

Identity Crime – A Different Perspective

**A discussion paper presented to the
Corruption Prevention Network Annual Conference 2003**

**By
Nick Wolanin¹
of the Australian Crime Commission**

Introduction

Identity theft and fraud are big problems, but the debate often seems stuck on the issue of how you can so easily churn out authentic looking birth certificates on a cheap colour laser printer. That's a problem right here, right now, but it's not the future. In 1988 I was investigating a guy who used a dot matrix printer to simulate cash register imprints on stolen blank NSW driver licence forms. Structurally, nothing's changed since then, including the debate, but I think there's something bigger over the horizon.

The Role of Government

On one view, the regulating and licensing of certain people to do certain things is the *raison d'être* of Government. The alternative is chaos where anyone can do anything. Part of holding back the chaos is proper record keeping of authorisations and licences. Engaging in a regulated activity without licence invites government intervention and sanction. Hence, there exists a market for false authorisation, which, at the moment, is largely satisfied through forgery or identity fraud. But our reliance on paper documents as proof is rapidly diminishing.

Checking Credentials

Traditionally it has been difficult to verify credentials with an issuing authority because it was only open Monday to Friday, 9 to 5, might be very distant geographically and was probably disinclined to provide information over the telephone. Academic credentials are a good example. When was the last time you actually double-checked a job applicant's academic transcript with the issuing university? We rely on the plausibility of the applicant's official looking documentation to be the proof of credentials. In fact they are synonymous in our minds because most regard the actual paper

¹ The opinions in this paper are those of the Author and not the ACC.

document as the credential. The paper documents are merely secondary evidence of something in the university's records, yet we treat them conventionally as primary evidence.

People wishing to fraudulently undertake an activity without proper government authority often seek to simulate that authorisation. Up to now, government has really only been a spectator because forgery of an official document only incidentally involves the issuing authority. The traditional response has been to use increasingly sophisticated documents which resist or more readily reveal copying or forging, but the focus is still on the document as primary evidence.

Compare this with the evolution of land title provenance. In Old System title the actual paper document was the instrument of ownership and had to be returned to the Registrar for annotation upon transfer, subdivision and such. The document itself was the instrument and as such could be forged either in its entirety or just in a particular, or copied and then passed off as authentic. The problems with this are obvious, hence the move in Torrens Title to regard the deed, if that term can still be used, as merely a memorandum about the contents of the land title register. No sensible person would act solely on a land title search document unless they were certain of its contents by obtaining one directly from the land titles registry. The system enables anyone to cheaply and readily obtain their own search certificate. Thus there is reduced opportunity for a scoundrel to pass off a forged certificate, for example to fraudulently obtain finance. In time, as internet access spreads, the community will grow to accept direct on-line access to the same information. There is already a capability in NSW to access land titles information “at source” through on-line brokers (see <http://lpi-online.lpi.nsw.gov.au/lpsearch/brokers.html>).²

Returning to the university example, if every institution set up a web site into which anyone could type in a student number (and some other details from a transcript) and see in response a list of subjects and results, where would be the value in forging a transcript? Of course this has privacy implications; but a real working example of on-line verification is the Commonwealth Government's [business entry point](http://www.abr.business.gov.au) web site.³ It will accept either a company name or an Australian Business Number (ABN) and then

² <http://lpi-online.lpi.nsw.gov.au/lpsearch/brokers.html>

³ <http://www.abr.business.gov.au>

tell you the corresponding piece of information. Instantly one can check whether a business registration exists and that the number being quoted is genuine.

ASIC also provide a similar system of [checking company names](#)⁴ and details and while it might not stop a genuine company operating dishonestly, they at least need to “legitimise” their crooked existence with Government. In other words, the framed certificate of incorporation on the company secretary's wall is mere decoration. The real proof of the company’s existence is in the Government record, which can be independently verified. A bogus company now needs a bogus official record and that can only be created by corrupting or tricking a government employee (or agent of government), or exploiting some loophole in an automated administrative system.

Of course there is the risk of spoofing (logically impersonating) a web site to generate false information, but I think you'll agree that is a challenging technical task and one which cannot be sustained for long.

Some banks in NSW are already linked to Births Deaths and Marriages and can check the details on a paper birth certificate directly with the register. What use then is a forged paper without a correspondingly forged electronic entry on the register?

Centralised Licencing

An important development is the centralised authentication of licensees. This is a reality in NSW. In time there will be a single infrastructure which will administer all NSW issued licences whether it be driving, wildlife culling, fishing, industrial machinery operation, you name it. The system will be highly resistant to the creation of false identities because it will, in real time, verify at-source the supporting details.

For example, if someone applies to be registered as a nurse in NSW, the system will use the applicant’s existing details (such as on a driver’s licence) to interrogate the university database which the applicant proffers as their accrediting institution. Only an authentic, real-time, electronic response from the University will lead to the registration of the person as a nurse (all other requirements being met). Hence, if an applicant applies for a crane operator’s licence (through Workcover) it will be through the same

⁴ <http://www.search.asic.gov.au/gns001.html>

centralised system which will have a “does not compute” fit if the applicant has different details such as residential address or date of birth on their driver’s (or indeed on any other) licence.

What this will mean is that as Joe Citizen builds up his interaction with the NSW Govt. through various means, the identity becomes more difficult to steal. In other words, when he applies for a driver licence, the on-line licencing system will grab his birth details directly from Births, Deaths and Marriages. What use then is a false birth certificate if it cannot point the system to a real database entry at BDM? The details on his driver’s licence must then square with the details from the University (which says he has a nursing degree) when he applies for his registration as nurse. And if he decides nursing is boring and decides to sell real estate instead, all the details above must square when he finishes his certificate at TAFE and seeks a real estate agent’s licence from Fair Trading. And so on.

Furthermore, when one enters the system with a photo (usually for a driver’s licence) that’s it. The same photo should be used for all subsequent documents. So, for example if one fronts for a pistol licence as a security guard, a new photo isn’t taken, the one on file (electronically at the RTA) just goes straight onto the document.

The longer a person is involved legitimately (or illegitimately, if they manage to get in) with the system, the harder it will be to steal their identity. If the system knows you from say 15 different angles, all with records of interlocking validity, any attempted interaction, without complete information (to create say a 16th document in another category) will sound the alarm.

Similarly, face recognition software could be applied to the RTA database to check for the same person appearing more than once.

All this is about to happen and should completely change the threat analysis in relation to ID theft and fraud. See this website for more info....

<http://www.oit.nsw.gov.au/pages/5.4.3.nswg1p.htm>

What does all this mean?

If I’ve convinced you that in the longer term, the use of forged paper is a dead-end for criminals, what are the future threats? I’d say in forged foreign

documentation and the corruption of public officials because both angles represent the main risks of crooks getting a foothold in the new electronic identity system. And once in, they can build a robust and multi-faceted false identity.

Foreign Documents

The foreign documents problem is obvious. For example, my Mother's Russian birth certificate is absolutely unverifiable. Moreover, at the time of her birth, they used the Gregorian calendar in her little neck of Siberia, so you can imagine my remonstrating with a young Australia Post officer about the date on the passport application differing, for good reason, from the birth certificate and her certificate of naturalisation.

How we solve the abuse of systems which enable the entry of persons with foreign documents should be one priority area. The other area is corruption.

Corruption

Eventually, the ubiquity of the internet will allow anyone to verify credentials directly with the issuer, without the need for secondary, documentary evidence.

In these circumstances, the risk for government regulation is that if forging a document no longer has a criminal value, criminals must find other ways to achieve the same outcome. To now get away with a false land title confidence trick, the government's records of land titles must be corrupted at source. Having accomplished this, a routine check of the land title register will yield up an apparently genuine and official record. This can only be done by tricking or corrupting officials involved in the processing of government records, or to insert "moles" into strategic positions within an agency through normal recruitment.

This trend; a movement from government being incidental to a crime toward becoming unwillingly complicit in facilitating a crime, will eventually impact upon all agencies which carry out some certification, verification or licensing role. If organised crime in the building industry can no longer get away with forged heavy equipment operators' licences, Workcover will become the target of record falsification. If confidence tricksters passing themselves off as trades people can no longer get away with forged licences, Fair Trading will become the victim of database falsification attempts. In

relation to the centralised, on-line licencing system in NSW, one can easily imagine the immense value to organised crime of a corrupt official.

In the meantime

A shorter term effect of increasingly sophisticated anti-forgery methods for paper documents is that the criminal milieu may abandon attempts at forgery and instead concentrate on corrupting officials to provide genuine blanks or completed documents with false details. In other words, when the effort necessary to corrupt becomes less than the effort to commit a crime without official assistance, corruption risks are likely to increase.

Conclusion

Whether it is the uptake of electronic ID systems or the hardening of anti-forgery methods for paper documents, the shorter and longer term trends are likely to be increasing official corruption unless we act in that area now.

Author's Biography

Nick Wolanin is the Manager, National Operations Directorate at the Australian Crime Commission. For the past 17 years, he has worked in various Commonwealth and NSW State law enforcement agencies and is an adjunct Senior Lecturer at the Australian Graduate School of Policing. He has formal qualifications in various sciences, including criminology and management.

Along with Marie O'Bryan, David Fenwick and Warwick Smith, he was a co-founder of the Corruption Prevention Network.