Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:27
Received 16 July 2003

Mr Alexander Hackett
Policy Officer
Policy & Coodination
AUSTRAC
PO Box 5516
WEST CHATSWOOD NSW 1515
☎02 9950 0087 🖹02 9950 0073
E-mail:
alexander.hackett@austrac.gov.au

Australian Transaction Reports and Analysis Centre (AUSTRAC)

Submission to the Parliamentary Joint Committee on the Australian Crime Commission

Inquiry into Cybercrime

May 2003

EXECUTIVE SUMMARY

AUSTRAC is both Australia's anti-money laundering regulator and specialist financial intelligence unit. In its regulatory role, AUSTRAC oversights compliance with the reporting requirements of the *Financial Transaction Reports Act 1988* (C'th) by a wide range of financial services providers, the gambling industry and others referred to as *cash dealers*[1]. As a financial intelligence unit, AUSTRAC provides financial intelligence to Commonwealth, State and Territory law enforcement, revenue and national security agencies and some Royal Commissions referred to as AUSTRAC's *partner agencies*[2]

AUSTRAC regularly works with representatives from industry, government and the public on proof of identity and fraud related issues. AUSTRAC chairs the AUSTRAC Proof of Identity Steering Committee, and is a member of the Australian Bankers' Association Fraud Task Force. The Director of AUSTRAC also chairs AGEC, Australia's Action Group into the law enforcement implications of Electronic Commerce.

AUSTRAC considers that the following issues in the area of cybercrime are of pressing concern in terms of potential limitations on the Australian Crime Commission, and other law enforcement and revenue agencies', abilities to combat cybercrime and related offences:

- Proprietary Financial Systems /Internet payment systems
- Overseas based credit cards tax evasion/fraud
- Proof of identity including identity theft and false identity
- New banking products and the globalisation of financial services and capital markets

[1] Cash dealers are defined in section 3 of the FTR Act and include: banks; credit unions; building societies; securities or derivatives dealers; insurance providers; casino operators and remittance dealers.
[2] These agencies are listed in the section 27 of the FTR Act and include; Australian Crime Commission, Australian Federal Police, Australian Securities and Investments Commission, Australian Security Intelligence Organisation, Australian Taxation Office, Australian Customs Service, various State and Territory police services, Anti-Corruption Commission (WA), Crime and Misconduct Commission (QLD), Independent Commission Against Corruption (NSW), the Police Integrity Commission (NSW), various State and Territory Revenue Services, and Royal Commission into WA Police.

BACKGROUND

The Australian Transaction Reports and Analysis Centre (AUSTRAC) is Australia's anti-money laundering regulator and specialist financial intelligence unit. In its regulatory role it is responsible for ensuring compliance with the reporting and account signatory identification requirements of the *Financial Transaction Reports Act 1988* (C'th) (FTR Act) by a wide range of financial service providers, the gambling industry and others, defined as *cash dealers* within the FTR Act. AUSTRAC collects, compiles, and retains the information collected from *cash dealers*. It also issues guidelines and circulars to *cash dealers* and the public required to report various transactions to AUSTRAC, informing them of their obligations under the FTR Act and the *Financial Transaction Reports Regulations 1990* (FTR Regulations). In its intelligence role, AUSTRAC collates and analyses information gathered from the financial transaction reports it has obtained. This intelligence is then provided to the Australian Crime Commission and other Commonwealth, State and Territory law enforcement, revenue and national security agencies and some Royal Commissions, which are collectively referred to by AUSTRAC as its *partner agencies*.

AUSTRAC's mission is to make a valued contribution towards a financial environment hostile to money laundering, terrorist financing, major crime and tax evasion. It does this both domestically and internationally. This is assisted through *cash dealers* identifying their customers to reduce the occurrence of false name bank accounts and to identify individuals using the financial system to finance crime and to launder the proceeds of crime. Through its compilation and analysis functions, AUSTRAC monitors and identifies money laundering related to serious crime and major tax evasion which it refers to its partner agencies.

AUSTRAC provides its partner agencies with both general and specific access to the financial transaction reports information it collects. The general access, governed by memoranda of understanding, is by way of controlled online access to the data and, where appropriate, by extracts of parts of the data holdings. This allows partner agencies to add AUSTRAC's intelligence from financial information to their intelligence holdings, thus assisting both the intelligence and investigative processes. The specific access includes referrals of information initiated by AUSTRAC, or by *cash dealers*, and by other law enforcement agencies, that may assist current investigations or initiate new investigations.

AUSTRAC also watches for money laundering techniques that seek to avoid the formal reporting and identification requirements of the FTR Act. AUSTRAC aims to ensure that the integrity of the system is maintained and that advice is given to Government when further preventative steps, such as amending legislation, may be required. AUSTRAC has powers to take court action for injunctive remedies to secure compliance with the requirements of the FTR Act. Criminal sanctions also apply for non-compliance.

Proprietary Financial Systems/Internet payment systems

The use of proprietary financial systems is of concern as it may permit electronic banking transactions without bank intervention or oversight. These transactions include: international funds transfers, account transfers, 'cheque writing', trading facilities such as Letters of Credit, and securities.

Proprietary financial systems should be distinguished from internet banking, which generally runs off the retail trading system of the bank.

Another area of concern for AUSTRAC is the burgeoning array of alternative payment systems. These are often only available via the internet and provide the possibility of converting funds into a virtual currency, such as e-credits, and disbursing funds overseas without triggering the reporting obligations of the FTR Act. Notable examples of these alternative currencies include Pay PAL and e-gold.

Legislative framework

Proprietary Systems

The existing provisions of the FTR Act do not generally capture any of this type of activity. While the FTR Act does have reporting obligations for international funds transfer instructions[3] under section 17B, users of proprietary financial systems may be able to directly access the proprietary system's global routing system for settlement instructions, creating uncertainty as to whether the instruction is reportable. It is likely that the instruction would be directly registered at the bank's overseas head office which would not normally have a reporting obligation under the FTR Act[4].

Alternative Payment Systems

The FTR Act currently reflects the banking environment of the 1980's and subsequently the definitions in section 3 limit the reportable transactions to those involving currency in its legal tender form and international funds transfer instructions as defined. Many of the providers of alternative electronic payment systems may not fall within the scope of the *cash dealer* definition in the FTR Act and therefore would not have reporting, or other, obligations under the FTR Act, including those for the transmission of international funds transfer instructions.

Overseas accounts and debit/credit cards used in tax evasion/fraud

An increasing area of risk in terms of money laundering and terrorist financing is the use of overseas based accounts and debit or credit cards issued from foreign jurisdictions, especially the use of accounts or credit/debit facilities available, or issued, from tax haven jurisdictions. For example, a person may make all purchases or transmissions of funds by credit card. These credits are processed by credit card providers in overseas jurisdictions, who deduct their fee or commission and forward

[3] International funds transfer instructions are defined in section 3 of the FTR Act as "an instruction for a transfer of funds that is transmitted into or out of Australia electronically or by telegraph,…"

[4] Section 6 provides for extra-territoriality, but it is questionable as to whether it would apply in these circumstances.

the remainder of the funds to a nominated account. The nominated account will be located in a third jurisdiction, possibly a tax haven jurisdiction, and may also have a debit card attached to it.

This account will then be drawn against by the person, effectively being the sole account used by the person for all transactions locally. Such an arrangement may allow the person to make use of funds, which, because they have not been directly transferred into Australia, will not be reported to AUSTRAC, and thus are invisible to AUSTRAC's *partner agencies*.

Legislative framework

Currently the FTR Act will only capture credit card activity if a suspicious transaction report is submitted on this activity to AUSTRAC or there is a local cash deposit or withdrawal on the card of $10,000 or more involving a *cash dealer*.

Proof of identity including identity theft and false identity

Currently, AUSTRAC hosts the Proof of Identity Steering Committee (POISC) which examines ways to improve the integrity of customer identity verification[5]. The POISC seeks to ensure that there is integrity in identification processes, and particularly in the documentation that may be issued by a wide range of government bodies that is now used as part of the process of identification.

AUSTRAC is also a contributor to the Australian Bankers' Association's Fraud Task Force which is addressing the costs of ID fraud and developing appropriate responses to identified threats such as card skimming, identity theft and internet fraud.

Concerns have been raised, both in the media and in other forums, such as parliamentary hearings, as to the effectiveness of Australia's program of identifying, and knowledge of, customers.

At issue is not so much the "100 point" identification system in the FTR Act, but rather the underlying integrity of the documents and checks that are available under the system, including the core identification documents, such as birth certificates, drivers licenses, passports, credit/debit cards etc.

Of particular concern is the number of criminal organisations that have been identified using high technology equipment to produce false identification documents. With the availability of encrypting, embossing and encoding equipment, counterfeit forms of identity can be generated and used in the process of laundering or stealing funds.

Legislative framework

The provisions of the FTR Act require that signatories to an account facility must be adequately identified. By and large, customer verification is completed employing the 100 point check method which is set out in Regulation 4 of the FTR Regulations. This

[5] The POISC includes representation from both industry and government including the Australian Taxation Office, the Department of Immigration Multicultural and Indigenous Affairs, Centrelink, the Australian Bankers Association and representatives from the four major banks.

method includes both the use of documents produced by the customer and verification checks of source materials such as the Electoral Roll, owner or landlord of a rented premises, or a public utility from its records. This is only a minimum requirement and *cash dealers* can use other verification methods such as on-line checks with Roads Authorities for drivers licences and birth registrations with the various offices of Births, Deaths and Marriages.

Other methods of customer verification are available under the FTR Act, including the Acceptable Referee method which relies upon the signatory having their identification documents sighted by a suitable referee, (as gazetted by the Minister for Justice and Customs), and the referee signing a declaration that an appropriate identification document was sighted. Under the FTR Act there is no requirement on the *cash dealer* to authenticate the Acceptable Referee.

New banking products and the globalisation of financial services and capital markets

The trend within the financial services markets has been a movement toward the opening of markets and financial sectors, especially to overseas clientele. The trend is toward a market provision of facilities and services that are enabled by remote access (internet or B-Pay styled telephone account access) and the push is to have customer verifications conducted remotely or even electronically. This has in part been enabled by the growth of internet usage, but also by the general process of globalisation whereby markets have opened up to service providers beyond their immediate jurisdictions and boundaries.

On the other hand, the world-wide trend amongst regulators and policy developers has been towards the tightening of controls, and increased oversight in both regulatory and self-regulatory formats, with particular emphasis in the area of "know your customer" and monitoring customer relationships. This poses a number of challenges for regulators and law enforcement and revenue agencies including Financial Intelligence Units, especially in terms of their legislative powers and the ability to meet increasing technical levels that also have a consequential effect on resourcing of their programs.

Recently, international bodies monitoring money laundering issues, such as the Financial Action Task Force on money laundering (FATF) and the International Monetary Fund (IMF), have also substantially enhanced compliance evaluation methodologies. Additional developments in the anti-money laundering regulatory field include a focus on risk assessment and management strategies as well as ensuring the harmonisation of local legislation with international benchmarks.

Legislative framework

The current provisions of the FTR Act were framed in the financial environment of the time of its drafting. The FTR Act has limited application to many of the electronic and other technological developments that have changed the face of financial services provision in the intervening decade and a half. Despite this, the FTR Act is still a very effective tool to counter money laundering and terrorist financing.

Developments such as remote banking, including phone-banking or internet banking have meant that the style and range of banking/customer interactions have multiplied significantly. It has also meant that the market pressure for new developments has increased. This has, in turn, meant impetus for legislative responses to changes in the market as well as international developments. Such anticipated responses include provision for the electronic verification of applicant customers, and updating domestic legislation in line with international benchmarks.

AUSTRAC has been working in partnership with the Attorney-General's Department to review the FTR Act. Issues such as these are being considered in that review.

Conclusion

AUSTRAC, as a regulator monitors and seeks to ensure compliance with the provisions of the FTR Act. In its role as Australia's specialist financial intelligence unit, AUSTRAC supports anti-money laundering and counter-terrorist financing efforts by compiling, analysing and disseminating financial intelligence to Commonwealth, State and Territory law enforcement, revenue and national security agencies.

AUSTRAC also monitors trends and marketplace developments in order to better advise Government as to which areas or activities pose the greater risks in threatening the integrity of Australia's anti-money laundering regulatory framework.

A number of the methodologies and trends outlined may emanate from the inevitable technological or marketplace developments that have occurred since the inception of the current legislation, while some may constitute explicit money laundering techniques that may result in avoidance of the formal reporting and identification requirements of the FTR Act.

It is essential that Australia's regulatory and law enforcement, revenue and national security programs are adequately supported by appropriate legislation or self-regulatory programs to ensure that there is no diminution of the various law enforcement, revenue and national security agencies' abilities to build accurate and effective intelligence profiles and to ensure that Australia's anti-money laundering/counter-terrorist financing systems are not compromised.

16 July 2003