Terrorist Mohamed Atta – master of identity crime.

Identity unknown?

Australians lose about $1.4 billion each year through identity crime and personal fraud.

When Mohamed Atta and 18 other terrorists executed the September 11 attacks in 2001, they had amassed a total of 364 false names between them. Indeed, Atta had been trained by Al Qaeda in passport alteration and 11 of the hijackers were suspected of using altered passports with detectable changes. Identity fraud was a fundamental enabler of the terrorist attacks.

So too, identity crime is a gateway enabler across all crime types. According to the Australian Bureau of Statistics Personal Fraud Survey 2010-11, Australians lost $1.4 billion through personal fraud. Alarmingly, the survey estimated that 1.2 million Australians aged 15 years and over were victims of at least one incident of personal fraud, including identity fraud.

The prevalence of identity crime as a means of disguising a criminal's activities in other nefarious acts further spreads the reach of these crimes deeper into Australian society. From the drug trade and human trafficking to financial fraud to terrorism – identity crime is a basic means of producing funds to finance other crime and a means of hiding from law enforcement and prosecution.

Furthermore, international research suggests identity crime is the fastest growing crime type. This growth is exacerbated by organised crime syndicates who contribute to its spread and then direct the proceeds to other criminal activities.

"It's a little bit like the Greek Hydra," says Federal Agent James McMillan. "You cut off one head and another two grow." Federal Agent McMillan is a former team leader with the Sydney Identity Security Strike Team (ISST). He says the lure of easy money and the relative simplicity of forging basic identity documents make it extremely difficult to halt completely.

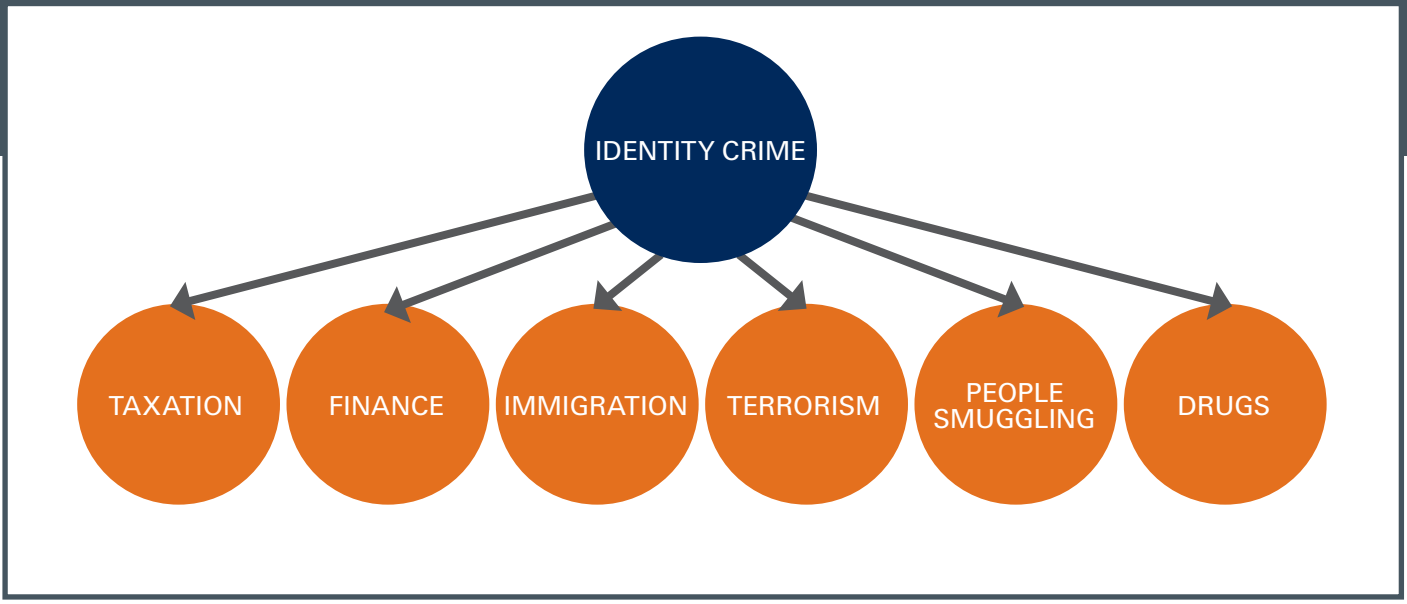
How it works

Identity crimes start with simple 'breeder documents' such as birth certificates and billing accounts, which can be produced on home computer technology. More elaborate documents such as a Medicare cards, credit cards and driver licences are produced with slightly more professional but easily used and commercially available equipment.

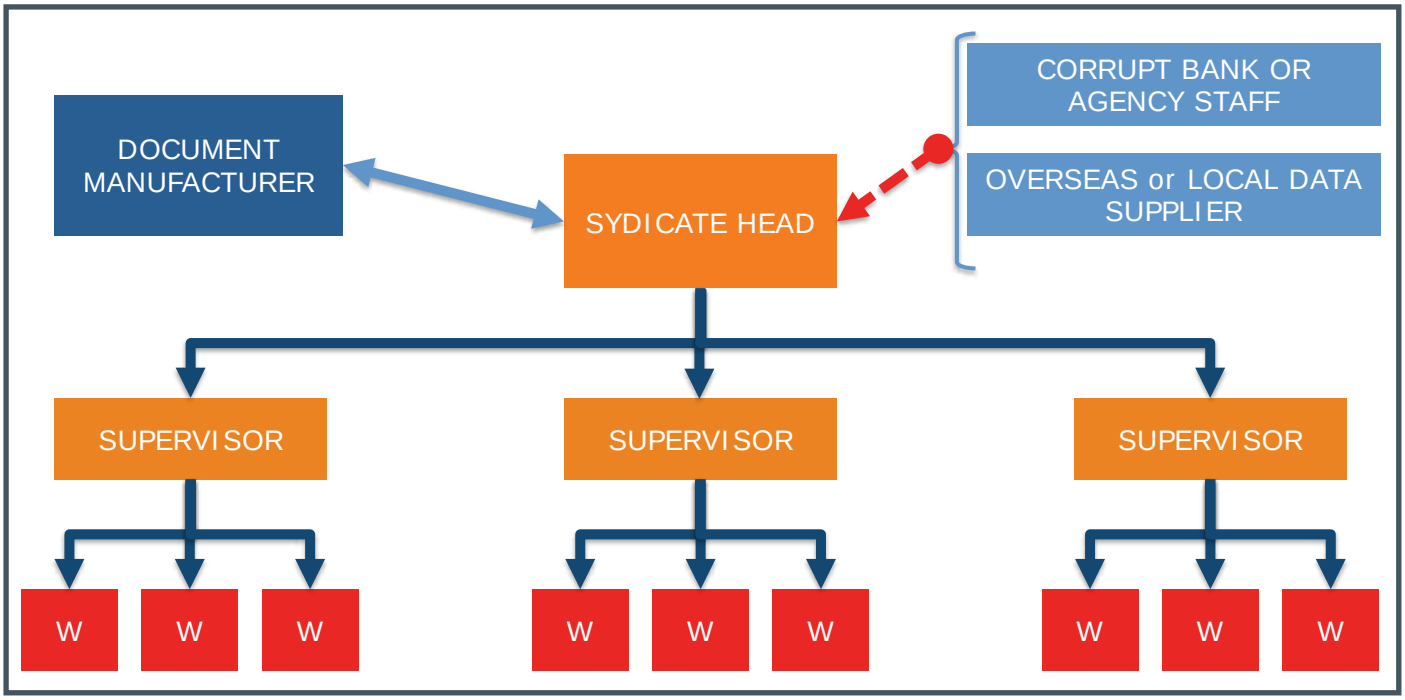
The 'identity bundle' is then used for the 100-point security-identification process that most Australian government agencies and financial institutions rely upon. This can be used to access everything from credit cards, bank accounts and employment, which could allow access to secure facilities and computer systems.

Operation Zulu is a classic example. The joint AFP and ATO investigation was commenced after ATO identified extensive Business Activity Statement (BAS) fraud. Stolen identification information had been used to establish 81 companies and businesses. Other false documentation was used to obtain Post Office boxes, bank accounts and telephone accounts.

The identity information was obtained from a job-vacancy scam. A criminal enterprise placed a job advertisement for a secure waste management company in an online newspaper. Employment applicants willingly handed over large volumes of



Identity crime enables crime throughout the community.



Highly organised crime syndicates are capable of defrauding millions of dollars in a single week.

What is identity crime?

Standard definitions are used by law enforcement agencies throughout Australia.

Identity: a term that encompasses the identity of natural persons (living or dead) and the identity of bodies corporate.

Identity fabrication: is used to describe the creation of a fictitious identity.

Identity manipulation: is the alteration of one's own identity.

Identity theft: is the theft or assumption of a pre-existing identity (or a significant part thereof).

Identity crime: is a generic term to describe activities/offences in which a perpetrator uses a fabricated, manipulated or a stolen/assumed identity to facilitate the commission of a crime or crimes.

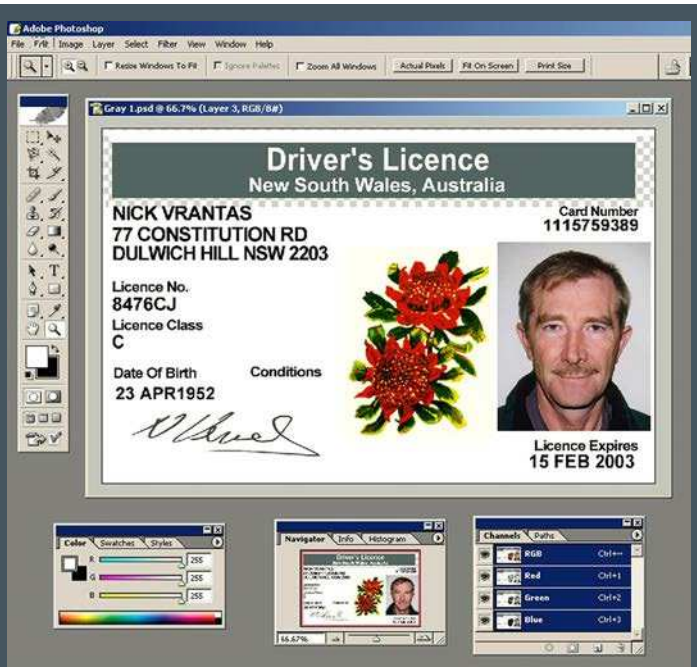
personal identity information as part of the interview process. The only face-to-face contact between the suspects and service providers was in the opening of the bank accounts.

The suspects used the information to create alternate identities. These identities were subsequently used to open the bank accounts, incorporate Australian proprietary limited companies and submit false BAS' to the ATO for the refund of Goods and Services Tax to those false companies.

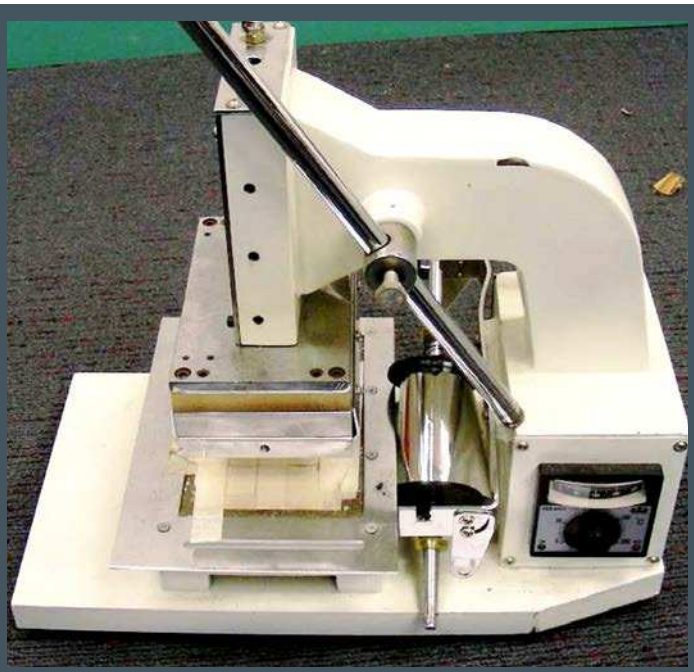
All this was done from a suburban mini storage shed using mobile telephones, a laptop and a high-quality printer – but was only possible through the manipulation of personal identification information. When the suspects were arrested in 2012, they had amassed $400,000 each in a very short time.

Enabling serious crime

An even more insidious use of identity crime is its ability to underpin more serious criminal acts. The Sydney Identity Security Strike Team (a multi-agency taskforce between the AFP, New South Wales Police Force and the Department of Immigration and Border Protection and supported by New South Wales Roads and Maritime Services) Team Leader Mike McKay says



Driver licence software template and card printer are capable of producing credible identity documents from a home factory.



A tipping/gilding machine seized during Operation Avarice places coloured black, red, silver or gold tipping foil on the raised embossing on plastic cards.

the broader problem of identity crime as an enabler to serious organised crime in all its guises cannot be underestimated. He says wherever a criminal act is being carried out by an offender there will be the desire to disguise their identity.

"False identities can be basically used for any criminal or nefarious activity where a person seeks to disguise their true identity in the hope of deceiving others, including law enforcement," says Federal Agent McKay.

"This can be as diverse as an underage person having a false driver licence with an altered date of birth through to serious and organised criminal syndicates using false identity documents for the importation of narcotics and subsequent remittance of those millions of dollars of proceeds of crime overseas."

Operation Zulu also highlights issues where identity crime enables other crime types. One of the suspects in Operation Zulu was first arrested by the Queensland Police Service in relation to the resolution of a major drug investigation. AFP investigations into the importation of Tier 1 illicit substances (heroin, cocaine and amphetamine type substances) reveal that a significant percentage of all parcel post importations are facilitated by a false identity.

Federal Agent McMillan says during state and federal investigations it is common to find identity crime is involved at some level in major drug investigations, human trafficking, people smuggling, frauds (credit cards, loans, mortgages, and immigration), money laundering, overseas remittances and terrorism.

"We often find when we do search warrants and resolutions of major identity crime investigations that there are also other crimes involved, such as seizing large amounts of narcotics and occasionally firearms and so forth," Federal Agent McMillan says.

Sophistication

The rise of identity crime is aided by the sophistication of criminal syndicates and the technology now available to support them. The potential benefit to criminals is staggering. So it is not surprising that criminals are organising criminal syndicates in ever-increasing sophistication. The recent resolution of Operation Arkanis in September 2013 is a case in point.

Operation Arkanis was focused on an Identity (ID) Crime syndicate in Sydney that was manufacturing NSW driver licences, Medicare cards and credit cards. The investigation had established the specific location of where the fake documents were being produced.

Confiscated materials from Operation Pulse.

Identity bundles are a key stepping stone to creating bank accounts and even companies under false identities.

Card embossing machines seized in Sydney during Operation Pulse.

Federal Agent McKay says what investigators found was effectively a manufacturing line.

"The house was set up for the production of counterfeit IDs," says Federal Agent McKay. "As you would expect, there were the relevant materials and equipment to manufacture IDs such as tipping machines, manual and auto embossers, and high quality double sided printers for printing cards on both sides."

"There was also the necessary equipment to allow the images and data to be copied onto these cards, such as laptops, some software programs and the stock with magnetic strips or data chips needed to produce credit cards, Medicare cards and driver licences."

Federal Agent McKay says there is little evidence that high-tech equipment and technologies needed to make fake IDs are procured from legitimate suppliers. He says the technologies required to make high-quality reproductions are mostly sourced from Asia. Incredibly, security measures such as holograms and magnetic strips are produced to such a high quality that the average person would not be able to detect the difference between real and fake products.

Operation Avarice illustrates the international reach of ID crime syndicates. This operation investigated a crime syndicate of predominantly Malaysian nationals operating on a scale previously unseen by ISST investigators.

The syndicate collected personal identification information and credit card information from dedicated providers in the United Kingdom, Malaysia and Spain. The card data was electronically transmitted to a syndicate head in Australia through various means. The syndicate imported manufacturing consumables into Australia, such as blank magnetic credit card stock, encoding and card printing equipment, which was legally sourced primarily from China and the USA.

The counterfeit credit cards and supporting identity documents, including Medicare cards and New South Wales driving licences, were used to undertake organised shopping activities across Queensland, New South Wales, the Australian Capital Territory and Victoria. These cards were used to purchase high-end electronics, store gift cards, tobacco and alcohol, which were then sold for profit.

Eight suspects were arrested in New South Wales and Victoria and charged with participating in a criminal group and dealing in instruments of crime valued in excess of $1 million. The investigation dismantled a major criminal syndicate that had been operating across Australia and internationally.

Law enforcement teamwork

Multi-agency teamwork is a major contributor to the success of law enforcement to counter ID crime. The AFP hosts the Sydney ISST, which is a multi-agency team comprising officers from the AFP, NSW Police Force, Department of Immigration and Border Protection and NSW Roads and Maritime Services (formerly the RTA), dedicated to investigating highly organised syndicates involved in the supply, manufacture, distribution and use of false identity documents and identity related crimes.

The ISST has had significant success with investigations over the past few years, and this is credited to the ongoing commitment of the embedded agencies, sharing of intelligence in real time and the combined use of our resources during periods of high demand.

The ISST sees the positive results with our engagement with the Criminal Assets Confiscation Taskforce and NSW Crime Commission in dismantling these criminal syndicates and restraining of the proceeds derived from their criminal enterprises.

The ISST works closely with financial institutions, state/territory/Commonwealth law enforcement agencies, regulators and industry in tackling ID crime and ID security. An important partner is also the Attorney General's Department, which leads the Government's work under the National Identity Security Strategy (NISS).

The NISS provides a framework for inter-governmental cooperation to strengthen Australia's federated personal identification processes. The NISS includes a number of measures to enhance identification and verification processes, combat identity theft and prevent the misuse of stolen identities. A keystone initiative of the NISS is the Document Verification System (DVS).

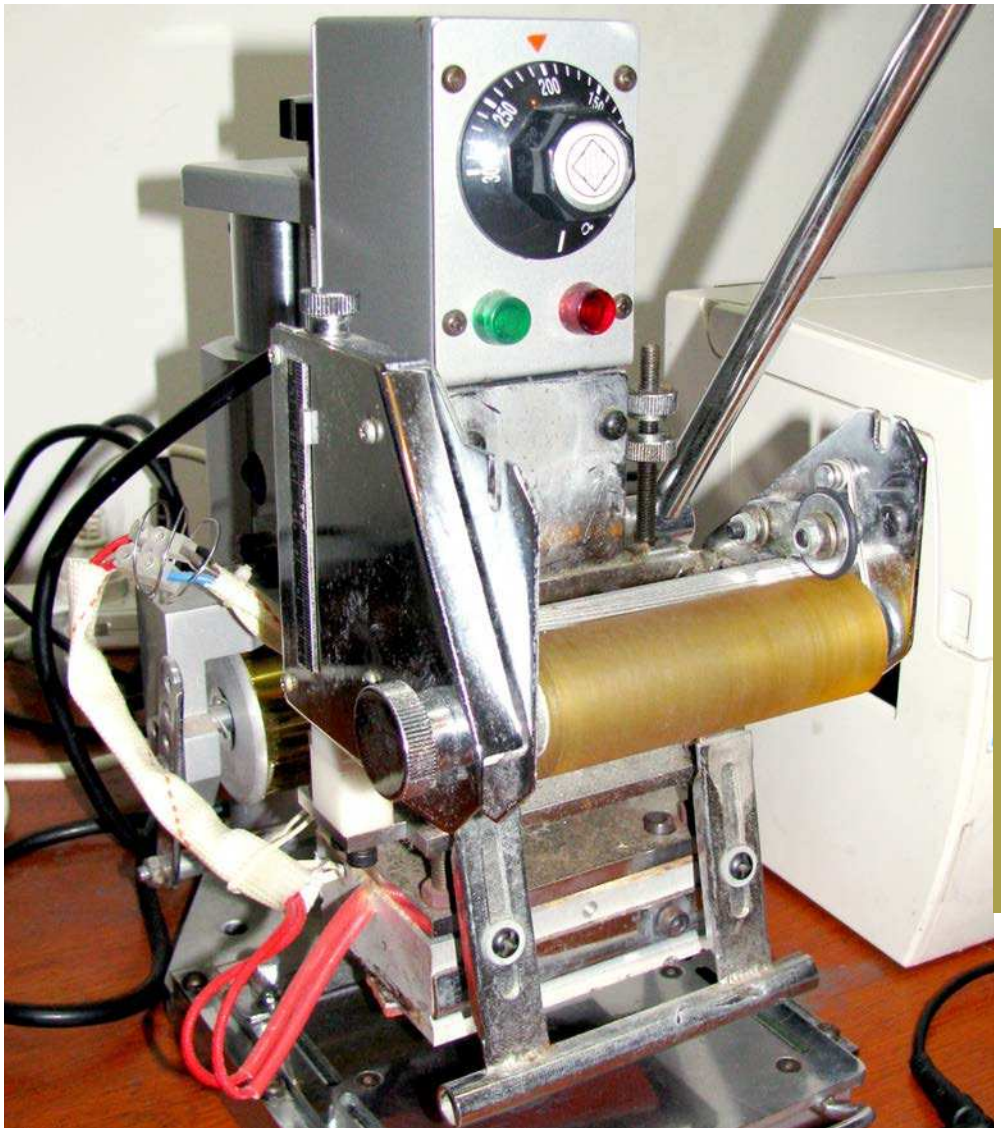
The DVS is a national online system that allows organisations to compare a customer's identifying information with a government record. It is a secure system that operates 24/7 and matches key details contained on Australian-issued identifying credentials, providing a 'yes' or 'no' answer within seconds. The DVS offers a practical way for organisations to reduce identity crime and misuse, which affects their reputation and their clients.

Until recently, the DVS was available only to government agencies. Since late 2013 however, the service has been extended to industry for use in businesses with legislative obligations to identify clients, such as the

Precautionary Tips

Police are reminding the public to take precautions to limit the risk of becoming identity-crime victims. There are some very effective tips that minimise a criminal's opportunity to use your personal details and identity. These include:

- Have a mailbox that is secure and always keep it locked.
- Always store any personal or financial documents in a safe place.
- Destroy old documents and cards before disposing of them, otherwise your trash could become someone else's means to stealing your identity.
- Beware of cold callers on the phone or salespeople who knock on your door offering you deals. Never provide your private financial or identification information to anyone, whether online, on the telephone or in person, unless you're totally satisfied they're legitimate.
- Be cautious when providing your personal details online, including credit card details. Always check the bona fides of an online company before making a purchase.
- Protect your identity on social networking sites. Keep your profile private and only become friends with people you know – your personal information and the comments you make provide a profile of yourself that someone can steal.
- Create strong, secure passwords – a mix of letters (upper and lower case), symbols and numbers – and don't share it with anyone. Be careful using public computers and don't save passwords into your web browser.
- Always keep your virus security on your computer up to date.
- Never reply to, click on links or open attachments accompanying email purporting to be from banks. Delete the email and telephone the bank to verify.
- Check your credit report every year. If you find that you have been marked as having unpaid accounts, for example, that you have never heard of, you might have become the victim of an identity theft.
- Keep your credit and debit cards secure and never let them leave your sight when paying for something, for example the bill at a restaurant.



A tipper seized in Sydney during Operation Pulse.

financial services and telecommunications sectors. Another recent innovation is the emergence of facial recognition technology, and the immense potential of biometric face recognition has been acknowledged for years.

Even so, Federal Agent McMillan says the individual citizen is a major player in minimising identity crime. The bottom line is that identity crime can start with stealing real identity details.

The online environment is a growing medium for identity criminals to access unsuspecting individuals. UK research indicates that 86 per cent of all credit card and store card fraud is conducted in an online environment. "The big one," Federal Agent McMillan says, "is never provide any personal identity information to people who don't need access to it – either in person, by phone or online".

He says simple changes in individual behaviour make a big difference to identity security. He adds that as well as investigating identity crime, the ISST has a responsibility to educate the community on how identity criminals use compromised data and obtain personal financial information.

"I think the combination of having education and effective investigation of these matters is the key to keeping the levels of identity crime down. The public also needs to be better educated about identity crime and how vulnerable they may be to criminal attacks."

"False identities can be basically used for any criminal or nefarious activity"

Confiscated materials from Operation Pulse.