CUSTOMER OWNED BANKING ASSOCIATION

www.customerownedbanking.asn.au

LEVEL 11, 35 CLARENCE STREET, SYDNEY NSW 2000 GPO BOX 4686, SYDNEY NSW 2001

15 May 2014

Mr Stephen Palethorpe
Committee Secretary
Parliamentary Joint Committee on Law Enforcement
Parliament House
Canberra ACT 2600

Sent via: le.committee@aph.gov.au

Dear Mr Palethorpe

**Inquiry into Financial Related Crime**

Thank you for the opportunity to contribute to the Joint Committee on Law Enforcement inquiry into financial related crime.

The Customer Owned Banking Association (COBA) is the industry association representing Australia's 83 credit unions, 7 mutual building societies and 10 mutual banks. Collectively, our members have assets of $86 billion and serve more than 4 million Australians.

Customer-owned banking institutions exist only to benefit their customers and communities. The sector's singular focus on its customers is demonstrated by market-leading customer satisfaction ratings.

COBA members are committed to responsible and ethical retail banking services that put their customers first. COBA and its members are committed to minimising the impact of financial crime on consumers.

Customer-owned banking institutions operate in an intensively supervised and heavily regulated environment, and in addition to being reporting entities under the *Anti-Money Laundering/Counter-Terrorism Financing Act 2006*, they are:

- Authorised Deposit-taking Institutions regulated by the Australian Prudential Regulation Authority under the *Banking Act 1959*;
- credit providers licensed under the *National Consumer Credit Protection Act 2009*; and
- Australian financial services licensees regulated under the *Corporations Act 2001*.

**Summary & Recommendations**
COBA's position is that:

- the latest anti-money laundering customer due diligence (CDD) reforms adequately support the Australian banking sector's anti-money laundering efforts for the foreseeable time;

- it would be beneficial to increase the capacity, via low cost methods, of the banking industry to verify foreign issued identity credentials such as passports and driver's licences;

- Australia's anti-money laundering tranche 2 reforms that relate to non-financial businesses and professionals should be implemented as soon as practicable;

- support should be increased for initiatives to raise community awareness about cybercrime prevention, particularly for vulnerable older people;

- Australia should continue to actively support international efforts to prevent, disrupt and prosecute financial crimes through a well-resourced AFP; and

- penalties for financial crimes should be reviewed to ensure they continue to be a genuine deterrent and are commensurate with the seriousness of the offence.

**COBA fighting financial crimes**

COBA commits significant resources to combatting financial crime and minimising its impact on our members and their customers. COBA works closely with its member organisations to maintain an extensive network of fraud prevention specialists, and to build strength, capacity and knowledge throughout the sector to respond to financial crime, through:

- strong, authoritative leadership and representation for the sector in the wider fraud prevention community of the Australian finance industry;
- a real-time, secure, member-only network for the dissemination and sharing of fraud intelligence; and
- support to our members to build and constantly improve business-wide fraud risk management strategies.

As part of this commitment, COBA has a dedicated Fraud and Financial Crimes (Financial Crimes) unit to work with members to respond to, and raise awareness of, financial crime. This is done through analysis of financial crime trends, the development of loss mitigation strategies for COBA members and the delivery of ongoing training and professional development for customer-owned banking crime prevention specialists. This unit is solely funded by the customer-owned banking sector, and has been providing specialised fraud and financial crimes advisory services since 2003.

COBA has its own capacity to securely disseminate information and alerts to members, and incident response capabilities to assist member institutions to manage the incidence and economic impact of financial crime. We do this through our own industry tailored secure 'FraudNet' hub that links our sector's fraud prevention network, while maintaining secure links to law enforcement agencies across Australia.

Through the Financial Crimes unit, COBA also maintains a strong working relationship with state and territory police (fraud and cyber-crime units), and the Cyber Crime Operations Division of the Australian Federal Police (AFP).

The joint international crime investigation, Operation Lino, led by the AFP is a notable example of the significant cooperation across law enforcement, COBA and its members, and the broader financial industry. Operation Lino commenced in June 2011 and concluded with seven people being charged in Romania for the largest credit card data theft in Australia's history.[1]

In addition, COBA works in close partnership with the Australian Bankers' Association and Australia's Computer Emergency Response Team. COBA is a founding private sector partner to the Australian High Tech Crime Centre 2003 National Response Plan to Cyber Crime.

[1] http://www.afp.gov.au/media-centre/news/afp/2012/november/seven-arrested-in-australias-largest-credit-card-data-theft-investigation.aspx?source=rss

We continue to participate in a wide range of related industry committees, including the Australasian Card Risk Council, Interbank Fraud Committee and various payment fraud sub committees, under the auspices of the Australian Payments Clearing Association.

**Financial crime – types and impacts**

In a banking industry context, the most common financial related crime involves fraud related to:

- payment types (e.g. cards and cheques);
- home loans and other credit facilities;
- money laundering; and
- technology enabled cyber-crime.

A common enabler of these types of fraud is the criminal misuse of personal identity information. Information contained in *Identity crime and misuse in Australia: Results of the 2013 online survey*[2] indicates that identity theft is now one of Australia's more common crimes.

The survey has found that:

- almost 1 in 10 people experienced misuse of their personal information in the previous 12 months, and 1 in 5 people experienced misuse of their personal information at some point in their lives;
- 5 per cent of people experienced identity crime or misuse resulting in a financial loss in the previous 12 months;
- identity crime directly affects around 1 million Australians each year;
- almost 1 in 10 victims did not report the incident; and
- victims experienced other significant impacts such as:
    - refusal of credit (14.1 per cent);
    - mental or emotional stress requiring counselling or other treatment (10.7 per cent); and
    - being wrongly accused of a crime (5.5 per cent). [3]

COBA members are taking active measures to combat identity fraud. Access to the Commonwealth Document Verification Service (DVS) is helping our members to meet their regulatory obligations to verify customer identities under the *Anti-Money Laundering/Counter-Terrorism Financing Act 2006* and the Anti-Money Laundering/Counter-Terrorism Financing Rules 2007.

The DVS is a national online system that allows regulated entities to compare a customer's identifying information with a government record. The DVS 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 allows businesses to verify information on a range of government issued identity credentials such as driver's licences, passports, visas and Medicare cards.

<u>Card and cheque fraud</u>

In terms of payment fraud, the latest statistics from the Australian Payments Clearing Association, for the period 1 July 2012 to 30 June 2013, reveal:

- 770 fraud transactions related to cheques, valued at almost $9.8 million; and
- more than 1.3 million fraud transactions related to Australian issued proprietary debit cards, and scheme, debit and charge cards, valued at more than $280.5 million.[4]

While the number of fraud transactions is disturbing, consumer protection safeguards are working effectively when comparing the rate of fraud to the total numbers of transactions, as illustrated in the table below.[5]

---

[2] http://aic.gov.au/publications/current%20series/rpp/121-140/rpp128.html
[3] http://www.attorneygeneral.gov.au/Mediareleases/Pages/2014/SecondQuarter/5May2013Identitycrimenowamongstmostcommoncrimesin Australia.aspx
[4] http://apca.com.au/docs/fraud-statistics/payment-fraud-statistics-financial-year-2013.pdf

| | Fraud Rates | |
|---|---|---|
| | As a % of total number of transactions | As a % of total value ($) of transactions |
| Cheques | 0.0004% | 0.0008% |
| Australian-issued cards | 0.0234% | 0.0461% |
| **Total** | **0.0226%** | **0.0161%** |

The rate of card fraud remains an ongoing concern however the Australian banking sector has robust measures in place to protect consumers from losses arising from unauthorised transactions.

The ePayments Code plays an important role in the regulation of electronic payment facilities in Australia. It is administered by the Australian Securities and Investments Commission, and has regulated consumer electronic payment transactions, including ATM, EFTPOS and credit card transactions, online payments, internet and mobile banking, and BPAY since 1986.

The Code complements other regulatory requirements, including financial services and consumer credit licensing, advice, training and disclosure obligations under the *Corporations Act 2001* and the *National Consumer Credit Protection Act 2009*. Among other things, the ePayments Code sets out the rules for determining who pays for unauthorised transactions, and establishes a regime for recovering mistaken internet payments.

Money laundering and cyber-crime

The Australian Crime Commission has suggested that that the level of this type of crime in and through Australia is at least $10 billion annually. [6] The Commission also notes the "full cost of money laundering to the Australian community is likely to be much higher when lost tax revenues and the full scope of unreported proceeds of crime is taken into account."[7]

The banking sector is actively working to minimise and disrupt money laundering activities. Under the *Anti-Money Laundering/Counter-Terrorism Financing Act 2006*, the banking sector has extensive and ongoing CDD and reporting obligations.

The Australian Transaction Reports and Analysis Centre (AUSTRAC) is finalising further enhancements to CDD obligations that will apply from 1 June 2014 and target complex business customers. These reforms will better align Australia's CDD rules with international Financial Action Task Force (FATF) standards by requiring, amongst other things, an AUSTRAC reporting entity to:

- understand who owns and controls the customer, including the beneficial ownership and control structures;
- understand the purpose and intended business relationship of the customer; and
- conduct ongoing due diligence of the business relationship, including scrutiny of the transactions involving that customer.

The latest CDD reforms adequately support the Australian banking sector's anti-money laundering efforts for the foreseeable time. It is however important to note that the international FATF standards require non-financial businesses and professionals such as lawyers, accountants and real estate agents to be regulated under the Australia's anti-money laundering regime. Australia's anti-money laundering tranche 2 reforms that relate to non-financial businesses and professionals should be implemented as soon as practicable.

---

[5] *Ibid*
[6] https://www.crimecommission.gov.au/publications/intelligence-products/crime-profile-fact-sheets/money-laundering
[7] *Ibid*

To further reduce opportunities for foreign based criminal syndicates to operate in Australia, the banking industry needs greater capacity to verify foreign issued identity credentials such as passports and driver licences.

Cyber-crime

In its report *Organised Crime in Australia 2013*, the Australian Crime Commission noted that "the overall cost of cyber and major technology-enabled crime to the Australian economy is estimated to be US$1.7 billion per year, with major cyber intrusions costing organisations an average of US$2 million per incident."[8]

In its *Targeting scams: Report of the ACCC on scam activity 2012*, the Australian Competition and Consumer Commission (ACCC) noted it had received over 83,000 scam-related contacts and inquiries from consumers and small businesses.[9] The estimated losses reported to the ACCC were more than $93 million. This represents a nine per cent increase from 2011.

The report also noted:

- advance fee/up-front payment scams were the most commonly reported scam type;
- computer hacking remained the second most reported scam type in 2012, at just over 13 per cent of the total scam reports to the ACCC;
- online shopping scams increased by 65 per cent with reported losses exceeding $4 million; and
- a high level of inquiries from the public and small businesses about banking and online account scams.

Cyber-crime is a problem that is affecting a growing number of Australians. According to the Queensland Police Service, Australians are losing more than $190,000 per day in internet dating scams. Average individual losses from online dating scams have been estimated as high as $28,000.

As the population ages, it is anticipated that older Australians will be increasingly targeted by cyber criminals because of their:

- significant superannuation savings, or need to supplement modest incomes;
- increasing online participation;
- increasing use of social networking and dating web sites; and
- lower understanding of personal security as new entrants to the online world.

The customer-owned banking sector continues to work cooperatively on a range of initiatives to disrupt such criminal activities, including:

- COBA-led fraud symposiums to train fraud prevention specialists in emerging risks and latest prevention strategies;
- ongoing support of *Cybercrime Security Awareness Week;*
- reporting all types of fraud to the ACCC SCAMwatch website;
- promoting the Government's StaySmartOnline website as a source of information to enable people to protect their personal and financial information online; and
- engaging in targeted campaigns facilitated by our active partnerships with Government.

COBA members also conduct various regional security seminars, in conjunction with police, to educate their customers about internet safeguards and the threats and risks posed by cybercrimes.

**Financial crime enforcement, sentencing and awareness**

Financial crime is increasingly conducted by organised crime syndicates based in foreign jurisdictions, as illustrated by Operation Lino referred to earlier in this submission.

[8] https://www.crimecommission.gov.au/sites/default/files/ACC%20OCA%202013-1.pdf
[9] http://www.accc.gov.au/system/files/Targeting%20scams%202012.pdf

In the case of Operation Lino, a foreign criminal syndicate used some 30,000 Australian credit cards to make unauthorised transactions of more than $30 million. AFP Manager for Cyber Crime Operations, Commander Glenn McEwen noted that "without the cooperation of 13 other countries, along with Australia's banking and finance sector, we would not have been able to track these illegal transactions to the criminal network in Romania."[10]

Financial crimes have profound negative impacts on individuals and families, and represent an ongoing risk to businesses across Australia. However, law enforcement, and the subsequent prosecution of criminal syndicates, is made more difficult given the increasingly international nature of financial crime.

Ongoing cooperation between Australia's law enforcement agencies and their foreign counterparts is critically important. Notwithstanding that Australia's legislative and penalty framework is not applicable to cases tried in overseas jurisdictions, Australian enforcement agencies should continue to support international efforts to target criminal enterprises. Australia should continue to support international efforts to prevent, disrupt and prosecute financial crimes through a well-resourced AFP. To this end, the AFP should have the capacity to develop and maintain cooperative relationships with foreign enforcement agencies to respond to emerging criminal activities.

COBA believes Commonwealth legislation and administrative arrangements are adequate in their current form, and do not require further reform. Penalties for financial crimes should be reviewed to ensure they continue to be a genuine deterrent and are commensurate with the seriousness of the offence.

Yours sincerely

**Luke Lawler**
**Senior Manager, Public Affairs**

[10] http://www.afp.gov.au/media-centre/news/afp/2012/november/seven-arrested-in-australias-largest-credit-card-data-theft-investigation.aspx?source=rss