Opportunities for fraud in the proposed Australian National Electronic Conveyancing System: Fact or Fiction?

By Rouhshi Low

ABSTRACT
The advent of the Internet and increased reliance on technology has seen a move towards computerisation of the land registration process. Whilst it has been argued that electronic registration will offer a faster and more efficient and cost effective method of conveyancing, the underlying principle of the Torrens system of security and integrity of title may be threatened if electronic land registration introduces a medium by which fraud can be perpetrated with ease. The purpose of this article is to critically analyse whether the types of fraud currently occurring in the paper system can continue to occur in the proposed Australian national electronic conveyancing system, and whether the adoption of the proposed system will introduce new opportunities for defrauding individuals.

Keywords: National Electronic Conveyancing System (NECS), electronic land registration, electronic conveyancing, Torrens system, land title fraud, identity fraud

1. Introduction
The advent of the Internet and increased reliance on information technology has seen a wave of change in all areas of law and legal practice. It was only a matter of time before these changes would make their mark on the land registration process. Jurisdictions such as Canada and New Zealand have recently transformed their paper land registration processes into an electronic system. In Australia, each State and Territory in Australia has agreed to participate in the development of a national electronic conveyancing system, rather than to pursue state based electronic systems. The national electronic system is referred to as the National Electronic Conveyancing System (NECS).
A National Steering Committee, made up of government and industry representatives, and a National Electronic Conveyancing Office to support the Steering Committee has since been established. A proposed National Business Model for the Electronic Conveyancing System has also been drawn up, to be discussed in consultation forums throughout 2006 by industry and government. The aim is to complete consultation by the end of 2006/early 2007, obtain in-principle agreement to the Business Model and begin building the NECS in mid-late 2007.

It has been argued that electronic registration will offer a faster and more efficient method of conveyancing that will eliminate the current problem of the registration gap as well as increase the accuracy of the register and reduce costs. However the benefits to be gained from an electronic registration system may be outweighed by the costs of fraud if the migration to an electronic environment increases the opportunities for fraud to occur. A survey conducted by AusCERT in 2005 found that the total annual loss caused by computer crime was $16,856,900. Of this, the loss caused by identity fraud amounted to $62,000. The underlying integrity of the Torrens system of State guarantee of title would be undermined if electronic land registration introduces a medium by which fraud can be perpetrated with ease. As pointed out by Graycar and Smith:

In the past, sophisticated paper-based systems were present to reduce the opportunities for fraud involving conveyancing transactions. As we move into on-line registration of titles and electronic transactions, new opportunities arise for people within organisations as well as for external customers to misrepresent themselves and to manipulate electronic transactions for financial gain.

The purpose of this article is to critically analyse whether the types of fraud currently occurring in the paper system can continue to occur in the proposed NECS, and whether the adoption of the proposed NECS will introduce additional opportunities for defrauding individuals. This is achieved by critically analysing the types of fraud occurring in the current paper based conveyancing system so as to identify the common factors enabling these types of fraud to occur and comparing this with the proposed NECS so as to determine whether

---

4 All States and Territories are represented in the National Steering Committee.
the opportunities to commit these types of fraud in the NECS will continue to exist. Possible new opportunities for fraudulent behaviour in the NECS will also be considered. The article will also discuss possible measures that can be adopted to combat the types of fraud identified in the above analysis.

2. Incidences of paper based fraud

The author was provided with data on compensation claims made against Victoria, Queensland, South Australia and Tasmania for the period 1990 to 2005\textsuperscript{11}. The incidence of fraud evident in that data can be summarised as follows:

<table>
<thead>
<tr>
<th>State</th>
<th>Type of fraud</th>
<th>Fraudulent party</th>
<th>Transaction</th>
<th>No. of claims</th>
<th>Total fraud claims</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tasmania (1990-2005)</td>
<td>Forgery of signature</td>
<td>Family member\textsuperscript{12}</td>
<td>Transfer</td>
<td>One</td>
<td>One</td>
</tr>
<tr>
<td>South Australia (1990-2005)</td>
<td>Forgery of signature</td>
<td>Family member</td>
<td>Mortgage</td>
<td>Two</td>
<td>Four</td>
</tr>
<tr>
<td></td>
<td>Forgery of signature</td>
<td>Family member</td>
<td>Transfer of a lease</td>
<td>One</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Falsely inducing the claimant to sign the last page of what later became a memoranda of mortgage.</td>
<td>Friend</td>
<td>Mortgage</td>
<td>One</td>
<td></td>
</tr>
<tr>
<td>Queensland (1989-2005)</td>
<td>Forgery of signature</td>
<td>Family member</td>
<td>Mortgage</td>
<td>Five</td>
<td>Twenty one</td>
</tr>
<tr>
<td></td>
<td>Fraudulently executing a Power of</td>
<td>Family member</td>
<td>Mortgage</td>
<td>One</td>
<td></td>
</tr>
</tbody>
</table>

\textsuperscript{11} The author requested for but was not provided with data from Western Australia and New South Wales. Data on claims for these two States can be obtained from a study by Hammond in 2000. See Celia Hammond, 'The abolition of the duplicate certificate of title and its potential effect on fraudulent claims over Torrens land' (2000) \textit{Australian Property Law Journal} 115. The information provided by the Registrar of Titles from Victoria contained more generalised information, hence it is not reproduced in the table. The report from Victoria did note that almost all the fraud occurring in Victoria involved family members with forged mortgages. Forged transfers rarely gave rise to claims, and usually in situations involving family members: Personal communication from the Victorian Land Registry to the author in 28 September 2005.

\textsuperscript{12} The term ‘family member’ includes: husband/wife, brother/sister, son-in-law/daughter-in-law and mother-in-law/father-in-law.
Attorney and using that power to mortgage the family home
Forgery of signature
Forgery of signature
Solicitor Director of the company who had introduced the victims to purchase the property that was the subject of the fraud
Mortgage Mortgage
Six Seven

Impersonation
Trusted friend
Mortgage
One

Misleading the owner into signing mortgage documents
Accountant
Mortgage
One

3. Implications from incidences of paper based fraud

Analysis of the data provided by the Land Titles Office in Victoria, Queensland, South Australia and Tasmania reveal certain trends in the perpetration of title fraud in Australia.

First, the most common perpetrators of land title fraud in Australia appear to be those who are known to the victim of the fraud, such as the victim's family members, relatives, close friends, and the victim's solicitor or accountant. These persons are able to perpetrate the fraud as they have the means and the opportunity to do so. They are usually trusted by the victim and have access to documents required to perpetrate the fraud. Thus this type of fraud is opportunistic in nature. Fraud that is perpetrated by persons unknown to the victim, where the victim is targeted by the fraudulent person, may be referred to as professional or calculated fraud. Whilst professional fraud is not represented in the table above, it usually occurs in the context of identity theft.

Secondly, analysis of the data also shows that there are several ways in which fraud can be perpetrated. The primary method appears to be forgery of the victim's signature. However as can be seen from the table above, there are incidences where fraud has been perpetrated by impersonating the victim of the fraud and by misleading the victim of the fraud into signing the relevant documentation necessary for the perpetration of the fraud. This article will focus
on these three types of fraud for the purposes of determining whether they may be perpetrated in an electronic system of land registration.

Thirdly, the majority of fraud claims usually involve mortgages, and in some cases, a combination of transfers and mortgages. In terms of the fraud claims involving mortgages, the Victorian report on the Victorian Fraud Experience\(^{13}\) noted an increase in fraud claims involving loans sourced through mortgage brokers during the period 2003-2005. Whether this increase in claims involving mortgage brokers is a new trend in land title fraud in Australia remains to be seen.

Having determined the common perpetrators of fraud and the common methods of perpetrating the fraud, the next step is to analyse the factors existing within the current paper based conveyancing system that facilitate the occurrence of these types of fraud.

This is achieved by undertaking an analysis of case studies of fraud by forgery of signature, fraud by misleading the victim into signing relevant documentation and identity fraud. In doing so, this article will place particular emphasis on fraud perpetrated by solicitors\(^{14}\) due to the vital role played by solicitors in the conveyancing process and the possibility that this role may be increased in the NECS. Whether this will increase the opportunities for fraud by solicitors in the NECS is an important issue that should be addressed. The findings from this analysis can then be used to assist in determining whether the same opportunities for fraud will continue to exist in the NECS.

4. Analysis of case studies to determine factors enabling fraudulent behaviour

4.1 Forgery of signature

As represented in the table above in [2], the most common perpetrators of this type of fraud are usually persons who are known to the victim of the fraud, such as the victim’s family members, friends, accountant or solicitor. Below are two case studies of fraud involving forgery of signature by family members.

In *Young v Hoger*\(^{15}\), Mr and Mrs Hoger were the joint tenants of their matrimonial home. Mrs Hoger and her daughter, Denice, sought to refinance an earlier loan by making an application to PJP Mortgage Management Pty Ltd (PJP), a mortgage broker, for an advance of $447,000. This loan was to be secured by a registered mortgage over the matrimonial home. Mr Hoger was unaware of this. When PJP found a client who was prepared to make the advance, it instructed its solicitor to prepare the mortgage documents. The solicitor sent the instrument of mortgage and a solicitor’s certificate to Denice and Mrs Hoger for execution with an accompanying letter setting out...
requirements for execution. The mortgage instrument was returned by Denice
to the solicitor, bearing the purported signatures of Mr and Mrs Hoger and the
signatures of a Justice of the Peace, as witness to their signatures. The trial
judge found that Mr and Mrs Hogers’ signatures on the mortgage were forged
by Denice\(^\text{16}\). Here the daughter was able to perpetrate the fraud because:

- All correspondence from the mortgagee’s solicitor were addressed to the
daughter and to Mrs Hoger or solely to the daughter\(^\text{17}\). The solicitor
acting for the mortgagees did not have any dealings, directly or indirectly
with Mr Hoger, nor did he make any attempts to contact Mr Hoger about
the proposed loan. Had he done so, he might have discovered the fraud;

- The mortgagee’s solicitor gave to the daughter the mortgage instrument
for execution. This provided the daughter with the opportunity to forge
the signature of Mr Hoger; and

- Either the Justice of the Peace who purportedly witnessed Mr Hoger’s
signature did not follow proper attestation procedures (that is he
witnessed Mr Hoger’s signature even though it was not signed in his
presence) or Denice or Mrs Hoger forged his signature as a witness\(^\text{18}\).

In terms of the witnessing of the signatures on the mortgage, it was pointed out
by Douglas J that the mortgagee’s solicitor did not know anything about the
circumstances of the purported execution of the mortgage nor did the solicitor
speak with or make any attempt to contact the Justice of the Peace who
purportedly witnessed the signatures\(^\text{19}\). Had the solicitor contacted the Justice
of the Peace, it is possible that he may have uncovered the fraud or at least
discovered some discrepancy with the manner in which the execution was
witnessed. Having said this, the mortgage instrument that was given to the
daughter was returned to the solicitor purportedly executed by Mr Hoger and
whose signature was purportedly witnessed by a Justice of the Peace. In this
situation it is not common practice for solicitors to verify the authenticity of the
signatures on the instrument by contacting the person who witnessed the
signature. In fact, as persons who are qualified to act as witnesses under
Torrens legislation are required to follow certain procedures when witnessing
signatures\(^\text{20}\), it is not unreasonable for a solicitor who receives land title
instruments which have been executed and witnessed by a person qualified to
act as witness to assume that the instrument has been properly executed and
the procedure laid down for witnessing complied with. As pointed out by the
Court of Appeal in \textit{Young v Hoger}:  

\begin{quote}
\text{Young v Hoger [2000] QSC 455, 21.}
\text{Young v Hoger [2000] QSC 455, 20.}
\text{The Justice of the Peace in \textit{Young v Hoger} was deceased at the time of trial hence no evidence
was available from him as to the circumstances of the execution: \textit{Young v Hoger [2000] QSC 455,
22}.}
\text{Young v Hoger [2000] QSC 455, 23.}
\text{In Queensland, for example, s162 of the \textit{Land Title Act 1994} (Qld) states that a person who
witnesses an instrument executed by an individual must:
(a) first take reasonable steps to ensure that the individual is the person entitled to sign the
instrument; and
(b) have the individual execute the document in the presence of the person; and
(c) not be a party to the instrument.}
\end{quote}
there is no evidence that it was considered to be prudent or even a common practice among solicitors to verify the authenticity of the signature of a party to a document, or specifically of the signature of a party to an instrument under the Land Titles Act, by speaking to the Justice of the Peace or other person who appears to have witnessed that signature.\(^\text{21}\)

Whilst it is unclear as to the manner in which execution was witnessed in *Young v Hoger*, it is clearly demonstrated in *Sansom v Westpac Banking Corporation*\(^\text{22}\) the importance of complying with attestation procedures as a preventative measure against fraud by forgery of the victim’s signature. In that case Mr and Mrs Sansom were the registered proprietors of their home in Port Macquarie as well as joint holders of an overdraft account with Westpac Banking Corporation. Mrs Sansom looked after their financial affairs and she signed most of the cheques drawn on their joint account\(^\text{23}\). She had also told the bank’s officers that Mr Sansom was ill with cancer. On May 1985, the Port Macquarie home was mortgaged to the bank to secure an increase in the overdraft limit. Mr Sansom knew nothing about the mortgage. Mr Tongue, a senior officer of the bank gave Mrs Sansom the mortgage documents for the purpose of procuring Mr Sansom’s signature. She forged Mr Sansom’s signature on the mortgage and returned the document to the bank. Mr Tongue attested to Mr Sansom’s signature to the mortgage document, falsely attesting that it signed in his presence. Later in 1987, the bank took mortgages over two more properties. Similar to the 1985 mortgage, Mr Monaghan, the bank’s manager, allowed Mrs Sansom to take the mortgage documents home for Mr Sansom to sign. Again she forged Mr Sansom’s signature on the mortgage documents and Mr Monaghan falsely attested that Mr Sansom had signed the mortgage documents in his presence. The 1987 mortgages were also registered. The bank did not get in contact with the husband before the mortgages were signed or did the bank attempt to verify the truth as to Mr Sansom’s illness\(^\text{24}\). Here the main factor that allowed the fraud to occur was the breach of the bank’s attestation procedure that execution of signatures should be witnessed in the presence of the bank officer. If the bank officers had insisted on Mr Sansom signing in their presence, the fraud would not have occurred. Handing over to Mrs Sansom the mortgages documents for the purposes of procuring Mr Sansom’s signature simply made it easier for Mrs Sansom to perpetrate the fraud. Finally, the bank had no contact with Mr Sansom. Perhaps if they had contacted him to verify the mortgage transactions, the fraud might have been uncovered. However as Rolfe J pointed out, the bank officers were told by Mrs

\(^{21}\) *Young v Hoger* [2001] QSC 453, [26].
\(^{22}\) *Sansom v Westpac Banking Corporation* (1996) Aust Torts Reports 81-383. Also see *Russo v Bendigo Bank Ltd* [1999] 3 VR 376 where the clerk employed by solicitor acting for mortgagee was given specific instructions by the solicitor not to attest unless in that person’s presence. However the clerk had attested to the signature although the registered proprietor was not present when the document was signed, thereby enabling the son-in-law to perpetrate the fraud by forging her signature on the mortgage. Note that in this case the court held that fraud on the part of the clerk was not established because the clerk was not aware of the legal significance of attestation clauses in the registration process. Ormiston J held that the clerk was not shown to be dishonest and that the claimant had failed to establish the requisite dishonesty or moral turpitude necessary to establish fraud within the Torrens system. The case is used here as an example of how dispensing with proper attestation procedure facilitated the fraud.

\(^{24}\) *Westpac Banking Corporation v Sansom & Anor* (Unreported, Supreme Court of New South Wales, 22 November 1994), 36.
Sansom that Mr Sansom was terminally ill with cancer and “if a wife says her husband is suffering from terminal cancer, in the absence of suspicious circumstances, there would be no reason to query the assertion”\(^25\).

These two cases demonstrate that these types of fraud are usually opportunistic in that the fraudulent party is known to the victim and trusted by the victim. They include persons such as the victim’s family members and friends. The ability of these types of perpetrators to commit the fraud is aided by the ease in which the fraudulent person can gain access to title documents and other identity documents such as rates notices and household bills as a means of establishing a right to deal with the land\(^26\). Furthermore, in these situations, the fraudulent person is usually seen as speaking for or on behalf of the victim and all correspondence and land title documents are given to the fraudulent party to procure execution by the victim. This not only provides the fraudulent party with access to forging the victim’s signature but also allows the fraudulent party to hide from the victim and from the other party to the transaction the fraudulent scheme in which the fraudulent party is engaged in. As seen in the above cases, had the solicitor for the mortgagee contacted the victim to ensure that the victim knew and was aware of the transaction\(^27\), the solicitor might have discovered the fraud.

The importance of verifying instructions before acting on them and ensuring that each signatory to the transaction is aware of the true nature of the transaction is also illustrated in the case of \textit{Igarashi v APC International Pty Ltd}\(^28\). In that case, the registered proprietors’ solicitors handed over the certificate of title to another firm of solicitors based on a written authority from the registered proprietors which had been forged by the fraudulent party. The fraudulent party then delivered to this firm of solicitors a bill of mortgage containing the forged signatures of the registered proprietors. The certificate of title and the bill of mortgage were handed over to the mortgagees and the mortgage registered.

Finally, where there are witnessing requirements, the fraudulent party may circumvent this by forging the signature of the witness. The forged signature of the witness could either be of a real person\(^29\) or of a fictitious person\(^30\). There have also been cases where the witness has attested to a signature even

\(^{25}\) \textit{Westpac Banking Corporation v Sansom & Anor} (Unreported, Supreme Court of New South Wales, 22 November 1994), 36.

\(^{26}\) For example in \textit{Young v Hoger} [2001] QSC 453, the solicitor acting for the mortgagee made a request to Denise for certified documentation to verify the identity of the Hogers and received copies of the Hogers passports as well as copies of Mr Hoger’s Commonwealth Bank Visa Card, Medicare card and electricity account of the Hogers, although contrary to the solicitor’s instructions, they were uncertified copies.

\(^{27}\) See also Editorial comment, ‘The relevance of indefeasibility of Torrens title land for conveyancing’ (1991) \textit{ANZ ConvR} 496, 505 noting the importance of solicitors when acting for parties acquiring interests in Torrens title land, particularly as purchasers or as mortgagees to ensure that their clients, amongst other things, “that each of the registered proprietors are aware of the transaction, having been represented by solicitors in the transaction”.

\(^{28}\) \textit{Igarashi v APC International Pty Ltd} [1996] 1 Qd R 267.

\(^{29}\) The case of \textit{Vassos & Anor v State Bank of South Australia & Anor} [1993] 2 VR 316 is an example where the signature of the witness was forged.

\(^{30}\) An example where the signature of a fictitious witness was forged is a claim that was made against the state of Queensland in 2004. In that claim, the son had fraudulently executed a mortgage over his parent’s property. He also forged the signature of the witnessing solicitor, which in this case was of a fictitious person.
though the signature was not signed in the presence of the attesting witness, thereby facilitating the fraud.

4.2 Fraud by misleading the victim into signing relevant documentation

An example of this Dannyell v Paradiso\(^{31}\). In that case, two brothers, David and Hugo Paradiso, were the registered proprietors of two adjoining properties in Adelaide. David Paradiso met the fraudulent person, Ivan Zoneff, at the home of his relative. At that meeting, Zoneff told David Paradiso that he (Zoneff) would help him recover certain moneys that David had loaned to a man called Rand. Zoneff also proposed to purchase the two properties owned by the brothers and continued to give hopeful reports of recovering the moneys loaned. Zoneff also persuaded David Paradiso to entrust the certificates of title to Zoneff for safekeeping. Later on, Zoneff persuaded Mr Paradiso to sign certain sheets of paper on the basis that it would be required in the matter regarding recovery of the money loaned to Rand. David Paradiso signed these sheets of paper without reading them. It turned out that the sheets of paper were in fact the printed form of page 7 of a standard form of mortgage used by landbrokers in South Australia. Zoneff then removed page 7 from each of the mortgage documents prepared by the plaintiff’s broker, inserted the sheets signed by David Paradiso and forged the signature of Hugo Paradiso. He then returned the documents and the certificate of title to the plaintiff’s broker and the plaintiffs advanced the agreed sum of money via a cheque that was endorsed on the back as “payable to the said Ivan Zoneff”. Here the fraudulent party managed to commit the fraud because of the trust that was placed by the victim of the fraud upon the fraudulent party. The fraudulent party’s possession of the certificate of title also facilitated the perpetration of the fraud.

4.3 Fraud by solicitors

The cases involving fraud by solicitors usually involve the solicitors forging the signature of the victim(s), usually on the instrument of mortgage and arranging for a loan without the knowledge or authority of the victim(s). For example, in Registrar of Titles v Franzon and Finance Corporation of Australia Ltd\(^{32}\), Mr & Mrs Franzon were the registered proprietor of an estate in fee simple as tenants in common in equal shares of land contained in five certificates of title. Before 15 July 1969 that land together with land owned by Mrs Franzon’s mother, was mortgaged to secure moneys owing to A.G.C (General Finance) Ltd (AGC). The solicitor for the Franzons (Mr Hopkins) applied without their authority to Finance Corporation of Australia Ltd for a loan. When this loan was approved, the solicitor forged the Franzons signatures to a mortgage over their land to secure the loan. With the money advanced by Finance Corporation, Hopkins discharged the mortgage to AGC and misappropriated the moneys received. Similarly in Gibbs v Messer\(^{33}\), Mrs Messer was the registered owner of Torrens title land in Victoria. She executed a power of attorney in favour of her husband which authorised him to sell, mortgage or otherwise dispose of the land. Mr and Mrs Messer then moved to Scotland. The power of attorney and the duplicate certificates of title were left with the solicitor, Cresswell, for safekeeping. The solicitor forged the signature of Mr Messer to an instrument of transfer that


\(^{32}\) Registrar of Titles of the State of Western Australia v Franzon & Others (1975) 132 CLR 611.

\(^{33}\) Gibbs v Messer [1891] AC 248.
transferred the land to a fictitious person ("Hugh Cameron"). The transfer was registered. The solicitor then purported to act for this fictitious person, and arranged a loan on security of the land. He executed the necessary mortgage by signing it as Hugh Cameron and himself attesting to the signature. The mortgage was registered and the solicitor absconded with the moneys.

In Queensland, as noted above, six fraud claims made against the State involved the same solicitor who had advertised in the newspaper offering high interest returns for registered first mortgages. Once registered, the solicitor continued to pay interest to the former mortgagees whilst fraudulently executing releases of the subject mortgages and subsequently re-mortgaging the properties using new investors. As the case involved discharge of a mortgage, witnessing of the signature on the discharge was not required.

Usually in cases of fraud by the solicitor, the solicitor is able to commit the fraud because the solicitor has easy access to documentation that would facilitate the fraud, such as in some cases the victim’s certificate of title. It is also submitted that the ability of the solicitor to commit fraud is facilitated by the fact that the solicitor has a unique role given the function that the solicitor performs in the conveyancing process. The trust that the client reposes in the solicitor to properly discharge his/her duties and responsibilities is another factor which may aide the solicitor’s perpetration of the fraud.

4.4 Fraud by impersonation of the victim or identity fraud

Though less common than forgery of signature, fraud by impersonation of the victim of the fraud, either using the victim’s identity documents or creating false identity documents, does occur. This type of fraud may be referred to as identity fraud. The term ‘identity fraud’ “generally involves a person falsely representing himself or herself as either another person or a fictitious person”. In terms of land title fraud, usually the identity fraud is perpetrated by a person known to the victim of the fraud who has access to the victim’s identity documents, such as a family member, trusted friend or a relative of the victim of the fraud. This

---

34 See Sharon Christensen and William Duncan, Professional Liability and Property Transactions (The Federation Press, New South Wales, 2004) for a discussion on the relationship between the solicitor and the client in the context of property transactions and the solicitor’s duties and responsibilities to the client.

35 Harry Pontell, ‘Pleased to meet you...won't you guess my name?: Internet fraud, cyber-crime, and white-collar delinquency’ (2002) 23 Adelaide Law Review 305, 306. See also Gary R Gordon and Jr Norman A Willox, ‘Identity Fraud: A critical national and global threat’ (2004) 2(1) Journal of Economic Crime Management <http://www.utica.edu/academic/institutes/ecii/publications/articles/BA2C8FE1-D0EC-26B6-50870F45EA5CC991.pdf>, 7: Identity fraud “is defined as the use of false identifiers, fraudulent documents, or a stolen identity (identity theft) in the commission of a crime...Identity fraud is broader than identity theft in that identity fraud refers to the fraudulent use of any identity, real or fictitious, while identity theft is limited to the theft of a real person’s identity”. In contrast, the term ‘identity theft’ may be defined as the “unlawful taking of another person’s details without their permission” and using that identity to commit a crime. Thus identity fraud, because it also includes creating or using a fictitious identity, covers a wider range of crimes than identity theft which is restricted to stealing a real identity. See Holly K Towe, ‘Identity theft: Myths, Methods and New Law’ (2004) 30 Rutgers Computer and Technology Law Journal 237 and Harry Pontell, ‘Pleased to meet you...won't you guess my name?: Internet fraud, cyber-crime, and white-collar delinquency’ (2002) 23 Adelaide Law Review 305, 306 noting that “Identity fraud is a far more inclusive crime category that identity theft, where one uses the identity of another to enact a criminal offence”.

234
category of fraud is opportunistic in nature\textsuperscript{36}. The fraud can be perpetrated with
the aid of a third party impersonating the victim or by the fraudulent party
himself/herself impersonating the victim. Impersonation by a party unknown to
the victim of the fraud is less common but has occurred, most recently in New
Zealand. This category of identity fraud is professional or calculated in nature as
the victim of the fraud is targeted by the fraudulent party and the fraud is usually
perpetrated using false identity documents. Below are case studies illustrating
these different categories of identity fraud.

\textbf{Family member using third party to impersonate victim}

In \textit{Grgic v ANZ Banking Group Ltd}\textsuperscript{37}, the father was the registered owner. His
son had a copy of the certificate of title and other documents relating to the
property. This was because of an earlier loan application was made to the
Commonwealth Bank which was rejected and the documents were handed
back to the son. In 1987 the son asked the father to enter into a guarantee for
the son’s new business but the father refused. The mother then colluded with a
workmate to impersonate the father. The son, his wife and the workmate went
to the ANZ Bank and the son introduced the workmate as his father. The
workmate was able to produce the certificate of title and other documents
relating to the land. Officers of the bank prepared the mortgage document and
the workmate signed (as the father). The officers witnessed the signature.
Here the fraud occurred because the bank officer accepted the introduction of
the son that the workmate was his father. He did not ask for further
identification. He also relied on the certificate of title and other documents
relating to the land as proof that the workmate was the father.

\textbf{Trusted friend impersonating victim without the aid of a third party}

An example of this type of fraud occurred in Queensland with the trusted friend
of the registered proprietor impersonating the registered proprietor using the
registered proprietor’s 18+ card. The trusted friend also had access to various
other documents such as rates notices and other household bills. The
documents were genuine documents. The fraud occurred because of
inadequate verification of identity by the lender. The trusted friend was able to
use the 18+ card to impersonate the registered proprietor even though she was
female and the registered proprietor was male.

\textbf{Impersonation by unknown party or professional fraud}

A few case studies illustrate this type of fraud. First, the New South Wales Land
and Property Information uncovered a scheme in 2002 involving forged
certificates of title. The scheme involved fraudulent persons creating counterfeit
certificates of title as well as assembling fraudulent personal identification
documents and presenting these documents to various financial institutions to

\textsuperscript{36} See also Norman Siebrasse, ‘Report on land title practices and fraud’ (Canada Mortgage and
Housing Corporation, 2003), 40, dividing fraud by impersonation into two categories:
“opportunistic fraud, perpetrated by someone who knows the victim…and professional fraud,
perpetrated by con artists who are not known to the victim.”

\textsuperscript{37} \textit{Grgic v ANZ Banking Group Ltd} (1994) 33 NSWLR 202.
secure a mortgage over the land. This case illustrates the role played by the certificate of title in facilitating the perpetration of land title fraud in the paper based land registration system.

More recently in New Zealand the Auckland District Law Society published an article in October 2005 warning practitioners about conveyancing fraud after a woman using used false passports, bank statements and tax certificates to convince three lawyers to arrange mortgages over homes she did not own. A total of $450,000 was placed in six bank accounts and she managed to withdraw the money before bank officials found out about the fraud.

These case studies on identity fraud demonstrate that identity fraud, whether by persons known or unknown to the victim of the fraud, usually occur in situations where:

- the fraudulent party is able to gain access to title documents and other identity documents, whether genuine or forged, and using these identity documents to impersonate the victim; and
- the mortgagee’s solicitor is not vigilant in verifying the identity of the person purporting to deal with the land and that the person has a right to deal with the property.

They also illustrate that in some cases, the easy availability of the paper certificate of title assists the fraudulent party in the perpetration of the fraud.

The above analysis demonstrates that the current paper system is susceptible to certain types of fraud. Given the push in Australia towards a fully computerised national conveyancing system, the question of whether the proposed electronic system will be susceptible to the types of fraud perpetrated in the paper system is a pertinent issue that needs to be addressed.
5. Identifying the features of the proposed NECS for comparative purposes

In order to determine whether the types of fraud perpetrated in the paper conveyancing system can be capable of being perpetrated in the NECS, the general features of the NECS must first be identified. This is achieved by examining two documents drawn up by the National Electronic Conveyancing Office – the draft National Business Model and the draft Operations Description. Whilst these two documents are currently in draft stage as the NECS is still in its consultative phase, it is possible to draw from the two documents certain overarching features of the NECS that can be used for the purposes of this article.

Under the current proposals, access to the NECS is restricted to industry participants who have successfully registered with the NECS. The current proposals describe three user roles:

- **Subscribers**: these are corporations, partnerships, government agencies and individuals employing or contracting industry practitioners and others meeting the minimum requirements for representing clients in using the NECS to prepare and/or certify and sign instruments;
- **Users**: these are employees or contractors authorised by a subscriber to prepare but not certify or sign instruments; and
- **Certifiers**: these are industry practitioners employed by or contracted to a subscriber and authorised by that subscriber to prepare, certify and sign instruments.

Thus any person wanting to lodge an instrument for registration (NECS terms this group of persons the ‘client’) must first choose a subscriber to represent that person in using the NECS and completing the transaction. The subscriber must verify the identity of the client. Once the client is properly identified, the subscriber completes a client authorisation form to act for the client. The form must be signed by the client in front of a witness.

---

43 The National Office was established by the State and Territory governments in August 2005 to establish and support the National Steering Committee in the development of NECS: <http://www.necs.gov.au/national-office/default.aspx> at 22 September 2006.


The next step is for a registered user of the subscriber to log on to the system\textsuperscript{49} and once logged on, to request the establishment of a workspace in which to compile the information needed for the transaction\textsuperscript{50}.

The system also allows for certain fields of information to be automatically pre-populated from the computerised freehold land register\textsuperscript{51}.

In terms of signing of documents, digital signatures\textsuperscript{52} will replace handwritten signatures, and under the current proposals, certifiers will be entrusted with the responsibility of digitally signing documents on behalf of their clients. It appears that certifiers will have to obtain a Grade 2 Gatekeeper compliant digital signature certificate (DSC) for the purposes of digitally signing instruments\textsuperscript{53}.

Once the workspace is completed and the certifier has digitally signed the instrument and made the appropriate certifications, financial settlement of the transaction takes place automatically and the instrument is electronically sent to the Land Registry for lodgement\textsuperscript{54}.

From the above description, it is possible to extract the following broad features of the NECS:

- Access to the electronic system is limited to authorised users of the system;
- Subscribers act on behalf of clients who must sign an authorisation form in front of a witness;
- Digital signatures will replace handwritten signature;
- Certifiers will be given the responsibility of digitally signing documents on behalf of their clients;

\textsuperscript{49} Each user receives a user-id and first time password during the application process to access the NECS. The user-id and password is then used to access the NECS: National Electronic Conveyancing Office, 'Draft Operations Description for a National Electronic Conveyancing System' (National Electronic Conveyancing Office, 2006), http://www.necs.gov.au/NECS-Operations-Description/default.aspx, 19.


\textsuperscript{52} For a description of the technology behind digital signatures and the steps required to digitally sign a message, 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 and YF Lim, 'Digital signature, certification authorities and the Law' (2002) 9(3) Murdoch University Electronic Journal of Law <http://www.murdoch.edu.au/elaw/indices/author/229.html> (also describes Public Key Infrastructure).


• Instruments will be prepared electronically on the NECS and lodged electronically via the NECS to the appropriate Land Registry.

The following analysis considers whether the types of fraud perpetrated in the paper conveyancing system can be capable of being perpetrated in the NECS system.

6. Impact of the NECS on paper based fraud

It is submitted that the changes that will be brought about by the NECS will impact significantly on the manner in which fraud can be perpetrated. The NECS will see more opportunities for fraud perpetrated by the solicitor. Identity fraud in the NECS can continue to be perpetrated in the same manner as in the paper system. In contrast, fraud by forgery of the victim’s signature and fraud by misleading the victim into signing documents may no longer occur in the same manner as in the paper system because in the NECS, subscribers will act on behalf of clients and individual clients will no longer sign land title instruments created on the NECS. The role of signing documents will be given to certifiers who will sign on behalf of their clients. These types of fraud may still be perpetrated in the NECS, albeit in a different manner. These findings are discussed in detail below.

6.1 Forgery of signature

As noted in [3], fraud by forgery of the victim’s signature are the most common types of fraud perpetrated in the paper system. In these cases the fraudulent party, usually a family member, would forge the signature of the victim on the land title document (such as a mortgage) and in some cases, forge the signature of the witness or the witness may attest to the signature even though it was not signed in his/her presence. In the NECS, certifiers will digitally sign instruments on behalf of their clients. Individuals will no longer sign instruments. Hence it would not be possible for fraudulent persons to perpetrate fraud by forging the signature of the victim on the land title instrument.

However, as noted above, in order to allow the certifier to sign on behalf of their clients and to act as agents for their clients, the NECS requires a client authorisation form to be completed and physically signed by the client (or the client’s appointed attorney) in front of a witness. Both the subscriber and the client must sign the authorisation form. Whilst it may not be possible for fraud to be perpetrated within the NECS by forging the signature of the victim on the actual land title document, fraud may be perpetrated in situations where the fraudulent person is given the opportunity to forge the victim’s signature on the authorisation form and forge the signature of the witness or where the person witnessing the signature does not follow proper attestation procedures. For example, using the scenario in Young v Hoger where the husband and wife jointly own property. The wife intends to mortgage the property without the husband’s knowledge. She visits a law firm who is a subscriber of the NECS. She convinces the solicitor of that law firm to allow her to take home the authorisation form for the husband to sign saying her husband is too ill to come into the law firm. She then forges her husband’s signature and brings the form back to the solicitor who then signs as witness to the husband’s signature even
though it was not signed in his presence. The solicitor then proceeds with the transaction.

In this respect, the manner of perpetration of the fraud between the paper system and the NECS is the same – forgery. The only difference between the paper system and the NECS is that in the paper system, the forgery is on the land title document, whereas in the NECS, it is on the authorisation form.

Hence the factors allowing for the fraud to occur in the paper system will apply to fraud by forgery of signature on the authorisation form in the NECS, that is:

- where the fraudulent person is provided with the authorisation form for the purposes of procuring execution by the victim. This provides the fraudulent person the opportunity to forge the victim's signature and the signature of the purported witness on the authorisation form;
- where the witness to the signature on the authorisation form purports to witness the signature even though it was not signed in his/her presence. The possibility of improper attestation is increased if there are no guidelines as to who may act as a witness.

6.2 Fraud by misleading victim into signing documents

It is submitted that the potential for fraud by misleading the victim into signing documents to occur in the NECS is eliminated because in the NECS, subscribers will act on behalf of their clients in digitally signing instruments. Hence it would not be possible to perpetrate fraud by misleading the victim into signing the necessary documentation because individuals will no longer be signing documents in the NECS. The fraudulent person would have to instead perpetrate the fraud in the manner described in [6.1] above.

6.3 Fraud by the solicitor

In the paper based system, solicitors usually commit land title fraud by forging the victim's signature. In the NECS, as noted above, solicitors who act as certifiers will have access to the digital signature certificate to digitally sign documents on behalf of their clients. Thus to perpetrate fraud in an electronic system, the solicitor acting as certifier would not even need to forge the victim's signature as is the case in the paper system. All the solicitor has to do is to prepare the documents, digitally sign it and electronically send it to the Land Titles Office for registration. Thus it could be said the NECS may provide solicitors who are certifiers with more opportunities to commit fraud. Thomas echoes this concern and whilst his comments relate to the New Zealand electronic land registration system, they are applicable to the Australian NECS55.

The supposed safety net of the system is that it cannot be operated by anyone other than solicitors, who undertake to the State not to abuse the system. There is an absence of other checks and balances in place to

---

prevent individual land titles from being transferred outright to strangers, at the whim of any fraudulent or incompetent solicitor.

6.3 Identity fraud
In the paper system, identity fraud, whether opportunistic or professional, usually occur in circumstances where the solicitor is not vigilant in verifying the identity of the person purporting to deal with the land and the fraudulent party is able to gain access to identity documents, the most prominent identity document in the paper system being the paper certificate of title. In the NECS, similar to the paper system, identity fraud will continue to occur if the subscriber is not vigilant in verifying the identity presented and simply accepts that the person they are dealing with is who they say they are. In situations where the fraud is perpetrated by persons known to the victim, the ability of these persons to commit the fraud is aided by the ease in which the fraudulent person can gain access to the victim’s identity documents. Where the fraud is perpetrated by persons unknown to the victim, the fraud can still be perpetrated if the fraudulent party is able to either forge or steal the victim’s identity documents.

Thus whilst computerisation of the land registration system will introduce some changes to current conveyancing practices, the same individuals currently perpetrating frauds in the paper system will be able to continue to do so in an electronic system, albeit in a different form.

It is further submitted that the NECS enjoys characteristics different to the paper system that may give rise to different types of fraudulent practice. This relate to the use of digital signing technology to replace the traditional handwritten signature and the persons who would be entrusted with the responsibility of using the digital signatures. This is discussed below.

7. Possible new types of fraud in the NECS
One possible new type of fraud that could occur in the NECS is the unlawful use of a certifier’s digital signature certificate to digitally sign documents. As noted above, in the NECS, certifiers will be given the responsibility of digitally signing documents on behalf of clients. Hence a fraudulent person with access to the NECS and access to the certifier’s digital signature certificate and password to activate the digital signature certificate would be able to commit fraud as the fraudulent person would be able to access the NECS, prepare the necessary documentation, digitally sign the document and lodge it for registration. For example, a law clerk working for a law firm could commit fraud if the clerk has access to the NECS (for example, if the clerk is a user of the NECS) and access to the digital signature certificate and associated password of a certifier working in the same law firm. The clerk would simply access the system, prepare the documents, digitally sign them and then electronically send them to the Land Titles Office for lodgement. In fact it could be said that unlawfully using the certifier’s digital signature certificate to digitally sign documents is analogous to forging of the certifier’s signature. The difference is that in the paper system, given a sample handwritten signature, anyone can make an attempt at forging that signature and handwriting analysis may be used to help detect the forgery. In contrast, in the digital environment, a person will not be
able to use someone else's digital signature certificate to digitally sign a document unless that person has access to (1) the digital signature certificate and (2) the password used to activate the digital signature certificate for digital signing. However, once the fraudulent party gains access to both the digital signature certificate and associated password, he/she would be able to use the digital signature certificate to digitally sign documents and it would not be possible to detect that the person using the digital signature certificate is someone other than the legitimate owner of the digital signature certificate. Unlike the traditional handwritten signature, there is nothing biometrically linking the digital signature certificate to its legitimate owner.

In the NECS, the most direct methods in which the fraudulent person can gain access to the digital signature certificate and associated password include:

- where the certifier is careless in safeguarding his/her digital signature certificate and associated password; and
- where the certifier shares his/her digital signature certificate and associated password with others.

Each of these can potentially be exploited by a fraudulent party to commit fraud.

Thus not only can the types of fraud currently being perpetrated in the paper system continue to occur in the NECS, albeit in a different manner, adoption of the NECS could also potentially introduce a new type of fraud, namely fraudulent use of a certifier's digital signature certificate to perpetrate fraud.

Given the importance of security and integrity of title under the Torrens system which can be undermined by fraud, it is critical that any move towards an electronic land registration system should also involve an examination of possible measures which can be adopted to minimise the occurrence of the types of fraud identified above.

8. Measures that may be adopted to prevent NECS based frauds

The following discussion considers possible fraud preventative measures and their effectiveness in preventing the types of fraud discussed above that may occur in the NECS. Some of these measures would be equally applicable in the current paper land registration system.

---

56 The author acknowledges that there may be other more sophisticated and/or technological methods whereby a fraudulent person can gain access to a certifier's digital signature certificate. However for the purposes of this article, the discussion is limited to the two methods listed as they are the most direct method of gaining access.

57 For a summary of the types of fraud that may occur in the NECS, see Table B in the Appendix.

8.1 Forgery of signature on the authorisation form

As can be seen from the analysis in [6.1] fraud by forgery of signature on the authorisation form may occur in situations where:

- the fraudulent person is provided with the authorisation form for the purpose of procuring execution by the victim. This provides the fraudulent person the opportunity to forge the victim's signature and the signature of the purported witness on the authorisation form;
- the witness to the signature on the authorisation form purports to witness the signature even though it was not signed in his/her presence.

In this type of fraud, it will be primarily the responsibility of the subscriber obtaining client authorisation to ensure that proper client authorisation has been obtained. It may be possible for subscribers to adopt best practice guidelines dealing with:

- Obtaining client authorisation in non face-to-face transactions;
- Attestation procedures

However the effectiveness of these guidelines in preventing fraud will again be dependent on the subscriber.

8.2 Fraud by the solicitor

In situations where the solicitor is an employee of a law firm who is a subscriber of the NECS, two measures that may be adopted by the subscriber to prevent fraud are to implement rigorous pre-employment screening techniques as well as to engage in regular monitoring of personnel\textsuperscript{59}. The first measure may assist in weeding out potential employees who may engage in fraudulent conduct. The second may assist in detecting fraudulent activity. The effectiveness of these measures will be dependent upon the vigilance of the subscriber in its implementation of its pre-employment screening techniques and monitoring of employees’ behaviour.

Obviously these measures will not be useful in situations where the solicitor is a sole practitioner. Perhaps one way of preventing this type of fraud is for the NECS to implement a type of security mechanism that can act as a check on the solicitor so that the solicitor would not be able to proceed with a transaction under the NECS unless he/she satisfies that security check. For example, requiring all potential clients to obtain a client ID from the NECS and requiring the solicitor to input the client ID before the solicitor can begin a transaction under NECS\textsuperscript{60}. The drawback with such a measure is that it may be very costly to implement and time consuming. Further it may not prevent fraud in situations where the fraudulent solicitor is able to impersonate a client and obtain a client ID from the NECS.

It may also be possible to utilise technology to detect the fraud. For example, the NECS could run regular audit trails to pick up unusual activities, such as,


\textsuperscript{60} 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) <http://www.adls.org.nz/profession/lawnews/2006/issueno02/ln0201.asp> at 26 September 2006.
single property transactions with a high turn around period or transactions where solicitors apply for loans on behalf of their clients. Since access to the NECS is restricted to authorised users who must use a user id and password to use the NECS and since certifiers must use a digital signature certificate to digitally sign instruments before they can be lodged, it should be possible to trace the fraudulent activity that is detected by the audit trails back to the fraudulent person. This way, future fraudulent activity may be prevented. The effectiveness of such a measure in detecting fraud will be dependent on the technological capabilities of the NECS and the audit practices of the organisation charged with detecting anomalies in the audit trails.

8.3 Identity fraud

As can be seen from the analysis of cases and statistics, lack of proper verification of identity of the party purporting to deal with the land is a contributing factor to the occurrence of identity fraud. Hence one measure that may be adopted to prevent identity fraud is a requirement that identity of the party purporting to deal with the land must be verified before the transaction can proceed.

Such a measure was adopted in Queensland in the recent amendments to the *Land Title Act 1994* (Qld)\(^6\). Under s11A of the *Land Title Act 1994* (Qld) the mortgagee will have to take reasonable steps to ensure that they are dealing with the true owner of the land. Similar obligations are placed on a transferee of a registered mortgage (s11B). Indefeasibility will not be available unless the mortgagee has taken “reasonable steps” to identify the person(s) who sign the mortgage.

Under the current proposals for the NECS, similar to Queensland, the requirement for verification of identity will be imposed. The difference is that in Queensland, the requirement is imposed on mortgagees. In the NECS, the requirement is imposed on the subscriber\(^6\). The Draft Operations Description describe the verification of identity procedure as generally involving\(^6\):

- Sighting of the originals of certain prescribed identity documents;
- Checking the information presented on those documents with the relevant issuing authorities;
- Completing a prescribed record of the documents sighted and information checked;
- Having the record signed by the client and the subscriber.

The precise nature of the types of documents to be used in this process is yet to be identified as the NECS is in consultative phase and the push is for uniform

---

\(^6\) See the amendments made to the *Land Title Act 1994* (Qld) by the *Natural Resources and Other Legislation Amendment Act 2005* (Qld). These amendments came into operation on 6 February 2006.\n

requirements and procedures for verification of client identities in all jurisdictions.  

What is the effectiveness of verification of identity in preventing fraud?

First, the effectiveness of this measure will largely be dependent on the subscriber responsible for verifying identity.

Secondly, verification of identity may not prevent fraud from occurring in situations where the fraudulent person is able to forge or illegally obtain identity documents. This is particularly so in cases of professional fraud. In the case of opportunistic fraud, the wrongdoers are often unsophisticated so that asking for identity documents will more likely prevent fraud than in the case of professional fraud. In professional fraud, the fraudulent person would usually have in his/her possession suitable identification, so that sighting identity documents may not be sufficient to prevent the fraud.

As Smith points out, discussing the 100 point score system as required to be taken by cash dealers for the verification of identity of account signatories under the Financial Transaction Reports Act 1988 (Cth) and the Financial Transactions Reports Regulations 1990 (Cth):

"Reliance on the 100 point system does not, however, provide a complete solution to the problem of identity-related fraud as it is possible to submit documents which have been forged or altered. Although the 100 points system itself provides a reasonable means of establishing identity, in practice it is easy to circumvent, largely through the inability of staff whose staff it is to verify documents to be able to do so quickly and accurately."

---


65 For example, between August 1995 and March 1996 an offender used desktop publishing equipment to create 41 birth certificates and 41 student identification cards, each in separate names, and a counterfeit driver's licence. They were used to open 42 separate bank accounts in Melbourne to pay cheques into accounts as wages and to make immediate withdrawals before they can be cleared, to register a business name, to obtain sales tax refunds and to defraud various retailers: see R v Zehir (1998) 104 A Crim R 109.

66 According to the Victorian Report on the Victorian Fraud Experience (personal communication by the Victorian Land Registry to the author in 28 September 2005), the reason why fraud claims reduced from six a year in the early and mid 1990s to about two a year in the late 1990s was the increased vigilance by banks and the legal profession in verification of identity procedures.

67 See Norman Siebrasse, 'Report on land title practices and fraud' (Canada Mortgage and Housing Corporation, 2003), , 40.

In such a situation, the root of the problem must be attacked – what makes it possible for fraudulent persons to obtain identity documents and commit identity fraud?

The ability of criminals to obtain identity documents and commit identity fraud has been linked to the complexities involved in the proof of identification process. In Australia, at present, a variety of documents, such as drivers’ licence, passports, rates and energy utility bills are accepted as proof of identity documents. These documents are issued by different organisations. Furthermore, in issuing a document that will be used as a proof of identity document, these organizations are themselves relying on proof of identification documentation issued by some other organization. Thus one proof of identity document can be used to obtain other proof of identity documents that reinforce and validate the identity in question. The identity fraud perpetrator can attack the proof of identity issuer with the weaker identity fraud controls, and use these legitimately obtained documents as proof of identity for the proof of identity issuers with the stronger controls. In this way the individual can secure appropriate identity documentation such as a driver’s licence, passport, or birth certificate which can then be used to provide the individual with access to other elements of a credible identity, such as a bank account. As these accumulate, the individual builds a more credible identity as they collect more fraudulent documents.

Improvements in technology such as imaging equipments, colour printers, the increase use of the Internet for online transactions have also resulted in greater ease of forgery and perpetration of identity fraud.

Suggested measures to combat identity fraud include:

- Improving the proof of identification system. A risk evaluation of the various documents currently being used as proof of identity could be undertaken and evaluated.

- Shifting attention from the identity document itself to the person using the identity document and towards the process of identity checking. Education on fraud awareness and prevention should be provided to personnel involved in the process of verification of identity so that they are trained in recognising false or altered documents.

---


• Support and incentives should be provided for issuers to improve on document processing and information system integrity\textsuperscript{75}. This could include counterfeiting prevention techniques. For example, plastic cards are now protected by security printing, micro-printing, holograms, embossed characters, temper evident signature panels, magnetic strips with improved card validation technologies and indent printing\textsuperscript{76}.

8.1 Unauthorised use of a certifier’s digital signature certificate

As noted in [7] above, a fraudulent person who has access to the NECS and manages to gain access to both the digital signature certificate and password to activate the digital signature certificate will be able to perpetrate fraud. Two issues need to be considered here – first safekeeping of the digital signature certificate so as to prevent fraudulent parties from gaining access to the digital signature certificate and secondly, generating a strong enough password so that even if the fraudulent person manages to gain access to the digital signature certificate, he/she would not be able to use it because he/she lacks the password necessary to activate the digital signature certificate.

In terms of storage mechanisms for the digital signature certificate, several options are available. The simplest and most convenient option may be to store the digital signature certificate on the solicitor’s hard drive\textsuperscript{77}. Other options include storing the digital signature certificate on a Universal Serial Bus (USB) device or a smart card\textsuperscript{78}. Unlike storing the digital signature certificate on the hard drive of a computer, storing the digital signature certificate on a USB drive or a smart card allows the solicitor to remove the digital signature certificate when it is not in use. The USB drive or smart card may also be stored in a secure storage, such as an office safe. However the solicitor may lose or misplace a USB drive or smart card easier than a desktop computer. Furthermore, a fraudulent person may have greater mobility with a digital signature certificate stored on a USB drive or smart card that it could be used from other terminals.

In any event, as the possibility exists that a fraudulent party may gain access to the digital signature certificate, regardless of the storage mechanisms used, whether through theft or through the solicitor’s carelessness, the password used to activate the digital signature certificate is of crucial importance. In this regard,

\textsuperscript{75} Suresh Cugnasen and David Lacey, Identity fraud in Australia: An evaluation of its nature, cost and extent (Standards Australia Ltd, Sydney, 2003), 115. See also Russell Smith, ‘Examining the legislative and regulatory controls on identity fraud in Australia’ (Paper presented at the Marcus Evans Conferences, Corporate Fraud Strategy: Assessing the Emergence of Identity Fraud, Sydney, Australia, 2002).

\textsuperscript{76} Russell Smith, ‘Best Practice in Fraud Prevention’ (Australian Institute of Criminology, 1998), http://www.aic.gov.au/publications/tandi/tandi100.html. Smith notes that the effectiveness of such security features is dependant on the person validating the identity to be familiar with all these features. There is also the possibility of sales staff being subject to intimidation or violence if they refuse to process the transaction: 5.

\textsuperscript{77} In New Zealand for example, the digital certificate is stored on the user’s C Drive.

\textsuperscript{78} The draft NECS Operations Description specify that the means of storage of the digital signature certificate is a matter for the subscriber to decide, however, the recommended storage in on a removable device such as a smart card or a USB: National Electronic Conveyancing Office, ‘Draft Operations Description for a National Electronic Conveyancing System’ (National Electronic Conveyancing Office, 2006), http://www.necs.gov.au/NECS-Operations-Description/default.aspx.
the password chosen should be a strong, that is, a hard-to-guess password, not something that is easy for the fraudulent party to guess or crack\textsuperscript{79}.

Educating certifiers on the importance of:

- secure storage of the digital signature certificate;
- using strong passwords; and
- not sharing digital signature certificates with other users

may also assist in preventing this type of fraud. However it would still be the responsibility of the certifier to adopt secure storage practices and usage of strong passwords.

Imposing duties and obligations on the solicitors to safeguard the digital signature certificate may be another method in ensuring the security of the digital signature certificate. For example, in the electronic system in New Zealand, in accordance with Rule 3.04 of the Rules of Professional Conduct for Barristers and Solicitors\textsuperscript{80}, a lawyer must ensure that the password for his/her digital certificate is not disclosed to anyone. The password must not be written down and must not be shared with anyone, including partners in the firm. The lawyer is also personally responsible for all instruments that are registered that have that lawyer’s digital certificate. Furthermore, under the Landonline Digital Certificate User Obligations, the subscriber must protect his/her private key from any compromise and take all necessary precaution to prevent the loss of the key pair, modification, disclosure or unauthorised use of the private key. The subscriber must inform Land Information New Zealand (LINZ) immediately if he/she suspects or knows of the loss, disclosure or other compromise of his/her digital certificate\textsuperscript{81}. 

\textsuperscript{79} For example, mixing upper case and lower case, using numbers or other characters not usually found in dictionary and making sure the password is at least eight characters long: Land Information New Zealand, \textit{Landonline security} \textless http://www.landonline.govt.nz/content/general/security.asp\textgreater at 17 January 2006.

\textsuperscript{80} Rule 3.04: A practitioner must not allow use of his or her Digital Certificate (DC) or the associate password by any other person: Commentary: (1) A Digital Certificate (DC) with certifying and signing privileges issued to a practitioner for the purpose of eDealing in Landonline is the electronic equivalent of a practitioner’s personal signature. Use of the DC for certifying and signing allows direct transfer or property rights. Every practitioner accepts full responsibility for the consequences of the use of his or her Digital Certificates. (2) The DC must be used only by the practitioner personally. The Rules are available from New Zealand Law Society, \textit{Rules of Professional Conduct for Barristers and Solicitors} (2004) \textless http://www.lawyers.org.nz/about/profcon.htm\textgreater at 19 January 2006. In New Zealand, the digital certificate is used to electronically sign documents. See: Land Information New Zealand, \textit{Landonline security} \textless http://www.landonline.govt.nz/content/general/security.asp\textgreater at 17 January 2006.

Similar obligations are imposed by the Law Society in Ontario, Canada whereby sharing of the encrypted diskette and pass phrase is unprofessional conduct and illegal under the Rules of Professional Conduct.\(^{82}\)

Of course the fact that these duties and obligations are imposed on the solicitor does not ensure that (1) they will be followed or (2) that fraud will not occur. The solicitor may not have followed the guidelines imposed thereby allowing fraud to occur and the solicitor may be liable for being negligent or careless. However, the fact remains that fraud has occurred. Further, even if the solicitor does follow guidelines and acts to safeguard the digital signature certificate, there may be instances, through no fault of the solicitor, that the fraudulent person does gain access to the digital signature certificate and uses it to perpetrate fraud.

The above analysis demonstrates that although a number of measures can be adopted to minimise the occurrence of fraud in the NECS, the implementation of each measure is not necessarily a complete guarantee against fraud.\(^{83}\) For example, verification of identity will not prevent fraud in cases where the fraudulent party is able to produce high quality forged identity documents. More importantly, the success of each measure in fraud prevention is dependant on the vigilance of the users of the system. For example, verification of identity as a fraud preventative measure is dependant on the extent to which the person carries out the task of verification of identity. Thus complete prevention of fraud, whether in a paper or electronic system, would be very difficult to achieve.

9. Conclusion

The move to an electronic land registration system in Australia will bring significant changes to current conveyancing practices. As can be seen from the analysis above, the types of fraud currently occurring in the paper system can continue to occur in the proposed NECS, albeit perhaps in different forms. The NECS may also see a new type of fraud—fraudulent use of a certifier’s digital signature certificate. Whilst certain measures may be adopted to prevent fraud from occurring, such as requiring the verification of identity before proceeding with the transaction, the implementation of these measures in itself is not a

---

\(^{82}\) See Subrule 5.01(7) and Subrule 5.01(8). Subrule 5.01(7): “When a lawyer has a personalized specially encrypted diskette to access the system for the electronic registration of title documents (“e-reg”), the lawyer (a) shall not permit others, including a non-lawyer employee to use the lawyer’s diskette, and (b) shall not disclose his or her personalized e-reg pass phrase to others. Subrule 5.01(8) imposes obligations on a lawyer regarding the use of the Personal Security Licence (PSP) by the lawyer’s non-lawyer employees. It provides that when a lawyer has a non-lawyer employee who has a diskette to access the system, the lawyer shall ensure that the non-lawyer employee does not permit others to use the diskette and does not disclose his/her pass phrase to others. Subrules 5.01(7) and 5.01(8) are available from the The Law Society of Upper Canada, *Rules of Professional Conduct* (2005) <http://www.lsuc.on.ca/regulation/a/profconduct/> at 22 January 2006.

In Canada, each user of the Ontario electronic land registration system must have a unique electronic security identity called a Personal Security Package (PSP), consisting of a personal security disk (floppy diskette with encrypted information) and a pass phrase to access the system. The personal security disk is used to electronically sign documents. For more information about the system see R 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.

\(^{83}\) For a summary of possible measures that may be adopted to prevent the types of fraud that may occur in the NECS, see Table C in the Appendix.
guarantee against fraud. It is the users of the system, exercising caution and vigilance that may prove to be the strongest preventative measure against fraud.
## Appendix

### Table A: Paper based frauds

<table>
<thead>
<tr>
<th>Type of fraud (paper system)</th>
<th>Manner of perpetration</th>
<th>Factors enabling the fraud to occur</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forgery of signature</td>
<td>Forgery of victim’s signature, usually on a mortgage</td>
<td>Easy access to the paper certificate of title and various other identity documents.</td>
</tr>
<tr>
<td>Usually opportunistic - perpetrated by persons close to the victim, such as the victim’s family members.</td>
<td>May also forge signature of the witness to circumvent attestation requirements. In some cases, the witness attests to the signature even though it was not signed in their presence.</td>
<td>The witness to the signature(s) on the instrument attests to the signature(s) even though the signature was not signed in front of the witness. Documentation provided to the fraudulent party to procure execution.</td>
</tr>
<tr>
<td>Misleading victim into signing documents</td>
<td>Usually perpetrated by misleading or inducing the victim into signing documents used to perpetrate the fraud.</td>
<td>Victim not contacted to verify instructions.</td>
</tr>
<tr>
<td>Usually opportunistic - perpetrated by persons whom the victim trusts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fraud by the solicitor</td>
<td>Most common type of fraud is forgery of the signature of the victim, usually on a discharge of mortgage. In these cases, attestation of the signature is not required.</td>
<td>Easy access to relevant documentation required to perpetrate the fraud such as in some cases the paper certificate of title. Solicitor’s unique role in the conveyancing process and trust placed upon the solicitor by his/her client.</td>
</tr>
<tr>
<td>Usually opportunistic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity fraud</td>
<td>Impersonation can be perpetrated with or without the aid of a third party, using the victim’s identity documents.</td>
<td>Access to the victim’s identity documents, including the certificate of title. Lack of vigilance in verifying the identity of the person purporting to deal with the land.</td>
</tr>
<tr>
<td>(1) By family members/trusted friends (opportunistic)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(2) Unknown party (professional)</td>
<td>Victim of the fraud is targeted. Impersonation using false identity documents</td>
<td>Ability to either forge identity documents, including the certificate of title, to perpetrate the fraud. Lack of vigilance in verifying the identity of the person purporting to deal with the land.</td>
</tr>
</tbody>
</table>

### Table B: Types of fraud that may occur in the NECS

<table>
<thead>
<tr>
<th>Type of fraud (NECS)</th>
<th>Manner of perpetration</th>
<th>Factors enabling the fraud to occur</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud by the solicitor who is a certifier under the NECS</td>
<td>Electronically preparing the instrument, digitally signing it and electronically lodging it to the Land Titles Office for registration. Unlike paper system, forgery of victim’s signature not required for the fraud.</td>
<td>Solicitors have access to the NECS and access to the digital signature certificate. Solicitor’s role in the conveyancing process.</td>
</tr>
<tr>
<td>Forgery of signature on the land title instrument</td>
<td>May still be perpetrated by the forgery of the signature is on the authorisation form, not on the land title instrument.</td>
<td>The fraudulent person is provided with the authorisation form for the purpose of procuring execution by the victim. This provides the fraudulent person the opportunity to forge the victim’s signature</td>
</tr>
</tbody>
</table>
Identity fraud

Whether by persons known or unknown to the victim, fraudulent person uses identity documents to impersonate the victim. Paper certificate of title no longer issued but other identity documents may be used in the perpetration of the fraud.

The witness to the signature on the authorisation form purports to witness the signature even though it was not signed in his/her presence.

Lack of vigilance in verifying the identity of the person purporting to deal with the land.

Ability to obtain identity documents, whether forged or stolen documents.

Unauthorised use of the certifier’s digital signature certificate

Using the certifier’s digital signature certificate to access the system, prepare and then digitally signing the documents.

Will also require the appropriate password to access the digital signature certificate

(1) certifier is careless in safeguarding his/her digital signature certificate & password used to activate the digital signature certificate

(2) certifier shares his/her digital signature certificate and password with others.

Table C: Possible fraud preventative measures for NECS based frauds

<table>
<thead>
<tr>
<th>Type of fraud NECS</th>
<th>Possible preventative measures</th>
<th>Effectiveness of preventative measures</th>
</tr>
</thead>
</table>
| Fraud by the solicitor who is a certifier under the NECS | (1) Where the solicitor is employed by a subscriber: implementation of pre-employment screening techniques and regular monitoring of personnel;  
(2) Where the solicitor is a sole practitioner:  
(a) Implementing a mechanism that can act as a check on the solicitor (such as requiring client IDs to be inputted before the transaction can proceed)  
(b) Using the NECS to run regular audit trails to detect unusual activity | (1) Dependant on the subscriber.  
(2) Both measures are dependent on NECS technological capabilities.  
Measure (a) may be too costly and time consuming to implement.  
Effectiveness of measure (b) also dependent on the audit practices of the organisation charged with detecting anomalies in the audit trails. |
| Forgery of signature | (1) Subscriber will have to ensure that appropriate authorisation is obtained from all clients  
(2) Imposing best practice guidelines for non face-to-face transactions and attestation procedures | Effectiveness of both measures are dependant on the subscriber. |
| Identity fraud | (1) Verification of identity of the person purporting to deal with the land before proceeding with the transaction.  
(2) Provide education and training to those responsible for verification of identity | (1) Effectiveness dependent on the subscriber responsible for verifying identity. May not be effective in situations where fraudulent person has access to forged identity documents of high quality.  
Measure (2) may assist in training personnel involved in the process of verification of identity to recognise forged |
| Unauthorised use of the certifier's digital signature certificate | (1) Certifier to use secure storage mechanisms for storing the digital signature certificate  
(2) Certifier to use strong passwords  
(3) Certifier to not share his/her digital signature certificate and passwords with others  
(4) Educating the certifier in (1) – (3)  
(5) Imposing guidelines for (1) – (3) | Effectiveness of all measures dependent on the certifier. |