/for_lawyers/resources. In Ontario, evidence of client authorization is provided by a document called the Acknowledgement and Direction form. A sample acknowledgement and direction form can be found at Teranet Inc, *Acknowledgment and Direction* <http://www.teraview.ca/resupgrades/downloads/ADR.pdf> at 22 January 2009. At the time of writing, both NECS and the Victorian EC also require client authorisation. For the NECS see National Electronic Conveyancing Office, 'Draft Operations Description for a National Electronic Conveyancing System V.6' (National Electronic Conveyancing Office, 2007), [9.2.3.3] and National Electronic Conveyancing System, *Expert Advice on NECS* <http://www.necs.gov.au/default.aspx?FolderID=116> at 20 January 2009. The Victorian EC client authorisation form is called a representation agreement. See Department of Sustainability and Environment, *Fact Sheets – What is Electronic Conveyancing* (2008) <http://www.landexchange.vic.gov.au/ec/s_factsheets.html> at 25 November 2008.

[31] For an explanation of this technology see Sharon Christensen, William Duncan and Rouhshi Low, 'Moving Queensland Property Transactions to the Digital Age: Can Writing and Signature Requirements Be Fulfilled Electronically?' (Centre for Commercial and Property Law Queensland University of Technology, 2002), 51-52.

[32] See Rouhshi Low, 'Maintaining the Integrity of the Torrens System in a Digital Environment: A Comparative Overview of the Safeguards Used Within the Electronic Land Systems in Canada, New Zealand, United Kingdom and Singapore' (2005) 11(2) *Australian Property Law Journal* 155.

Certificate' and in British Columbia, the 'Juricert authenticated digital certificate'. In both the NECS and the Victorian EC system, it appears that a Grade 2 Gatekeeper-compliant Australian Business Number-Digital Signature Certificates (ABN-DSCs) will be used.[33]

In all systems, users wanting to obtain a digital certificate or PSP[34] to digitally sign instruments must undergo a registration process. In British Columbia, lawyers or notaries apply to Juricert[35] who validates the identity and professional credentials of these applicants. In the New Zealand and Ontario systems, since the digital certificate and PSP is used both to digitally sign instruments and to access the system, the process for obtaining the digital certificate/PSP is as described above.

As for the NECS and the Victorian EC System, the application process for obtaining a DSC will depend on the entity issuing the DSC. Generally speaking, for the Australian Business Number-Digital Signature Certificates (ABN-DSCs), which are a type of Non-Individual Grade 2 digital certificate,[36] a 100-point identity verification check is required but only the authorised officer of the organisation has to go through a personal identification check.[37]

---

33 National Electronic Conveyancing Office, 'Draft National Business Model for the establishment of a National Electronic Conveyancing System V.10' (National Electronic Conveyancing Office, 2007), [11] and see Department of Sustainability and Environment, *Fact Sheets – Digital Signing Certificates* (2008) <http://www.landexchange.vic.gov.au/ec/s_factsheets.html> at 25 November 2008. Also see National Electronic Conveyancing Office, *Expert Advice on NECS* <http://www.necs.gov.au/default.aspx?FolderID=116> at 20 January 2009 where additional advice was obtained on digital signing certification for the NECS.

34 For the purposes of this paper, the term 'digital certificate' is used to describe the instrument used to digitally sign instruments in New Zealand, British Columbia, NECS and Victorian EC while the term 'PSP' used to describe the instrument in Ontario.

35 Land Title and Survey Authority of British Columbia - Land Title Division, 'Land Titles Electronic Filing System (EFS) User's Guide' (26 July 2006), 31. The Juricert website is at http://www.juricert.com/index.cfm.

36 See Verisign, *ABN-DSC Digital Certificate* <http://www.verisign.com.au/gatekeeper/abndsc-info.shtml> at 22 January 2009.

37 See Verisign, *Gatekeeper Digital Certificates Overview* <http://www.verisign.com.au/gatekeeper/overview.shtml> at 22 January 2009.

2 *Classes of authorised users entitled to digitally sign instruments*

In all the systems, the class of persons able to digitally sign instruments is restricted. In the New Zealand system for example, eDealings may only be signed on behalf of their clients by conveyancing professionals.[38]

In the NECS, only certifiers may digitally sign instruments and in the Victorian EC System, subscribers digitally sign instruments created on the Victorian EC System.[39] In British Columbia, any lawyer or notary may digitally sign, so long as the lawyer/notary has been Juricert authenticated.[40] Thus it appears that for all systems solicitors fall within the class of users able to digitally sign instruments.

D *The paper certificate of title*

1 *Use of the paper certificate of title*

In the systems in New Zealand[41], British Columbia[42] and Ontario[43], paper certificates are no longer used. At the time of writing, it is unclear whether certificates of title

---

38 New Zealand Law Society, *EDealing Guidelines (for Electronic Registration)* (2008) <http://www.lawsociety.org.nz/home/for_lawyers/resources> at 22 January 2009. The EDealing Guidelines describes 'conveyancing professional' as a practitioner or licensed landbroker. It should be noted that licensed landbrokers will soon be replaced by conveyancing practitioners: Warren Moyes, Senior Advisor to the Registrar-General of Land, Land Information New Zealand wmoyes@linz.govt.nz, email (23 January 2009) and *Lawyers and Conveyancers Act 2006* (NZ).

39 See National Electronic Conveyancing Office, 'Draft Operations Description for a National Electronic Conveyancing System V.6' (National Electronic Conveyancing Office, 2007), [4.4] and Department of Sustainability and Environment, *Fact Sheets – Digital Signing Certificates* (2008) <http://www.landexchange.vic.gov.au/ec/s_factsheets.html> at 25 November 2008.

40 Darcy Hammett, Director of Strategic Operations, Land Title and Survey Authority of British Columbia <Darcy.Hammett@ltsa.ca>, email (25 May 2006).

41 Section 18 of the *Land Transfer (Computer Registers and Electronic Lodgement) Amendment Act* 2002 (NZ) prohibits the Registrar from issuing certificates of title for electronic transactions land and if land is declared under s 25 of the Act to be electronic transactions land, all certificates of title for that land are cancelled as from the date on which the declaration takes effect. Section 25 of the Act allows the Registrar to declare land to be 'electronic transactions land' by notice in the New Zealand gazette and such a declaration under this provision was published with effect from 14 October 2002: New Zealand Gazette 2002, Issue 150, p 3895.

42 Duplicate titles cannot be obtained for mortgaged land but may be issued for unmortgaged land on the written application of its registered owner in fee simple: see *Land Title Act RSBC* 1996 s 76(1).

will be used in the NECS, as the issue is still the subject of national uniformity consultations.[44]

For the Victorian EC system it appears that, in order to use the EC system, if an electronic certificate of title (eCT) does not exist for the land that is the subject of a transaction, then the subscriber in possession of the paper certificate of title (pCT) for the land must apply to Land Victoria for the pCT to be converted into an eCT. The pCT must be surrendered to the Registrar. The subscriber making the application obtains eCT control and this can now be used in the EC system.[45]

2 *Use of a client identification process and certifications as to identity*

In some electronic registration systems, instead of requiring production of the paper certificate of title as evidence of a right to deal, there is a formal client identification process. This is the case in the New Zealand system, where client identification must be established when the A&I form is completed and certifications made that reasonable steps have been taken to confirm identity.[46] It appears that the NECS[47] and Victorian EC[48] will follow a similar format to New Zealand.

---

43 See *Land Titles Amendment Act 1979* (Ont) ss 32 & 33.

44 See National Electronic Conveyancing Office, 'Draft Operations Description for a National Electronic Conveyancing System V.6' (National Electronic Conveyancing Office, 2007), [9.2.6.15].

45 Department of Sustainability and Environment, *Fact Sheets – Working with Certificates of Title* (2008) <http://www.landexchange.vic.gov.au/ec/s_factsheets.html> at 25 November 2008.

46 Section 164A(3) *Land Transfer Act 1952* (NZ). Only practitioners may make certifications: s 64B *Land Transfer Act 1952* (NZ). At the time of writing, s 2 of the *Land Transfer Act 1952* (NZ) defines practitioner as 'a practitioner within the meaning of s 6 of the *Lawyers and Conveyancers Act 2006* (NZ) or a landbroker licensed by the Registrar under s 229 of the *Land Transfer Act 1952* (NZ) but as noted above, licensed landbrokers will soon be replaced by conveyancing practitioners.

47 At the time of writing, it appears that the representative subscriber will be required to verify their client's identity. The precise procedure involved is unclear at this stage as it is the subject of national uniformity consultations. See National Electronic Conveyancing Office, 'Draft Operations Description for a National Electronic Conveyancing System V.6' (National Electronic Conveyancing Office, 2007), [9.3.2] and [9.2.3.2]. Also see National Electronic Conveyancing System, *Expert Advice on NECS* <http://www.necs.gov.au/default.aspx?FolderID=116> at 20 January 2009.

48 The identity check will be performed when the representation agreement is completed. Subscribers may be verifiers of identity: see Registrar's Requirements: Department of Sustainability and Environment, *Electronic Conveyancing – Registrar's Requirements Release 3* (2008) 9 <http://www.landexchange.vic.gov.au/ec/r_regdocs.html> at 25 November 2008.

In contrast, in the Ontario[49] and British Columbian[50] systems, there is no specific requirement for identity verification procedures. Certifications as to identity are not required.

IV DISCUSSION: IMPLICATIONS FROM A FRAUD RISK PERSPECTIVE

In this section, implications from a fraud risk perspective arising from the above common and differing features will be discussed. Where, due to the scope of this paper, it is not be possible to engage in an in-depth discussion of the issues raised, they will be flagged for further research.

A *Access*

One implication arising from restricted access rather than open access is that it potentially improves security by restricting fraud to insiders - those who have access to the system. Opportunities to perpetrate fraud by outsiders are potentially reduced because they would need to acquire access to the system first before they can perpetrate fraud.[51] There are two provisos to this conclusion:

First, restricted access as a security measure may only have an effect on some types of fraud, not all. Out of the types of frauds capable of being perpetrated – forgery,

---

[49] Note that the Law Society of Upper Canada has recently produced a document outlining the steps required of a lender in a mortgage or loan transaction to ensure adequate care and skill is taken in mortgage or loan transactions. See: Law Society of Upper Canada, *Due Diligence in Mortgage or Loan Transactions* (2008) <http://rc.lsuc.on.ca/jsp/fightingRealEstate/index.jsp> at 4 November 2008.

[50] The recommendation from the Law Society of British Columbia is for solicitors to obtain some sort of picture identification. See Law Society of British Columbia, *Real Estate Fraud - A Prevention Primer* (2005) <http://www.lawsociety.bc.ca/publications_forms/iissues/05-03_risk.html> at 22 January 2009.

[51] It was noted by Smith that 'insiders' and 'outsiders' is the 'most general classification of people who could possibly have access to a particular computing system'. Smith classifies insiders as 'people with an established relationship with the system's proprietor. Typical insiders are employees of the proprietor's organization'. Outsiders are classified as 'people without a similar relationship to the organization': see Richard Smith, *Authentication: From Passwords to Public Keys* (2002), 73. In an electronic registration system, insiders would include employees of authorised users of the system (such as solicitors working in a law firm) and employees of the system itself.

identity fraud, fraudulent alterations and fraudulent misrepresentations, some of these require access for fraud to be perpetrated, some do not. For example, identity fraud does not require access for the fraud to be perpetrated whereas for fraudulent alterations, access will now be required because access is required to alter the necessary land title documents. Thus restricting access could mean reduced opportunities for fraudulent alterations by outsiders but would not have any effect on identity fraud.

Secondly, the potential of restricted access in improving security against fraud depends on the strength of the system's security.[52] As noted above, there are various methods of controlling access and various ways by which applicants may apply for access.

Arguably systems using multi-factor authentication such as a combination of token and knowledge based authentication methods will provide greater security than those using single factor authentication such as those using usernames and passwords (knowledge based) because it means that the fraudulent person must first obtain the token, and then guess or ascertain the password, before he or she can access the system. In systems using knowledge based authentication methods, all the fraudulent person has to do is to obtain the username and password.[53]

In terms of the registration process, requiring all potential users to go through the registration process to gain access where each applicant's identity is independently verified potentially provides better security than a nomination process because in a nomination process, the integrity of the process is dependent on the nominating officer. It is beyond the scope of this paper to discuss the methods in which the registration process including where a nomination procedure is used could be strengthened, but this could be the subject of further research.

---

[52] This type of risk was identified in the risk assessment conducted by Clayton Utz on behalf of NECS, that the NECS system security may be inadequate enabling a third party to enter NECS (such as by hacking into the system) and change or delete workspace data: see National Electronic Conveyancing Office, 'Risk Assessment of the National Electronic Conveyancing System' (National Electronic Conveyancing Office, 2007), Volume 3, 23, risk reference 31 and risk reference 3.

[53] See for example, National Research Council (U.S) Committee on Authentication Technologies and Their Privacy Implications, *Who Goes There: Authentication Through the Lens of Privacy* (2003) and Christina Braz and Jean-Marc Robert, 'Security and Usability: The Case of the User Authentication Methods' (Paper presented at the Proceedings of the 18th International Conference on Association Francophone d'Interaction Homme-Machine, Montreal, 2006), 201.

However to successfully perpetrate fraud in an electronic registration system, the fraudulent person must not only be able to access the system, but must also be able to digitally sign any instrument prepared on the system. This suggests that it is the security surrounding digital certificates/PSPs that is critical as they are used for digital signatures. The potential for fraud arising from misuse of the digital certificate/PSP is discussed below.

B *Preparation, lodgement, examination, registration*

In all electronic systems, land title instruments are prepared electronically. This may make it easier for fraudulent persons with access to the system to perpetrate fraudulent alterations, because unlike a physical alteration, an electronic alteration on an electronic document will not leave any physical evidence of the alteration.

In the paper system, the practice of the Land Titles Office manually checking instruments lodged for registration before updating the register may be said to act as a safeguard against this type of fraud, since any alteration of an instrument might leave some form of a physical mark which might then be noticed by the officer and appropriate action may then be taken. Of course the effectiveness of this safeguard depends on the vigilance of the examining officer.

Should manual examinations and manual updating of the register be continued in an electronic system so as to continue this layer of security? One view is that automatic registration without manual intervention will make 'title less secure'.[54] Since New Zealand is the only system thus far which allows for automatic registration, monitoring of that system *vis-a-vis* fraud claims will be useful in determining the effects of removing manual examinations on fraud. One point to consider here is that electronic systems can use technology to improve security and minimise fraud. In particular, one feature of public key cryptography technology is that any alterations made to a document after a digital signature has been applied to it will invalidate the digital signature.[55] Thus this feature of technology, together with restricted access,

---

[54] See Rod Thomas, 'Fraud, Risk and the Automated Register' in David Grinlinton (ed), *Torrens in the Twenty-first Century* (2003) 349, 366-367 raising this concern in New Zealand – as the New Zealand system allows the register to be updated with any manual intervention.

[55] These features are available in both the New Zealand and Ontario systems. In New Zealand, if an e-dealing is edited by anyone after it has been certified and signed, the Landonline system clears all certifications and signatures so that the e-dealing must be re-certified and re-signed by all parties to the e-dealing before Landonline will accept the e-dealing for lodgement and registration: Land Information New Zealand, *Landonline E-*

may give electronic systems a different, but not necessarily less effective, layer of security against fraudulent alterations. The use of PKI technology for digital signatures may also enable the system's administrators to maintain an audit trail of those using the system which may assist in tracking fraud.

C *Execution and witnessing*

1 *Authorised users digitally signing land title instruments*

It can be seen from the discussion in [III] that in all electronic systems, it will be authorised users with signing privileges, and not the client, who will be required to digitally sign land title instruments before it can be lodged for registration. This arguably presents one of the greatest implications of moving to an electronic system – an introduction of a new fraud risk – fraudulent misuse of a digital certificate/PSP to digitally sign land title instruments and lodging them for registration.[56]

It is beyond the scope of this paper to consider in detail how a fraudulent person may obtain access to a digital certificate/PSP. Issues to consider here include whether and if so how an existing user's digital certificate/PSP may be 'targeted' to perpetrate fraud and as an alternative, whether it may be possible for the fraudulent person to 'target' the application process instead in order to obtain a digital certificate/PSP.

For the former, points to consider include the manner in which the digital certificate/PSP is generated, issued, password protected and stored by the user, because these impact on the ability of the fraudulent person to gain access to a digital certificate/PSP.[57]

Dealing Handbook for Students (2008) <http://www.landonline.govt.nz/edealing/training-resources/education-resources/index.asp> at 8 April 2008. Similarly in the Ontario system, any changes made to an electronic document after a document has been digitally signed triggers the removal of those digital signatures and the document will need to be re-signed by those parties: Teranet Inc, *Teraview Reference Guide 5.3.3* (2007) <http://www.teraview.ca/resupgrades/ru_manuals.html> at 28 April 2008. See also Simon Hally, 'How Secure is E-Registration' (2005) 29(7) *Canadian Lawyer* 47, 47.

[56] Perry in 2003 raised this issue of the security of using digital signatures in an electronic conveyancing system proposed for England and Wales: Raymond Perry, 'E-Conveyancing-Problems Ahead?' (2003) 67 *The Conveyancer and Property Lawyer* 215, 218. In Rouhshi Low, 'Opportunities for Fraud in the Proposed Australian National Electronic Conveyancing System: Fact or Fiction?' (2006) 13(2) *Murdoch University Electronic Journal of Law* 225 this was also identified as a new type of fraud within NECS.

[57] These were also identified in Rouhshi Low, 'Opportunities for Fraud in the Proposed Australian National Electronic Conveyancing System: Fact or Fiction?' (2006) 13(2) *Murdoch*

For example, an insecure method of generation and issuance may provide the fraudulent person with an opportunity to intercept and gain access to the digital certificate/PSP. Unsecure password practices such as disclosing passwords to others or re-using passwords for various applications increases the risk of the fraudulent person being able to misuse a user's digital certificate/PSP. The fraudulent person may also obtain an existing digital certificate/PSP if the authorised user is careless about where it is kept. Thus from a fraud risk perspective, further research into how users may be encouraged to adopt secure practices is vital to enhancing security.

In terms of the registration process, the strength of the system's registration processes is vital as it assists in preventing fraudulent applications for access and/or digital certificates/PSPs[58] and helps to ensure that only legitimate users are given access and/or issued with digital certificates/PSPs. The reasoning in [IVA] applies here.

It is observed that these considerations do not arise in the paper registration system. They are unique to an electronic system because of the use of technology to replace the handwritten signature. In the paper system, handwritten signatures can be forged, but there was never a requirement or a need for individuals to keep their signatures safe. It is simply not possible. Replacing handwritten signatures with digital signatures introduces a new element into the process. And because of the potential for fraud whether because the fraudulent person has managed to obtain an existing digital certificate/PSP or circumvented the registration process to obtain one, the use of digital signatures therefore imposes 'new' obligations on users as well as the entity responsible for the registration process that do not exist in the paper system. The user is now responsible for keeping the digital certificate/PSP safe. The entity issuing the digital certificate/PSP is responsible for developing and maintaining effective registration processes to minimize the risk of a fraudulent person impersonating an authorised user. In fact, attacking the registration process in this manner is an additional avenue for the fraudulent person to perpetrate identity fraud so that it could be said that in an electronic system, there might be two

---

University Electronic Journal of Law 225 as important points of consideration in terms of preventing fraud in the NECS.

58 This occurred in 2001where VeriSign (a Microsoft product) was tricked by an unknown individual pretending to be a Microsoft executive into issuing false digital certificates in Microsoft's name. VeriSign officials assumed responsibility for the mishap, stating that it was the failure of the human part of the verification process: John Markoff, *Warning From Microsoft on False Digital Signatures* (2001) <http://query.nytimes.com/gst/fullpage.html?res=9406E7DC143CF930A15750C0A9679C8B63> at 21 January 2009.

opportunities for identity fraud: (i) identity fraud of the owner of the land and (ii) identity fraud of an authorized user of the system.

These additional responsibilities of adopting safe practices and processes also raise regulatory and compliance issues which are beyond the scope of this paper but could be the subject of future research:

- should measures, such as best practice guidelines on usages, be imposed to ensure safe practices?
- if so, by whom should they be imposed and how can they be imposed, for example, contractually or legislatively?
- should there be rules or legislation governing liability issues in the event of fraud occurring through the carelessness of either party?

In Ontario and New Zealand rules and obligations surrounding the use of digital certificates/PSP exist.[59] A comparison of these rules and obligations with those proposed by the Victorian EC and the NECS will assist in assessing the value of such measures and the most suitable manner in which they may be imposed.

2 *Restricting digital signature abilities to certain authorised users*

In all system, digital signing abilities are restricted to authorised users, and in some cases, to specific classes of authorised users. As observed in [3], solicitors are likely to fall within this class. One potential implication from this is that it might provide solicitors with a greater opportunity to perpetrate fraud than what they currently possess in the paper registration system because in an electronic system:

- they will have access to the system;
- they will able to digitally sign instruments on behalf of clients; and
- their digital signature on the instrument need not to be witnessed.[60]

So to perpetrate fraud in an electronic registration system, the solicitor would not even need to forge the victim's signature, or mislead the client into signing

---

[59] These were discussed in Rouhshi Low, 'Opportunities for Fraud in the Proposed Australian National Electronic Conveyancing System: Fact or Fiction?' (2006) 13(2) *Murdoch University Electronic Journal of Law* 225.

[60] This conclusion was also reached in Rouhshi Low, 'Opportunities for Fraud in the Proposed Australian National Electronic Conveyancing System: Fact or Fiction?' (2006) 13(2) *Murdoch University Electronic Journal of Law* 225. Also see Rod Thomas, 'Fraud, Risk and the Automated Register' in David Grinlinton (ed), *Torrens in the Twenty-first Century* (2003) 349 where Thomas raised similar concerns in New Zealand.

documents, or create false powers of attorney, or fraudulently alter instruments, as is the case in the paper registration system. All that the solicitor would have to do would be to prepare the instrument, digitally sign it and submit it to the Land Titles Office for registration. As noted above, being able to fraudulently use a digital certificate/PSP to digitally sign instruments for lodgement and registration is a new opportunity for fraud in an electronic system. As seen in the discussion here, solicitors will have the greatest opportunity to perpetrate this new type of fraud.

Thus the concern is that in an electronic system, because solicitors play a greater role, but without corresponding checks and balances, the system affords them with a better opportunity to perpetrate fraud. It is therefore imperative that security mechanisms that can be employed to minimise this fraud risk be developed. It is beyond the scope of this paper to discuss potential security mechanisms of this nature but this could be the subject of future research.[61]

3 *Client no longer signing land title instruments*

In all the electronic systems, clients no longer sign land title instruments for registration. Rather an authorisation form is signed instead. This change in practice may see a shift in forgery cases – instead of forging the signature of the victim on the land title instrument, fraudulent persons will now have to forge the signature of the victim on the authorisation form**.**

This coupled with the observation in [IVC2] that authorised users with digital signing privileges will digitally sign land title instruments, show that in terms of forgery of signatures, the fraudulent person has a choice in an electronic system - either target the client's handwritten signature on the authorisation form – by manually forging it, or target an authorised user's digital certificate/PSP (as discussed in [IVC1]).

It may also see a change in the perpetration of fraudulent misrepresentation. Since only authorised persons have access to the system to prepare the relevant land title instruments which must be digitally signed before lodgement can occur, it would not be possible for fraudulent persons to either prepare for themselves the relevant land title instrument or to direct a solicitor to prepare one before misleading the victim

---

[61] Some of these measures were discussed in Rouhshi Low, 'Opportunities for Fraud in the Proposed Australian National Electronic Conveyancing System: Fact or Fiction?' (2006) 13(2) *Murdoch University Electronic Journal of Law* 225 in the context of the NECS, such as the use of pre-employment screening techniques, monitoring of employees and auditing mechanisms. They could be further developed. In addition, the safety mechanism discussed below in [4.4] – use of a client ID is also relevant here.

into signing it. Instead, the fraudulent person would now have to mislead the victim into signing the authorisation form.[62]

D *Non-use of the certificate of title*

The concern in abolishing the paper certificate of title in an electronic registration system is that it will result in more identity fraud. When the New Zealand system was introduced, Thomas argued that '[T]he absence of an outstanding duplicate certificate of title (or anything in substitution of the same) is argued to be a key flaw in the new system, making it more vulnerable to fraud'.[63]

But will this be the case? It is argued that identity fraud might be perpetrated in an electronic registration system in the same way as in the paper registration system – when the fraudulent person is able to successfully impersonate the victim of the fraud to convince the authorised user responsible for the transaction that he or she has a right to deal with the land. The difference is that in the paper registration system, since the certificate of title is the document used to evidence a right to deal with the land, identity fraud uses the certificate of title. In an electronic registration system, the manner in which identity fraud may be perpetrated would depend on the system and how identity and right to deal might be established.

For example, if certain types of identity documents, such as driver's licence or passports, are used, identity fraud is possible if:

> the fraudulent person can obtain genuine identity documents belonging to the victim and use them, alone or in collusion with someone else, to impersonate the victim; or
>
> the fraudulent person is able to falsify identity documents and is able to use them, whether alone or in collusion with someone else, to impersonate the victim. These falsified documents may be those of a genuine or a fictitious person.

---

[62] In Rouhshi Low, 'Opportunities for Fraud in the Proposed Australian National Electronic Conveyancing System: Fact or Fiction?' (2006) 13(2) *Murdoch University Electronic Journal of Law* 225 [4.2] the conclusion drawn was that in the NECS, this type of fraud will be eliminated because subscribers will be digitally signing the land title instrument not the victim. Whilst this is true, it may be also possible for the fraudulent person to mislead the victim into signing the authorisation form instead and the authorised user accepts the authorisation form believing that the victim understands its effects.

[63] Rod Thomas, 'Fraud, Risk and the Automated Register' in David Grinlinton (ed), *Torrens in the Twenty-first Century* (2003) 349, 349.

In the Victorian EC System where electronic certificates of title are used in conjunction with an identity verification process, the fraudulent person would have to circumvent the identity verification process as described above as well as direct the authorised user in control of the electronic certificate of title to nominate the electronic certificate of title to the transaction.

If, however, a paper certificate of title already existed but has not been converted into an electronic certificate of title, the fraudulent person would have to produce the paper certificate of title so that it could be converted into an electronic certificate of title and nominated to the transaction. The certificate of title and the identity documents used for the identity verification process could be genuine or falsified.

So the requirement that an electronic certificate of title must be nominated to the transaction before the transaction can proceed may act as a safeguard against identity fraud in the sense that it requires the fraudulent person to take that extra step – to either obtain the paper certificate of title so that it may be converted into an electronic certificate of title and nominated to the fraudulent transaction or to direct the authorised user in control of the electronic certificate of title to nominate it to the fraudulent transaction.

But there may be ways of circumventing this. For example, paper certificates of title of other identity documents may be forged. More importantly, as the authorised user is given control of certificates of title in electronic format, the need for certificates of title will not act as a safeguard against fraud perpetrated by the authorised user; as they may simply prepare a transaction, nominate the electronic certificate of title to the transaction, digitally sign it and lodge it for registration. These transactions would appear on the face of it to be legitimate transactions.

Hence it is argued that the identity verification process is vital in curbing identity fraud. A paper certificate of title may be one component of this process. If a paper certificate of title is not used other identity documents will take its place, so it is still the identity verification process that is important, not the document itself. As noted by Cocks & Barry: 'It is the identity of the party that is crucial, not the physical possession of the paper title. Fraud is perpetrated when someone impersonates another by stealing their identity. Having possession of the paper title is not enough in itself, it is simply indicative of identity'.[64]

---

[64] Russell Cocks and John Barry, 'Electronic Conveyancing: Challenges for the Torrens System' (2001) 8(3) *Australian Property Law Journal* 270, 276.

An alternative safety mechanism to the certificate of title that has been suggested is to issue identification numbers (client IDs) to registered owners of land and to require this number to be entered into the electronic transaction before the transaction can be accepted for lodgement by the relevant Land Titles Office.[65] This may make it more difficult to perpetrate fraud, because the fraudulent person would need to know the identifier to successfully lodge the transaction. This is similar to using an electronic certificate of title, except that in that case, these are in the control of the authorised user of the system, whereas it is the registered proprietor who is in control or in possession of client ID.

At the time of writing this paper, none of the electronic systems use this safety mechanism. This makes it difficult to assess its viability and value as a fraud prevention mechanism. Its ability to combat fraud will to a certain extent depend on the ability of clients in keeping the client ID safe. Further, it may not prevent fraud in situations where the fraudulent person is able to impersonate a client and obtain a client ID from the system or in situations where the client shares the ID with the fraudulent person.

The use of client ID also raises other issues including:

- who should be responsible for assigning these client IDs?
- when and how should client IDs be assigned? The transmission of the client ID to the registered proprietor must be secure, to prevent fraudulent interceptions of the client ID;
- should the client ID be linked to the registered proprietor or to the land? For example, if the registered owner sells the property, will the new owner take over the client ID of the previous owner or will a new client ID be issued?

This technological option could be further investigated so that a proper assessment can be made as to whether it would useful to incorporate this mechanism in an electronic system.

---

[65] This safety measure was suggested by Thomas, for the New Zealand electronic land registration system. See: Catriona MacLennan, 'Mortgage Frauds Prompt Calls for System Changes' (2006) 2 *Law News* 1. It was also discussed in Rouhshi Low, 'Opportunities for Fraud in the Proposed Australian National Electronic Conveyancing System: Fact or Fiction?' (2006) 13(2) *Murdoch University Electronic Journal of Law* 225. and in Celia Hammond, 'The Abolition of the Duplicate Certificate of Title and its Potential Effect on Fraudulent Claims Over Torrens Land' (2000) 8 *Australian Property Law Journal* 115. Note that this safety measure may also assist in minimizing fraud by solicitors (misuse of digital certificate/PSP) as discussed above in p 124,125.

The discussion above demonstrates the importance of identity verification procedures in combating identity fraud. But its success depends entirely on the vigilance of those responsible for verifying identity[66] so that it is equally important to develop measures to encourage due diligence during the identity verification process. It is beyond the scope of this paper to discuss these in details but issues to look at here include:

- whether it should be left to individual authorised users to formulate internal policies and practices in these matters, or whether the system should impose a formal process for verification of identity with identified best practice guidelines.
- whether imposing penalties for non-compliance could be another strategy for encouraging compliance. If so:
    - what type of penalties may be imposed?;
    - how can these penalties be imposed, contractually or legislatively?

Perhaps one penalty that may be examined is disentitling the party failing to verify identity of an indefeasible title. In Queensland[67] mortgagees must take reasonable steps to verify the identity of the person purporting to sign a mortgage as mortgagor. As noted by Weir, these provisions were introduced to 'create greater discipline in the finance industry by punishing lax identification procedures when dealing with persons purporting to be registered owners'.[68] The effectiveness of this measure in countering identity fraud should be monitored.

Technological advances may also be a contributing factor in the ability of criminals to perpetrate identity fraud. Of particular concern are technological advances in computer software and hardware which have provided criminals with greater capabilities of producing high quality fake or forged identity documents.[69] In this

---

66 This point was also raised in Rouhshi Low, 'Opportunities for Fraud in the Proposed Australian National Electronic Conveyancing System: Fact or Fiction?' (2006) 13(2) *Murdoch University Electronic Journal of Law* 225.

67 See ss 11A and 11B of the *Land Title Act 1994* (Qld). Indefeasibility is denied in situations where the mortgagee fails to comply with ss 11A or 11B and this failure enabled the mortgage to be executed by someone other than the true owner: s 185(1A) See *Land Title Act 1994* (Qld).

68 Michael Weir, 'Indefeasibility: Queensland style' (2007) 15(1) *Australian Property Law Journal* 79, 79.

69 This occurred in New Zealand in 2005 where the fraudulent person used fake passports, bank statements and tax certificates to convince three lawyers to arrange mortgages over homes which the fraudulent person did not own: See Catriona MacLennan, 'Warning

situation, despite an identity verification process, it will be difficult to prevent identity fraud because of the difficulty in detecting whether the identity document is genuine or false.

This ability to circumvent identity verification procedures via fake identity documents is an indication that to be effective in preventing identity fraud, the problem needs to be addressed on a wider, nationwide level, addressing issues such as improving the issuance process of identity documents, improving the accuracy of identity information held on databases and improving the security features of documents used to prove identity.[70]

Improvements in technology have also resulted in the development of a variety of malicious software or malware, such as worms, viruses and Trojan horses that criminals can use to capture information. An indication of increases in these types of attacks can be seen in a 2006 AusCERT survey which found a rise in Trojan and rootkit attacks[71] to facilitate identity fraud and reported that the increase in losses for

---

About Conveyancing Fraud Using False Passports' (2005) (39) *Auckland District Law Society Law News* 1 and Anne Gibson, 'Department Protects Homes From More Fraud', *New Zealand Herald* (Auckland), 2006.

70 For plastic cards, the technology could include security printing, micro-printing, holograms, embossed characters, tamper-evident signature panels, magnetic strips with improved card validation technologies and indent printing: Russell Smith, 'Best Practice in Fraud Prevention' (Australian Institute of Criminology, 1998) 5. Also see Rouhshi Low, 'Opportunities for Fraud in the Proposed Australian National Electronic Conveyancing System: Fact or Fiction?' (2006) 13(2) *Murdoch University Electronic Journal of Law* 225; Suresh Cugnasen and David Lacey, *Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent* (2003); Geoff Main and Brett Robson, 'Scoping Identity Fraud' (Attorney General's Department, 2001) and the Australia Government's National Identity Security Strategy: Australian Government Attorney-General's Department, *Identity Security* (2008), <http://www.ag.gov.au/www/agd/agd.nsf/Page/Crimeprevention_Identitysecurity> at 12 January 2008. See in particular the Report to the Council of Australian Governments on the elements of the National Identity Security Strategy which identifies and recommends a set of security features for proof of identity documents for the purpose of reducing the risk of forgery or unauthorised alterations to the documents. Some of these security features include the use of watermarks, hidden image and security ink. The document also recognises that improvements in biometrics technology may also see biometrics being used for identity verification: National Identity Security Coordination Group, 'Report to the Council of Australian Governments on the elements of the National Identity Security Strategy' (Attorney-General's Department, 2007), 15 & 45.

71 AusCERT, '2006 Computer Crime and Security Survey' (AusCERT, 2006), 22. For an example of a typical case study of an identity theft Trojan attack, see AusCERT, '2006 Computer Crime and Security Survey' (AusCERT, 2006), 23.

online ID theft 'may represent a changing trend for the worse, along with the relatively high levels of trojan related infections reported'.[72] This finding accords with the prediction of the Australian Crime Commission: that '[T]he incidence of high-tech/cybercrime in Australia is likely to further increase and diversify with a shift through third generation to fourth generation technologies and the introduction of new internet protocols'.[73]

Whether these predictions translate to the conveyancing sector, particularly in electronic systems where instruments are prepared and lodged online, remain to be seen. But it may serve as a warning to those using the system including the system administrators that counter measures such as firewalls and encryption techniques should be assessed and developed to combat these forms of technological attacks. Education and training should also constitute part of this package as it would be useless to have technological safeguards without a corresponding understanding of how they may be used and/or if users adopt unsafe practices.

V Conclusion

Various jurisdictions have either developed or are adapting technological systems to support or replace their paper land registration systems. The impact of this from a fraud risk perspective was explored in this paper. By comparing the salient features of fully operational, automated registration systems in New Zealand and Canada and the systems proposed in Australia, it was found that the extent of fraud risks were dependent on the types of features used. Some features, such as using multi-factor authentication methods, may provide greater security than single factor authentication methods. Any proposals to convert to an electronic registration system should first consider carefully these various features and their impact on fraud before switching to such a system. Perhaps one of the greatest risk implications identified here is that enabling electronic instruments to be lodged upon the digital signature of an authorized user potentially provides a new avenue for fraud – fraudulently using the digital certificate/PSP. It also raises new requirements that do not exist in the paper system – the need for users and the system to adopt secure practices to prevent the fraudulent use of digital certificates. This raises compliance, regulatory and liability issues that could be the subject of further research. The fact that solicitors are likely to fall within the class of users able to digitally sign instruments, lodge and

---

[72] AusCERT, '2006 Computer Crime and Security Survey' (AusCERT, 2006), 25.

[73] Australian Crime Commission, 'Submission to the Parliamentary Joint Committee on the Australian Crime Commission Inquiry into the Future Impact of Serious and Organised Crime on Australian Society' (Australian Crime Commission, 2007), 9.

register arguably provides solicitors with the greatest opportunity to perpetrate this new type of fraud. Thus in designing measures to prevent this new type of fraud, appropriate checks and balances to limit solicitors' opportunities for fraud should also be included. The rise in identity fraud and in particular the ability of criminals to use technology to perpetrate identity fraud is a concern. But arguably where technology may assist fraud, technology may also be used to prevent or minimize fraud. This is one advantage electronic systems have over paper systems – electronic systems can utilise technology as a fraud minimisation tool. This is evident from the conclusions drawn regarding reduced opportunities for fraudulent alterations in an electronic system. Thus the potential of technology in curbing fraud should not be overlooked; although as observed in this paper, it may not be effective in preventing frauds that occur prior to entry into the system, a prime example being identity fraud. But perhaps the greatest consideration identified in this fraud risk assessment is the risk of fraud through human frailty – no amount of security will prevent fraud if those involved in the system adopt unsafe practices. Hence measures to encourage secure practices should be regarded as a vital component of fraud prevention, to be developed alongside technology.