

**The PenOp Signature: An
Australian Legal
Perspective**

Mallesons Stephen Jaques
Solicitors

Level 10
Central Park
152 St George's Terrace
Perth WA 6000
Telephone (61 8) 9269 7000
Fax (61 8) 9269 7999
DX 91049 Perth
Ref: GAF:BD:09 5016 9656

The PenOp signature - legal issues in Australia

| Contents | PAGE |
|---|-------------|
| Executive Summary | 2 |
| Introduction | 3 |
| Signatures - Basic Characteristics | 4 |
| Digital Signatures - General | 6 |
| Digital Signatures - Australian Legislation | 8 |
| Specific Aspects of the PenOp Signature | 12 |
| The PenOp Signature: Evidence | 15 |
| Conclusion | 19 |

1 **Executive Summary**

- 1.1 Legislative changes are currently being contemplated which will (if enacted) affect the law in Australia in relation to electronic transactions. There are currently Bills before the Commonwealth Parliament, and at least the Victorian State Parliament, dealing with “paperless” transactions and digital signatures. The effect of such legislation, if enacted on a reasonably uniform basis by all States and Territories, and the Commonwealth, will be to facilitate the use of systems such as the PenOp signature.
- 1.2 In relation to the general law concerning the use of signatures, and “paperless” transactions, Australia differs little from England. A signature is still a widely used and readily accepted method of signifying an intention to be bound by an agreement.
- 1.3 Unless there are specific requirements for a document to be in “writing” (in the traditional paper based sense), or for documents to be in a particular style or form, then whether or not the parties chose to make their transaction purely electronic, with a digital signature, is a matter for them. This may however have evidential consequences if a document is sought to be relied upon in Court proceedings. Whilst the various Evidence Acts in force in Australia all allow “Business Records” to be admissible notwithstanding the common law rules of hearsay, strictly proving certain electronic documents under the Acts may be time consuming and expensive. This is however the case with any purely electronic document that evidences an agreement.
- 1.4 The PenOp signature system may also be challenged as to authenticity of the signature or the integrity of the data that comprises the document to which the signature has been applied. It then becomes a matter for the relevant Court to decide on the available evidence, whether there is sufficient evidence to discharge the burden of proof required to establish the authenticity of the signature or integrity of the document.
- 1.5 Overall, on the material available to us, it appears the PenOp system has a number of features which if proven to be effective ought to enable a legally valid transaction to be entered into by using the PenOp signature. However, every intended use of the system would need to be considered in the light of specific regulatory or legislative requirements. Advice will be required as to the capacity of the PenOp signature to meet such requirements on a case by case or industry basis.
- 1.6 We note that proposed legislation will if enacted facilitate electronic commerce and the use of digital signatures such as the PenOp system.

2 Introduction

- 2.1 This paper is written to provide general overview of the legality of the PenOp signature for the purposes of Australian law.
- 2.2 In writing this paper, regard has been given to two prior opinions, namely a report by Mr Benjamin Wright "*The Legality of the PenOp Signature*" ("**the Wright Report**") in relation to the position of the PenOp signature under United States law, and the report of Dr Ian Walden "*Legal Aspects of the PenOp Signature under English Law*" ("**the Walden Report**"), which deals with the English legal position.
- 2.3 In the Wright Report, there is a detailed summary of the functioning of the PenOp system, and PenOp application. There is a more truncated description given in the Walden Report. We have relied upon the accuracy of these descriptions of the method of operation of the PenOp signature system in preparing this paper. It is not proposed to repeat the technical details in this paper; rather we shall endeavour to give an Australian legal perspective to the proposed PenOp signature. Accordingly, this paper is intended to be read in conjunction with the Wright and Walden Reports, although it is also written as a separate paper.
- 2.4 The importance of technology such as the PenOp system lies in its capacity to facilitate electronic trade and transactions by providing a degree of certainty and security to the parties involved. E-commerce is often conducted at a distance, with parties who may well be in completely different countries, who never see each other or even speak to each other.
- 2.5 Nevertheless, until recently most commercial transactions involving the creation of formal legal relations (ie a contract) have been "paper based", with the agreement being held in a physical form. Legal rules relating to the formation and enforcement of agreements have been relatively easy to modify to suit the use of technology such as photocopiers, telexes, and facsimile machines: these technologies remain essentially paper based.
- 2.6 The PenOp signature, which operates electronically yet still retains the "handwritten" signature, may provide a useful manner of allowing fully electronic or paperless transactions, while still retaining the familiar manner of signing a "document" to signify assent. This paper considers the legal implications of utilising the PenOp signature for commercial transactions, from an Australian legal perspective.

3 Signatures - Basic Characteristics

- 3.1 A signature, in its most basic form, is essentially no more than a mechanism confirming assent to a document or proposal. For the large majority of ordinary consumer transactions it is not required. Agreement is based upon no more than the payment of the price asked for a particular item or service that has been requested. However many commercial transactions require a great deal more certainty than either an oral or implied agreement is able to provide, and the best way to provide such certainty is to reduce the agreement to a written form.
- 3.2 For a signature to perform its basic task (confirming assent to a document) it is not necessary that a signature be legible or a complete name; a mark is acceptable if a person is unable to write; and the signature or mark may be applied at any place in a document provided it is clear that assent is being given to the entire document.¹
- 3.3 Traditionally a signature has been applied to paper using ink or some alternative means of marking that paper.² What is acceptable as a signature has changed to suit the means of doing business, which takes into account advances in technology. For example, a rubber stamp is effective as a signature provided it is an authorised application of that stamp.³ The Courts also have recognised documents verified by a facsimile signature.⁴ There are potentially some evidential problems created by the acceptance of a facsimile signature as verification of assent, mainly due to the fact that the placing of the signature was not witnessed (generally) by the recipient. Any such problems can be minimised by basic checks, such as the facsimile number from where it was sent, and by a telephone call to the person sending the facsimile.
- 3.4 The following is a summary of the various legal and physical characteristics of signatures:
- (a) that it is “bonded” to (or not able to be separated from) the paper or document;
 - (b) it is identifiable with a particular individual, and reproducible easily by that individual (and preferably only that individual);
 - (c) the signatory must intend to be bound by the contents of the document at the time of signing;
 - (d) it is easily recognised by third parties for what it is, and what it means (an intention to be bound);

¹ See **Morton v Copeland** (1955) 139 ER 861; **Baker v Denning** (1838) 112 ER 771; **Durrall v Evans** (1862) 158 ER 848.

² For the purposes of this report we do not intend to discuss the execution of documents under seal. We refer generally to the article by Peter Shafron “**Valid Execution of Documents**” (1990) 65 Law Society Journal 62.

³ This proposition was affirmed in Australia as early as 1884: see **R v Moore, ex parte Myers** (1884) 10 VLR 322.

⁴ See for example **Molodysky v Vema** (1989) NSW Conv R 55-446.

- (e) it can be located anywhere in the document unless there is a contrary legislative requirement;⁵
- (f) does not matter what kind of mark is made provided it evidences the intention to be bound;
- (g) a rubber stamp or other mechanical means of affixing the mark will suffice, subject however to contrary legislative requirements;
- (h) there is no requirement for a signature to be indelible. Pencil will be acceptable, and it has even been suggested that lemon juice which only appears as writing when heated will be a valid medium of signing a document.⁶

3.5 Whatever the manner of affixing a “signature” to a document, it must achieve the core function of *binding the signatory to the contents of the document* (be it stored electronically or in physical form). Further, provided there are no vitiating circumstances, it ought to do this irrespective of whether or not the signatory has actually read the entirety of the document.⁷

3.6 If these are the essential physical and legal characteristics of a traditional signature, it ought not to matter whether the signature is used for a transaction that is purely electronic (although capable of being printed in hard form if required). These characteristics and requirements are capable of being satisfied electronically.

⁵ For example, certain documents such as wills have formalities as to where they must be signed.

⁶ See **Shafron** (supra n4) at 62.

⁷ This is a reference to the rule in **L’Estrange v Graucob** [1934] 2 KB 394, to the effect that a party who chooses to sign a document may be bound by its terms, notwithstanding he has not read it.

4 Digital Signatures - General

- 4.1 In this paper, we use the expression “digital signature” interchangeably with “electronic signature”. A “digital signature” is so described because data transmitted electronically is transmitted as a stream of digital information. The object of a digital signature is not to encode or decode the text of a message. Encryption devices are available, and these can be used by parties who are concerned to ensure that the full contents of a document are kept confidential. However, for most general commercial purposes, encryption is too expensive, and requires too much computing power to be warranted.
- 4.2 A digital signature involves taking a “sample” of the message to obtain a “fingerprint”. This process is known as “hashing”. It is the hash value⁸ of the message that is encoded, and decoded as part of the digital signature verification process. If the two values match, ie the decoded hash of the digital signature matches the value sent, then it is a fair inference that the message has not been interfered with. This is because the hash value of a message will change if there is any alteration whatsoever to the data that is hashed. We will examine the mechanism that PenOp uses in more detail later.
- 4.3 The basic legal and practical issues affecting commerce involving electronic transactions (and hence digital signatures) are:
- (a) The risk of there being interference with the data. This is effectively a concern that what is received does not match what is sent. Alternatively, that data is not sent from the party from whom it purports to have been sent. A digital signature can provide a technical means to authenticate (in some circumstances) not only the text of the message, but also its author.
 - (b) Incompatibility with present laws is another issue. There is no doubt that electronic transactions, and digital signatures, are not always going to comply with statutory or other legal requirements. At least in Australia, several legislative responses are currently being proposed to deal with many of the issues of compliance with statutory requirements. In order to be legally satisfactory, electronic communications ought to be admissible as evidence in legal proceedings, satisfy statutory or other formal requirements, and comply with any obligations for record keeping.
 - (c) The applicability of established legal rules concerning the formation of contracts. Such issues relate to the legal rules that have been developed over time determining the rights and liabilities of parties in commercial relationships, such as the time and place of the entering into contracts. Certainty as to such matters is especially

⁸ The Wright and Walden Reports refer to the “hash value” as the “checksum”. These are different expressions used to describe the same thing, which is a string of data. This is itself encrypted as a “signature” for that document, which uses far less computing power than a full document encryption.

important where transactions are international, and two or more completely different legal systems may be involved.

- 4.4 Any or all of the above matters may concern traders, and others who may wish to utilise digital signature technology. Before committing to implementing a digital signature system a person or company will need to ensure that it not only performs the required task of demonstrating assent to a document, and possibly verification of the signatory, but also that its use will be acceptable under the various acts and regulations that govern business of the nature contemplated. Such checks should extend to considering the legal requirements for the formation of an enforceable contract in other jurisdictions in which business may be conducted.
- 4.5 That said, under the general law and leaving aside any specific legislative requirements, a digital signature is perfectly capable of being accepted as a signature. In many respects, its features closely resemble a traditional signature, in that:
- (a) the “fixing” of a digital signature is perfectly capable of evidencing an intention to be bound by the contents of a document;
 - (b) it can be “attached” to the document in such a way (electronically) that separation from the document is not possible;
 - (c) it is able to be “person specific”, although the hash will, of course, be different for each and every document; and
 - (d) it is capable of providing a degree of security, at least to the same level as that afforded by a physical signature.
- 4.6 In short, there is no practical reason why a digital signature such as that offered under the PenOp system is not perfectly capable of fulfilling the basic requirements of a “signature” as a matter of general law.

5 Digital Signatures - Current Australian Legislation

- 5.1 Australia has basically “tiered” system of government, with the most important “tiers” being the Commonwealth, and the various States and Territories that together comprise the Commonwealth. Upon Federation in 1901, the States conceded certain legislative functions to the Commonwealth. However, the States retain significant law-making ability. Further, there is nothing to prevent a State Government and the Commonwealth Government from making laws which cover the same ground, provided the laws are within power. Such legislation may conflict. In the event of a conflict, the Commonwealth legislation is taken to prevail. Given the relatively complex legislative framework that exists in Australia, it is not proposed in this paper to provide a detailed analysis of all the possible Acts which may inhibit the use of electronic signatures, or which may permit the use of electronic signatures.⁹
- 5.2 There are two principal ways that the proposed PenOp digital signature software may interact with existing Australian legislation. The first such way is where legislation specifically requires that a signature be provided (for example a tax return, or on a bill of sale, or a cheque). The second is a much more general requirement for certain commercial contracts to be in writing. The best known example of this, is the Statute of Frauds, first enacted in the United Kingdom in 1677 and received as law into the States of Australia.¹⁰ It has been suggested by at least one author that although there are no decided cases as to whether or not a digital signature would be sufficient for the purposes of the Statute of Frauds, it ought satisfy its requirements.¹¹ The reasoning behind this assertion is that the name of the signatory can be accessed via an electronic certificate.¹²
- 5.3 Acts may contain specific definitions of “document” or “writing”. For example, one such Commonwealth Act, the Corporations Law, has definition of “document” which specifically includes computer disks and tapes capable of reproducing images or writings, and it also defines “writing” as including any mode of representing or reproducing words in a visible form.
- 5.4 In circumstances where Acts have no specific definitions as to what is a “document”¹³ and what is, or is not, “writing”¹⁴ the various Evidence Acts and Interpretation Acts (both State

⁹ Some work is currently been undertaken in the area of identifying acts which have requirements for signatures and which may or may not be amenable to having those requirements fulfilled by way of a digital signature. See for example the analysis of legislation referred to in Sneddon **“Legislating to Facilitate Electronic Signatures and Records: Exceptions, Standards and the Impact on the Statute Book”** (1998) 21 UNSW Law Journal 334, in particular at 354 ff.

¹⁰ Imperial Act 29 Charles II Chapter 3. At the time of its enactment, the Statute of Frauds was concerned to prevent “fraudulent practices”. It was to some extent a creature of its day, as at the time it was enacted the plaintiff and the defendant were not competent witnesses.

¹¹ See McCullagh, A; Little, P; & Caelli, W: **“Electronic Signatures: Understand the Past to Develop the Future”** (1988) 21 UNSW Law Journal 452 at 459.

¹² In this regard, the PenOp system is manifestly more convenient than a traditional digital signature, in that the name of the signatory is capable of being displayed, and printed in documentary form if required.

¹³ The Evidence Acts of each the various States contain definitions of “document”. For a listing of these definitions, see **“The Laws of Australia”** (The Law Book Company) Part 16.5 para 7.

and Federal) will usually provide a definition. For example, for the purposes of Commonwealth legislation which does not specifically provide such definitions, the Interpretation Act 1901 (Cwth) provides a definition of “document” which is very much tied to a physical form, be it paper or recording. It may be wide enough to encompass data generated from a computer system, and in any event the definition is referred to as being inclusive, and not absolute.

- 5.5 It must always be a matter for an individual user to determine the application in which it is intended to apply the PenOp signature method, and verify that such an application will be legal according to whatever statutes and regulations govern the activities being undertaken. At present, given the number of statues in force in Australia, both Commonwealth and those enacted by the separate States and Territories, this can only be done on a case by case or industry by industry basis.¹⁵
- 5.6 Nevertheless, this process is likely to be simplified in the future, if proposed legislation is enacted. A Bill is currently before the Commonwealth Parliament, being the **Electronic Transactions Act 1999** (the “ETA”). The ETA is based to a substantial degree upon the United Nations Commission on International Trade (UNCITRAL) Model Law on Electronic Commerce of 1996. It is yet to be passed into law in Australia. It is expected that the various States and Territories will enact “mirror” legislation to ensure that the laws apply to the great majority of transactions in Australia.¹⁶
- 5.7 If the ETA is enacted, it would alter existing Commonwealth legislation to the following effect:
- (a) to ensure that a transaction currently valid under existing Commonwealth legislation is not invalidated only by reason of it being conducted by means of one or more electronic communications;
 - (b) to provide that any requirements under a law of the Commonwealth as to:
 - (i) giving information in writing;
 - (ii) providing a signature;
 - (iii) producing a document;
 - (iv) recording information; and

¹⁴ “Writing” is defined in various ways by each of the State and Commonwealth Interpretation Acts. There is a common thread in all the definitions, that is that “writing” involves a mode of representing words or symbols in a visible form.

¹⁵ For an example where detailed consideration has been given to the legal efficacy of a specific type of transaction in circumstances where it may be conducted electronically, see Gamertsfelder: **“Electronic Bills of Exchange: Will the Law Recognise Them?”** (1998) 21 UNSW Law Journal 566.

¹⁶ Most commercial transactions would not be subject to Federal laws of a relevant nature, and so the enactment of uniform State legislation is most important to the success of the law reform process.

(v) retaining a document;

can be met by appropriate electronic forms; and

(c) that the purported sender of an electronic communication is bound by it for the purposes of a law of the Commonwealth only if the communication was sent by the purported sender or with authority of the purported sender.

5.8 The proposed legislation has specific provisions relating to any requirement for a signature.¹⁷ The proposed legislation provides that a digital signature will satisfy any signature requirement under a law of the Commonwealth if:

(a) a method is used to identify the person and to indicate the person's approval of the information communicated; and

(b) having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated.

5.9 The notes on the Bill published by the Commonwealth Government say that the proposed legislation in relation to signatures is intended to be "technology neutral". It is intended that by drafting the legislation in this manner, further developments in relation to digital signatures can be accommodated without further legislative change.

5.10 The notes also specifically state that there is no requirement that the signature method be contained in the electronic communication itself. However, it must satisfy the other requirement, such as being capable of identifying the identity of the person applying the signature, and signifying the approval of that person to the contents of the document.

5.11 We emphasise that the ETA does not operate to validate a transaction that would otherwise be invalid. For example, if a transaction is not properly executed, or is executed without authority, then it may be invalid. The ETA does not alter this position. All the ETA does is provide that a transaction is not invalid *by reason only* of it being electronic or partly electronic.

5.12 Other than the Commonwealth, at least one State is also proposing to enact legislation will affect the proposed PenOp system. In Victoria, the *Victorian Electronic Commerce Framework Bill* is currently being considered. This Bill also makes provision for the recognition under Victorian law of electronic signatures, which is defined to mean a process applied by the person to a document in electronic form that serves to authenticate the document by that person, and contains acknowledgment that the document is being signed.

¹⁷ There are however exemptions from the general provision relating to digital signatures, to the effect that regulations may exempt specific acts from the general provisions, and also Rules of Court are exempted (although the Courts themselves can modify their rules to accept digital signatures).

Although it does not mirror the ETA, it nevertheless would serve much the same purpose (if enacted).

- 5.13 Like the proposed Commonwealth Act, there are exceptions to the uses for which electronic or digital signatures can be put, specifically in relation to wills, trusts, powers of attorney, affidavits, court processes, or negotiable instruments.¹⁸
- 5.14 Until legislation such as that discussed above is enacted by the Commonwealth and the States and Territories, users of PenOp will need to seek specific advice as to whether the use to which the system is intended to be put is likely to be affected by any Acts or Regulations. This degree of detail cannot be provided in a paper such as this: the important point to be made is that any requirements of both Commonwealth and State legislation will need to be researched and addressed before commencing to use the PenOp (or any other) system.

¹⁸ For a more detailed summary of the proposed Victorian Bill, see **Sneddon** (supra n9) at 343-345.

6 Specific Aspects of the PenOp Signature

- 6.1 The information that we have concerning the operation of the PenOp signature is derived from brochures provided by PenOp, and the descriptions found in the Wright and Walden Reports. It is not intended to reproduce in detail the comments made in those reports as to the operation of the proposed PenOp signature. However to enable this paper to be read without reference to those other materials it is important that it provides a brief description of PenOp's manner of operation, and its essential characteristics.
- 6.2 From the user's point of view the PenOp system is designed to be the digital equivalent of writing a signature on a piece of paper. It permits a user of the system to sign his or her own name, in his or her own handwriting. This signature is written using a stylus upon a digitising pad. From the users point of view, the "signature" is not a digital signature, but an actual signature. This is then converted to a digital form.
- 6.3 There are two essential features of the PenOp signature. The first is called the "Signature Capture Service" (SCS). This occurs when the person signs his or her name on the digitising pad (or the screen)¹⁹. The SCS works in conjunction with software which prompts the user to complete the various steps involved in applying his or her signature. It comprises the following basic steps:
- (a) the SES receives information to verify the user is who he or she claims to be;
 - (b) the PenOp system then produces what is known as the "Gravity Prompt". This feature indicates the purpose for which the signature is being captured, and may refer to the electronic document that is being associated with the signature; and
 - (c) the signature is then inscribed by the signatory on a pad or the screen.
- 6.4 The "Gravity Prompt" is a very important feature. We are informed that the particular wording of the Gravity Prompt is intended to be determined by the developer of the particular application. The wording of the "Gravity Prompt" may well change depending upon the specific legal requirements of certain types of documents. This is obviously a matter upon which individual users should seek separate advice, as the wording of the Gravity Prompt forms part of the process by which an intention to be bound is evident, and so has legal consequences.
- 6.5 When the signature is inscribed, and confirmed, the software samples the signature, measuring its size, shape, relative positioning of the curves etc, and even the relative speed at which each feature is imparted. The statistics that are thus produced are called the "act-of-

¹⁹ On the information available to us it appears that the inscription of the signature does not necessarily require a digitising pad. The signature can be inscribed directly upon a window on the computer's screen.

signing statistics”. Once the signature is approved, the SCS then hashes the document to which the signature is “affixed”, to produce the digital signature for that document.²⁰

- 6.6 The PenOp software goes further than this. It uses the act-of-signing statistics, the first hash or digital signature (which relates to the specific document), and other information such as the date and time of signing, the identity of the machine, the claimed ID of the user, the words that appeared in the Gravity Prompt and (as an option) the data reflecting the graphic image of the user’s signature, and computes a second hash value or digital signature, in respect of *all* of this information.
- 6.7 The information referred to above, together with the second hash value or checksum, is encrypted to generate what PenOp refers to as a “Biometric Token”. A final hash of the integrity checksum is calculated and incorporated into the Biometric Token. The entire Biometric Token is then encrypted and subsequently stored.
- 6.8 The generation of the Biometric Token in this manner links not only the signature and the document, but also the person to the signature. Whilst we do not have the capacity to comment on the technical aspects of the security of this system, from a legal perspective, provided evidence is led as to the manner of operation of the system, and that evidence is accepted by a court, the production of the Biometric Token ought to present a very secure link between the signature and the document. Retaining the optional image of the signature may well add to the weight of evidence that can be presented to prove (or disprove) the signature, as it is in a form (handwriting) that the Courts will find familiar.
- 6.9 There is also a second feature to the PenOp system which can be implemented if required. This feature is called the “Signature Verification Service” (SVS). The process we have described above, which generates the Biometric Token and then encrypts the data, provides a secure link between the signature and the document. It does not necessarily answer the question: is the person who claims to be Mr Jones or Ms Smith actually that person?
- 6.10 The SVS depends upon previous data for its operation. It works by evaluating whether a particular Biometric Token matches the act of signing the statistics that have previously been stored. It will then produce a figure representing the percentage of the most recent signature that matches the earlier stored data. As was pointed out by Dr Walden, verification is not a requirement for legal validity and any organisation making use of the PenOp system ought to separately consider whether or not such a feature should be implemented.
- 6.11 The principal use to which the PenOp system is likely to be put (and there are a variety of uses for this software which go beyond verifying a document) is by the attachment of the Biometric Token to a document to evidence a “signature” or assent. With appropriate

²⁰ In the papers of Mr Wright and Dr Waldren, the hash value is referred to as a checksum. Both expressions refer to the string of data that represents the contents of the electronic document.

evidence and expert advice, which will be discussed in more detail later, this should be sufficient to verify that a particular signature was attached by a particular document.

- 6.12 It will leave open for dispute whether or not a particular person “signed” the document. The SVS process may provide probative evidence of the identity of the person signing the document, however this depends upon the data that is utilised as the basis for the “comparison”. Again, we will discuss this in more detail in the next part of this paper, which looks at the legal issues arising from the PenOp system as described, and in particular the admissibility of evidence.

7 The PenOp Signature: Evidence

- 7.1 An essential part of considering the commercial utility of any digital signature system, including the PenOp system, is to consider whether or not this operating system will be accepted as evidence in the Australian Court's system.
- 7.2 In Australia, like the United States, there are both State and Federal Courts. This is because there are certain matters which are within the legislative power of the Commonwealth. Federal Courts generally deal with such matters. Examples include immigration, customs, international obligations, certain aspects of taxation and social security, defence procurement, corporations, and many others. In the State Courts, there is a hierarchy, with the Supreme Court being at the top, followed by District or County Courts (depending of the State), and the Local Courts at the bottom²¹.
- 7.3 Jurisdictional limits to the powers conferred on the lower Courts vary from State to State. Further, the forms used and procedures adopted vary significantly between the courts both within the hierarchy, and between the States, which can often have a substantive impact upon the rights of parties²². Under the Australian legal system, it is perfectly possible for States to have different approaches to different legal issues. Likewise the Commonwealth can have a different approach. However, in relation to the admissibility of evidence, it is fair to say that there is generally a high degree of correlation between the Courts of the States and the Commonwealth. In other words, if evidence is admissible in one State Court, it is quite likely to be admissible in every other State Court, and also in the Federal Court.
- 7.4 There are two basic sources of law regulating the admissibility of evidence. One is the common law (or Judge made law), and the other is statutory. This latter source of law is principally found the various Evidence Acts that apply to the particular States, and to the Commonwealth. The Commonwealth, and certain States, have recently revised their Evidence Acts, to improve the useability of the Act, in proving documentary transactions.²³
- 7.5 Therefore, in order to consider the admissibility of a document that exists electronically consideration needs to be given to the common law position, and also the operation of the various Evidence Acts.

²¹ There are several other statutory tribunals given the capacity to hear specific disputes, including the Administrative Appeals Tribunal, the Commercial Tribunal, and the Small Claims Tribunal. Rules of evidence tend to be more relaxed in such "quasi judicial" tribunals.

²² The rules of the Courts, for example, may affect the capacity of a plaintiff to commence proceedings outside the limitations period. Differing rules have in the past resulted in "forum shopping" to obtain an advantage for certain litigants.

²³ For example, under section 48(1) of the Evidence Act (Commonwealth), it is possible to tender a document that is stored in such a way that it can only be retrieved by use of a device (such as a computer and printer), by tendering a document that has been produced by such a device. Therefore, if the documents stored are "Business Records", then by reproducing them in physical form, they ought to be able to be tendered as evidence before a court. It will still be necessary to comply with the requirements for the proof of Business Records under that Act.

7.6 Before looking at these issues, we point out that the principal evidential problem lies with the document being created and held in electronic form, rather than with the PenOp signature. In order for the PenOp signature to be considered by a Court, the document to which it is attached must be admitted into evidence. Problems relating to the admissibility of electronic documents are ubiquitous, not confined to electronic documents utilising the PenOp signature.

Common Law

7.7 At common law, it is difficult to prove the contents of a document generated electronically. This however depends upon the contents of the document sought to be proved. Generally, facts asserted in documents such as computer records cannot be proved by producing a printout from the computer. This is only hearsay evidence of the facts contained in the document. Rather, a witness to the facts must be called. Obviously this is difficult if not impossible in many cases.

7.8 There is a possible exception to this that may be relevant: that is, where a computer is used to record and retrieve data that is not supplied by a human source. If the computer acts as no more than a recording device, like a tape recorder, then the data may be admissible without a witness to affirm the facts.

7.9 Overall, it is difficult to prove the contents of electronic documents under the common law, because of the hearsay rules.

Evidence Acts

7.10 The various Evidence Acts all have provisions relating to the proving of “Business Records”²⁴. Generally, a Business Record is a document produced in the course of a business that is the product of a particular procedure, often involving mechanical entry of data with subsequent processing by a computer. The various provisions these provisions allow documents to be proved as a Business Record despite the hearsay rule, which may otherwise operate to prevent computer generated documents being admitted into evidence.

7.11 However the admissibility does not determine the weight to be given to the document. A document may be admissible as a Business Record, yet accorded little weight because of evidence that the information may not be accurate.

7.12 Despite the provisions of the various Evidence Acts, it can still be difficult to prove a computer generated document as a Business Record, with some jurisdictions being more difficult than others. The provisions in the various Evidence Acts are not identical and in some cases quite dissimilar between States. It is not appropriate for us to set out the

²⁴ Evidence Act 1995 (Cwth) s69 (applies to the ACT); Evidence Act 1906 (WA) s79C; Evidence Act 1995 (NSW) s69; Evidence Act 1977 (Qld) s93; Evidence Act 1929 (SA) s45a; Evidence Act 1910

procedures that must be followed, and the requirements that must be met in order to “prove” (have admitted as evidence) a computer generated document on a State by State (and Territory) basis. Materials and commentary on such issues can be found in “**Laws of Australia**” and other similar publications.²⁵

- 7.13 South Australia, Queensland and Victoria have specific provisions in their Evidence Acts that regulate the production of computer generated documents.²⁶ Again, advice should be sought on a case by case basis in respect of these provisions.
- 7.14 The essential point to note is that until changes are made to the laws governing the admissibility of evidence in Australia, there will always be the potential for objections to be taken to the production of computer generated documents as evidence in Court proceedings. If objection is taken, the difficulty of proving the document varies between jurisdictions.
- 7.15 The use of the PenOp signature is only one aspect of the matter. PenOp merely provides a method of ensuring (as far as realistically possible) that the document retains its integrity (ie. it has not been tampered with), and it was signed by a particular person and so the terms have been accepted. If objection is taken to the admissibility of the entire document because it is electronically generated, the PenOp signature does not necessarily add to the burden of proving an electronic transaction that may already exist. Rather, with proper evidence of the operation of the system, a Court may be better informed about the probability that a document has not been modified or tampered with, and that it has been “signed” or agreed to by a particular party.
- 7.16 There is however, always the possibility that the defendant to an action can challenge the authenticity of a document, even if it is otherwise admissible as a Business Record. This type of challenge is open to a defendant irrespective of whether or not a document is generated from computer data, or is written on paper and is signed in ink. If such a challenge were to be made, proper evidence in admissible form would need to be lead as to the operation of the PenOp system, and in particular the generation of the Biometric Token. This evidence would then be assessed by the court or tribunal, and it would form a view as to whether or not the document was admissible or not.
- 7.17 If the authorship of the signature inscribed under the PenOp system was challenged, and the author was sought to be verified by the SCS system, then further detailed evidence would need to be lead as to the operation of this system, and its reliability and accuracy. We can not comment on the technical aspects of this, save as to note that the capabilities of any technical system are always open to be questioned.

(Tas) Pt III Div 2B; Evidence Act 1958 (Vic) s55; Evidence (Business Records) Interim Arrangements Act 1984 (NT) ss1-22;

²⁵ **Laws of Australia** (supra n13) at part 16.6; **Cross on Evidence** (Australian Edition) esp. at 35185-35370.

²⁶ Evidence Act 1929 (SA) s45a; Evidence Act 1958 (Vic) s55B(7); Evidence Act 1977 (Qld) s95

- 7.18 That said, one of the available features of the PenOp system, as we understand it, is the ability to reproduce the actual signature, rather than merely a string of numbers or letters which represents the checksum. Courts are used to dealing with disputes as to the authenticity of signatures which have a physical form, and this may give them a degree in comfort in determining disputes. Also, individuals are familiar with signing their names to signify consent. It may be (although this cannot be verified) that the act of signing a name may make it less likely for a person to dispute the fact that he or she agreed to the terms of an electronic document.
- 7.19 Nevertheless, it is fair to say that any digital system signature, absent the benefit of presumptions under Legislation, is open to be challenged as to its accuracy and reliability, and if it is challenged, the evidence which will need to be led to verify its accuracy and reliability is likely to be relatively complex and time consuming (and thus more expensive than simply proving the traditional paper document). This is a factor that intending users ought to consider.
- 7.20 There are undoubtedly way to minimise the risks of problems arising when entering into commercial relationships. It may be that parties intending to use the PenOp could include terms in the standard agreements they enter into providing that the parties confirm their acceptance of the system. Again, this is a matter that needs to be addressed by individual users, and appropriate advice taken.

8 Conclusion

- 8.1 Under the general law, a signature is little more than a mark that is applied by a person to a document which verified that person's assent to the contents of that document. It is useful when it comes to enforcing agreements, as (absent an allegation that the document has been tampered with or the signature is not authentic) it is difficult to dispute a written agreement that has been signed by a party.²⁷
- 8.2 So far as it is applied to particular commercial circumstances that are not otherwise affected by statutory requirements, there is no apparent reason why the PenOp signature should not prove to be as acceptable as a standard written signature. Written signatures are not themselves without risk of being challenged. Equally, the PenOp system provides an alternative that, whilst not free of the possibility of being challenged, nevertheless appears to be sufficiently secure to suffice for ordinary commercial transactions, particularly where the identity of the signing party is not a critical issue.
- 8.3 Against this general background there are inevitably going to arise situations where the legality (and thus enforceability) of the PenOp signature will need to be assessed against legislative or regulatory requirements. Such requirements may relate to the form of signature,²⁸ or may relate to the form of the document (that it be of a particular type, ie not necessarily electronic). As we have discussed, there are many areas where regulations and legislation could affect the proposed operation of the PenOp digital signature, or indeed any other type of digital signature. Requirements for certain contracts to be "in writing" are but one example of this: and there is considerable scope for argument as to exactly what may constitute "writing" depending on the various definitions that may be provided.
- 8.4 A major consideration for any person contemplating doing business via a purely electronic medium is the enforceability of any agreement entered into. This not only depends upon statutory requirements (whether it is legally permissible to enter into a particular type of agreement in a purely electronic form) but also upon the capacity to "prove" the agreement in enforcement proceedings.
- 8.5 Evidential difficulties arise both in respect of the electronic document itself, and also in proving that the PenOp signature system reliably authenticates a document. The Evidence

²⁷ We note that no matter how secure a signature is in identifying a person's assent to an agreement, it can never prevent arguments being raised as to pre-contractual misrepresentations, or equitable or statutory matters (such as unconscionable conduct either at equity, or under the Trade Practices Act) that may otherwise vitiate the agreement.

²⁸ For example, under the Interpretation Act 1984 (Western Australia), "sign" is defined: "...includes the affixing or making of a seal, mark, or thumb print...". Thus where a West Australian Act requires a document to be signed, and does not otherwise provide a means of doing so, the affixing or making of a seal, mark or thumb print will be satisfactory. However, the use of the words "includes" means that there are undoubtedly other acceptable methods. What is acceptable will depend upon the circumstances and a construction of the particular Act or Regulation. It may be that the PenOp signature method is acceptable in many cases, although this must be approached on a case by case basis, with advice taken prior to embarking on any course of conduct which relies upon such a method.

Acts of the various States and the Commonwealth all have provisions facilitating proof of “Business Records”, and several also have specific provisions governing computer generated documents. This does not mean that it will necessarily be easy to prove an electronic document in the face of a vigorous challenge, although this may be the case irrespective of the operation of the PenOp signature system.

- 8.6 It is most important for prospective users to identify as precisely as possible the nature of the transactions to which it is proposed to apply the PenOp system, and to seek specific advice in respect of such transactions. In this way, possible problems can be identified and the user may be able to minimise any risks.
- 8.7 If the proposed legislation regulating electronic commerce (such as the ETA discussed above) is enacted, and broadly similar legislation is enacted throughout the Australian States and Commonwealth, then the use of digital signatures for should be greatly facilitated. However, no State or Territory, nor the Commonwealth, has at this time actually enacted legislation in this regard.

This paper provides general information only, and it is not intended to be treated as being legal advice on any specific issue, nor is it intended to be exhaustive legal analysis on all aspects of the PenOp signature. If legal advice is required on any particular issue discussed in this paper the reader should seek specific advice from a solicitor. No warranty is given for the accuracy of any of the information referred to or repeated in this paper.