AUSTRALIAN BANKERS' ASSOCIATION INC.

Paul Stacey
Tax & Security Manager

AUSTRALIAN BANKERS' ASSOCIATION INC.
Level 3, 56 Pitt Street, Sydney NSW 2000
p. +61 (0)2 8298 0416 **f.** +61 (0)2 8298 0402

www.bankers.asn.au

9 May 2014

Committee Secretary
Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
CANBERRA ACT 2600

Email: le.committee@aph.gov.au

Dear Committee Secretary,

Inquiry into financial related crime

The Australian Bankers' Association (**ABA**) appreciates the opportunity to provide the Parliamentary Joint Committee on Law Enforcement with its submission to the "Inquiry into financial related crime" **(Inquiry**).

The ABA is the peak national body representing banks that are authorised by the Australian Prudential Regulation Authority to carry on banking business in Australia. The ABA's membership of 24 banks comprises the four major banks, former regional banks that now operate nationally, foreign banks that are represented and carry on banking business in Australia as Australian banks and a mutual bank.

The ABA's submission relates only to paragraphs (a), (b), (c) and (e) of the Inquiry Terms of Reference.

(a) The character, prevalence and impact of financial related crime in Australia

In the past five or so years criminal activity relating to the financial services industry (**FSI**) has seen a significant reduction in assaults and robberies and an increasing incidence of the use of technology to commit crime. The crime as such has moved from a person to person involvement to a distant, technology to technology process involving/allowing;

- the conduct of currency and money laundering;
- the conduct of fraud against customers and others;
- organised crime groups conducting crime (not just fraud) against customers or other people and organisations through on-line technology, products and services;
- individuals and organisations to conduct "hacktivism" using FSI as a conduit;
- criminals to use on-line FSI channels to commit crime; and

- the emerging use of Money Service Business (MSB) and digital currencies through non-financial institutions.

Other points for consideration:

- the attractiveness of Australia to crime due to the strong economy;
- the movement from opportunistic crime to well organised crime;
- the impact of the cost of crime to major banks and the economy - regulatory, customer impact, community, business expenses, etc;
- the Australian Crime Commission (ACC) estimates that serious and organised crime costs Australia $15B every year;
- the formation of innovative crime groups;
- leveraging new products, faster payments, customer self-service, competitiveness vs. the increase of financial crime to the bank/industry (i.e. customer convenience vs. increased exposure to fraud); and
- in the past the above frauds were "paper based" and had to involve (at some point) interaction with a person. This had many inherent limitations as a crime and posed higher risk to the criminal, but that has all changed.

The use of technology to interact with people everywhere and at all times has been embraced across the world leading to a change in the way business is conducted. Unfortunately, the early adopters of this technology change have been criminal groups and individuals who are largely able to hide or takeover identities and use the geographical constraints of the criminal justice system.

A commonality among these types of crimes is that the offender, to a great degree, depends upon the lack of technological skills and agility of law enforcement and the FSI to successfully commit the offenses and escape undetected. Generally the criminals feel some confidence in their chances to evade detection of their crimes.

These criminal activities are conducted across the legal and political borders between states, and transgress legal, cultural, religious and organisational boundaries among and within states primarily using the links between financial service organisations. This now has seen a shift globally where criminals cross-border their offences, therefore crossing jurisdictions.

In our view, the FSI is often the first responder to criminal activity by default (as the conduit for this type of crime) and are looked to by the customer, the counterparty and law enforcement for prevention, monitoring, detection and response to crime. The Government also looks to the FSI as a major player in managing financial crime by enacting legislation that requires FSIs to conduct their activities (including the imposition of reporting obligations) in accordance with the provisions of various laws without any monetary or asset support.

In light of the above, the amount of money that is involved in "attempts" and "actual" payments card fraud and related crime on ABA member organisations has risen from:

- 2008 = 419,417 incidents worth $150.7 million, to
- 2013 = 1,373,025 incidents worth $280.5 million.

It should be noted that much of the above crime (such as credit card fraud) does not get reported to the law enforcement authorities and does not form part of the statistical information concerning crime.

To support the above position that crime has morphed from personal to technological, for the same period armed robbery has gone from:

- 2008 = 41 incidents, to
- 2013 = 39 incidents

To further highlight this change, armed robberies 15 years ago on the same institutions were:

- 1998 = 326 incidents

The number of Suspicious Transactions Reports reported by the members of the ABA has gone from:

- 2005 = 29,089, to
- 2013 = 44,062

(b) The methods and practices used by the perpetrators of financial related crime (including the impact of new technologies)

Other considerations:

- Commercialisation of fraud and how fraud tools are marketed and the threat of superannuation being a crime target.
- Australia's internet user base is large and growing. This was estimated by the ABS in December 2013 at 12.4 million subscribers.
- Increase in the "informal banking sector" with the use of alternate remitters e.g. MSB etc.
- Digital currency.

The use of computers and being universally connected has changed the methodology of crime in the financial sector. In the FSI the computer is:

1) the target of the crime;

2) is the instrument of the crime; and

3) is supplementary to the crime[1]

The introduction of smart cards (payWave), store cards, gift cards and similar devices have added to the definition of "computer" and added to the complexity of preventing, detecting and responding to financial crime,[2] including the new payments platform (real time payments) which will have the most significant impact. In addition, financial institutions are striving to continually improve the customer experience with banking that is easy to us, convenient and competitive. These changes have the potential to impact on the safeguards from financial crime.

According to the Australian Institute of Criminology, these may be broken down to:

1) Syntactic attacks

- Exploitation of technical vulnerabilities to commit fraud (e.g. malware, plastic card skimming, illegal funds transfers, Wi-Fi).

2) Semantic attacks

- Exploitation of social vulnerabilities to gain personal information (e.g. scam solicitations, identity-related fraud, auction fraud).

3) Blended attacks

- Attacks using technical tools to facilitate social engineering e.g. Phishing;
- Using an unsolicited request to visit a counterfeit website in an attempt to trick users into disclosing personal banking information[3].

The increased interconnectivity of information exchange systems mean that financial transactions affecting people in Australia are not necessarily physically or identifiably located within this country. Information and money are increasingly being accessed and moved by individuals and enterprises through the use of various communication networks that transcend national boundaries.[4]

At the same time, business has moved to the use of the same assets, the computer and international connectivity, to conduct and extend traditional businesses and create new goods and services.

Generally the types of crimes that are being committed are around:

- stealing customer identity;
- false web-sites;

---

1 Carter, D.L., and A.J. Katz, "Computer Crime: An Emerging Challenge for Law Enforcement," FBI Law Enforcement Bulletin, 1996 in www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf. 2014.

2 CHIP technology is far more secure than magstripe technology and payWave transactions, which authenticate the card, and prohibit counterfeit transactions. All payWave are soon to be full online transactions authorised by host system, so should not be negatively affected in terms of detection.

3 http://www.aic.gov.au/media_library/conferences/other/smith_russell/2012-12-cdpp.pdf 24/4/2014

4 http://www.afp.gov.au/media-centre/publications/platypus/previous-editions/1998/september-1998/blazing.aspx 24/4/2014 - Blazing new trails in fighting financial crime

- falsely pretending to be a customer through fake identity (identity theft);
- intercepting or hacking emails – then through social engineering falsely pretending to be a customer;
- intercepting or stealing snail mail;
- opening accounts using false identities;
- money laundering or structuring (using innocent agents or not);
- internet scams that pray on the desires of financially (or romantically) desperate individuals;
- certain computer viruses may also be used to harvest personal information for identity theft crimes; and
- extortion to "unlock" information or to publish information that may include internet search "history".

The Internet has also generated a whole new range of payment systems and methodologies, the most common so far being the credit card which can be compromised through various means. There has also been an increase in the use of mobile devices. The Australian Bureau of Statistics estimated at December 2013 that there were 20.3 million mobile handset internet subscribers.

The systems also allow customers to move funds between their own accounts and issue instructions to make third-party payments. Criminals have now intercepted, or used false presences, and changed these instructions for their own benefit, also using third parties (such as Western Union) to transfer funds anywhere in the world.

The use of digital currency, previously used for on-line games has now broken into the mainstream with Bitcoin leading the way with Bitcoin ATM's and other mergers with traditional monetary systems. Even the US Inland[5] Revenue Service has recognised Bitcoin and law enforcement has confiscated this currency as part of their confiscations of crime program.

(c) The involvement of organised crime

Anecdotally the ABA's Financial Crimes Steering Group has seen a dramatic growth of organised crime using technology to conduct crime using the FSI. Financial crime is an industry and will continue to be in the future.

According to the AFP, organised crime groups, in Italy, Japan, Colombia, Russia and Eastern Europe, Nigeria and the Far East, and outlaw motorcycle gangs continue to be responsible for a large proportion of the crime and "dirty" money flowing through financial channels. We concur with the views of the AFP as set out in an old report:

> *"In addition to drug trafficking, these enterprises generate funds from loan sharking, illegal gambling, fraud, embezzlement, extortion, prostitution, corruption, illegal trafficking in armaments, human beings and organ parts, organised motor vehicle theft and many other offences. In some*

[5] Tyler Durden on 10/26/2013 09:19 -0400 the FBI arrested Ross William Ulbricht - the creator of the marketplace Silk Road also known as Dread Pirate Roberts, some were surprised that the Feds only confiscated about $3.6 million worth in Bitcoins from Ulbrecht. http://www.zerohedge.com/news/2013-10-26/feds-confiscate-record-29-million-bitcoin-booty-dread-pirates-hard-drive 2014

> *countries, criminals who had been previously solely engaged in drug trafficking have been either broadening their activities to take part in a wider range of criminality, or have switched to fraud."* [6]

Although this report is some years old, it reflects the current state of play and criminals are increasingly using the FSI to commit crimes, launder and profit from their criminal activity.

Our understanding through our own experience and from briefings with law enforcement, is that these overseas gangs have links to Australian organised crime and are attracted here as the activity, even if caught, attracts lower penalties than that of other jurisdictions.

Data compromises are also an increasing risk for the FSI. The reputational risk of compromises may be higher than the actual money lost.

In many of the data compromises that have occurred across the globe, one criminal group may pay for information that has been stolen, or under old criminal terms "fence the stolen information", but on other occasions, knowing that a resolution to the data breach is only a matter of time, will share part of the information knowing that they will have a limited amount of time to make a monetary gain from the information and only so much can be done during that time.[7]

The USA retailer, Target, had a data breach from an international organised gang (yet to be identified) around Christmas of 2013. Credit card details of 40 million customers were stolen from the system within a three week period when it was vulnerable. It was reported in the Wall Street Journal that there was $2 million in fraud on the Visa V (Target) credit cards it issues and none on Target's store-issued debit cards. The article goes on to say:

> *"Ellen Richey, chief legal officer at Visa Inc., said the percentage of cards stolen during the Target breach that have been used for fraud is much lower than the 2% to 5% rate that the card issuer normally sees in such circumstances due to the relatively quick notification of the breach.*[8]

It does seem that in this case fraud may not have been the primary motivation, and the monetary loss from the crime, some $2M, not an extreme loss. Yet the on-costs of replacement cards, reputation costs of informing the market and customers and supporting law enforcement have been significant.[9]

This area of malicious cybercrime is an increasing risk in the FSI where there are specific groups in play to develop the cybercrime and those who deliver or commit the crime. This involves targeted co-operation cross border to support crime in the FSI and the outsourcing to money-laundering professionals.

---

6 www.afp.gov.au/media-centre/publications/platypus/previous-editions/1998/september-1998/blazing.aspx 24/4/2014 - Blazing new trails in fighting financial crime

7 Target suffered one of the largest credit-card thefts in corporate history in the weeks leading up to Christmas 2013, when hackers stole data on 40 million credit- and debit-card accounts.

8 http://online.wsj.com/news/articles/SB10001424052702304688104579464091428141708 2014.

9 Target has acknowledged it failed to react to early signs that hackers had gotten into its computer systems. Mr Mulligan said… "We need to continue to invest and make it better. That's the challenge for us."[9] http://online.wsj.com/news/articles/SB10001424052702304688104579464091428141708 2014.

(e) In relation to identity fraud—credit card fraud in particular

Identity fraud continues to occur through various channels such as using a phishing email to obtain customer banking details (electronic fraud) to then apply for a credit card application.

Credit card fraud methodology includes, but is not limited to:

- stealing cards and making purchases by forging signatures;
- using credit card details to pay for goods or services over the phone or internet (card not present);
- tricking people into revealing access codes for accounts and then making internet or telephone purchases;
- capturing credit card details and PIN number with hidden devices during an ATM or EFTPOS transaction (ATM credit card skimming); and
- skimming credit cards at point of sale, resulting in a clone card being made and used by a fraudster.

All of the above methods of credit card fraud involve the fraudulent use of another's identity. This fraud has rapidly increased as the use of technology to make payments has been universally adopted and also due to the involvement of organised crime The industry invests a significant amount in fraud detection and prevention technology i.e. CHIP cards coupled with PIN mandate, advanced data analysis tools, real time decline solutions and PCI DSS.

Whilst identity fraud relating to credit cards is an issue, a potentially more serious and worrying problem is emerging. With the increased utilisation by security teams of data analytics, Australian financial institutions are increasingly detecting potential identity fraud, particularly amongst non-Australian resident customers, specifically the use of what appears to be false passports in the customer on boarding (Know Your Customer) process.

Unlike the Attorney-General's Document Verification Service, there is no mechanism for Australian banks to verify that a passport which looks genuine is actually legitimate, or that it has actually been used to legally enter Australia (helping reinforce one identity per person). Numerous instances have been identified where accounts have been opened by foreign customers (e.g. tourists, students, working holiday visa holders) using a passport which appears genuine, but which returns an invalid result when checked with the issuing authority overseas. In these cases, it is not unusual for accounts to be used for money laundering purposes, or to be used to perpetrate fraud against the parent (or another) financial institution. The current reliance on attempting to manually verify individual identity documents with the issuer is sometimes feasible for one-off cases (depending on the issuing jurisdiction), but it becomes unworkable as volumes increase.

Ideally, a mechanism would be developed to enable Australian banks to validate foreign customer identity documents as legitimate, either at the source through the host country, Interpol, or as a fall-back against Australian Customs and Immigration Passenger Movements. Early identification of false or suspicious identities, combined with an agreed reporting mechanism (e.g. AUSTRAC, AFP) would

enable early intervention by law enforcement as well as potentially disrupt organised financial crime and money laundering activity.

Yours sincerely,

_____

Paul Stacey