Uniting Church in Australia
SYNOD OF VICTORIA AND TASMANIA

Justice and International Mission Unit
130 Little Collins Street
Melbourne Victoria 3000
Telephone: (03) 9251 5271
Facsimile: (03) 9251 5241
jim@victas.uca.org.au

31 January 2017

Financial Crime Section
Transnational Crime Branch
Criminal Justice Policy and Programme Division
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600
E-mail: antimoneylaundering@ag.gov.au

Submission of the Synod of Victoria and Tasmania, Uniting Church in Australia to the Consultation Paper 'Trust and company service providers: a model for regulation under Australia's anti-money laundering and counter-terrorism financing regime'

The Synod of Victoria and Tasmania, Uniting Church in Australia, welcomes the opportunity to make a submission to the consultation paper on *Trust and company service providers: a model for regulation under Australia's anti-money laundering and counter-terrorism financing regime.* The Synod supports the inclusion of trust and company service providers under the AML/CTF Act due to the very real harms money laundering does by allowing criminals to profit from the harms they cause. The Synod has had a particular focus on the impact of money stolen from developing countries being laundered through Australia. By addressing this issue, the Australia Government offers one less place for organised criminals and corrupt businessmen and government officials to shift stolen funds to. Australia is an attractive location for criminals to shift money to if they can do so, as we have a stable financial system meaning the laundered money will be secure for the criminals to benefit from.

The meeting of approximately 400 Synod representatives from congregations across Victoria and Tasmania in 2014 passed a resolution which included bringing company service providers under the AML/CTF Act:

> *14.7.19.3. The Synod resolved:*
> *(a) To continue its support for action by the Commonwealth Government to combat corruption,*
> *both in Australia and internationally; and*
> *(b) To request the Commonwealth Government:*
> *(iii) To extend Australia's anti-money laundering/counter-terrorism financing laws to cover designated non-financial businesses and professions named in the Financial Action Task Force international standards, and specifically to real estate agents in relation to the buying and selling of property, dealers in precious metals and stones, lawyers, accountants, notaries and company service providers;*
> *(c) To write to the Prime Minister, the Attorney General, the Leader of the Opposition and the Shadow Attorney General to inform them of this resolution.*

The World Bank and UN Office on Drugs and Crime (UNODC) have previously conducted research showing how shell companies with concealed ownership are used to facilitate a

range of criminal activity. They published a report reviewing some 150 cases of corruption where the money from laundered. In the majority of cases:[1]

- A corporate vehicle (usually a shell company) was misused to hide the money trail;
- The corporate vehicle in question was a company or corporation;
- The proceeds and instruments of corruption consisted of funds in a bank account; and
- In cases where the ownership information was available, the corporate vehicle in question was established or managed by a professional intermediary to conceal the real ownership.

In two-thirds of the cases some form of surrogate, in ownership or management, was used to increase the opacity of the arrangement.[2] In half the cases where a company was used to hide the proceeds of corruption, the company was a shell company.[3] One in seven of the companies misused were operational companies, that is 'front companies'.[4]

The FATF reported that the majority of legal persons in Australia are registered with ASIC and the Australian Business Register while others with State or Territory authorities.[5] While the information seems to be largely available to competent authorities and to the public, very limited verification is conducted on the registration information. Hence, there is no certainty that information maintained on legal persons is accurate or up-to date.

ASIC advise that 80 to 95% of the companies registered are registered online by a third party which are lawyers or accountants, with a large majority registered by trust and company service providers (TCSPs) specialising in company registration as well as trusts and self-managed funds.[6]

FATF noted the limited verification conducted on the registration information of company and trust legal persons and arrangements, raising concerns as to the veracity and accuracy of the information recorded in ASIC registers and potential misuse of companies for ML/TF purposes.[7]

The consultation paper correctly outlines the strong reasons why TCSPs should be subjected to AML/CTF obligations (page 6):

> *The regulation of TCPs under the AML/CTF regime would contribute to enhancing and systematising their awareness of ML/TF risks and aid these professionals in better understanding the identity of their clients, the source of the funds underpinning transactions and the nature of the transaction being handled. An obligation to conduct customer due diligence (CDD) would assist these professionals to identify 'red flags' that may be early indicators of criminality or potential misconduct, and reduce their exposure to criminal liability. Red flags can relate to the client, the source of the client's funds and the choice of TCSP….*
>
> *If a TCSP is subject to AML/CTF regulation, has an awareness of the ML/TF risks facing their business and is conducting robust CDD, they increase the likelihood of identifying these indicators and enable a proper assessment of the extent to which*

[1] Emile van der Does de Willebois, Emily M Halter, Robert A Harrison, Ji Won Park and J. C. Sharman, 'The Puppet Masters', The World Bank, 2011, p. 2.
[2] Emile van der Does de Willebois, Emily M Halter, Robert A Harrison, Ji Won Park and J. C. Sharman, 'The Puppet Masters', The World Bank, 2011, p. 58.
[3] Emile van der Does de Willebois, Emily M Halter, Robert A Harrison, Ji Won Park and J. C. Sharman, 'The Puppet Masters', The World Bank, 2011, p. 34.
[4] Emile van der Does de Willebois, Emily M Halter, Robert A Harrison, Ji Won Park and J. C. Sharman, 'The Puppet Masters', The World Bank, 2011, p. 39.
[5] FATF, 'AML and CTF measures Australia Mutual Evaluation Report', April 2015, p. 105.
[6] FATF, 'AML and CTF measures Australia Mutual Evaluation Report', April 2015, p. 110.
[7] FATF, 'AML and CTF measures Australia Mutual Evaluation Report', April 2015, p. 105.

the client exposes them to ML/TF risks. The TCSP would also be well positioned to identify the report suspicions about specific customers or transactions earlier in the transaction chain, thereby activating the protections of the AML/CTF Act and providing 'early warnings' to detect and deter criminal activities. More robust CDD requirements for TCSPs, in particular, would enhance Australia's visibility and transparency of beneficial ownership of trust accounts and company structures that TCSPs often establish or initiate on behalf of their clients.

1. What services provided by TCSPs pose a ML/TF risk?

AUSTRAC has stated that in Australia "organised crime groups are increasingly using networks of businesses, companies, partnerships and trusts to support criminal activity and launder illicit funds."[8] Project Wickenby uncovered significant use of professional advisers to form trusts and complex corporate and financial structures for large-scale tax fraud and money laundering.

The FATF found evidence in Australia that particular services were vulnerable to misuse for the purpose of ML/TF which include:[9]

- creation of trusts and companies;
- management of trusts and companies; and
- setting up and managing charities.

Research by Findley, Nielson and Sharman also found Australian corporate service providers were near the top of corporate service providers in terms of being willing to set up an untraceable shell company even when there was significant risk the company in question would be used for illicit purposes.[10]

The ATO had publicly stated "Over a hundred Australians have already been identified involving tens of millions of dollars in suspected tax evasion through the use of 'shell companies' and 'trusts' around the world." In October 2013, the Australian Federal Police charged three men with tax and money laundering offences involving $30 million. It is alleged they used a complicated network of offshore companies to conduct business in Australia while hiding the profits offshore, untaxed. The profits were then transferred back to Australian companies controlled by the offenders and disguised as loans so the interest could be claimed as a tax deduction. The level of alleged criminal benefit was estimated at $4.9 million.

As an example of a case where shell companies with concealed ownership were allegedly used to facilitate money laundering through Australia, US authorities sought to seize the assets in three Westpac accounts held by Technocash Ltd holding up to $36.9 million.[11] Technocash Limited was an Australian registered company. The funds are alleged to be connected to shell companies owned by the defendants in the case.[12] It is unclear if Westpac had detected the connection between Technocash and key figures in Liberty Reserve and their alleged criminal activities, particularly money laundering. According to the case filled by the US Attorney for the Southern District of New York, Liberty Reserve SA operated one of the world's most widely used digital currencies. Through its website, the

[8] AUSTRAC, 'Money laundering in Australia 2011', 2011, p. 28.
[9] FATF, 'Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals', June 2013, p. 83.
[10] Michael Findley, Daniel Nielson and Jason Sharman, 'Global Shell Games: Testing Money Launderers' and Terrorist Financiers' Access to Shell Companies', Centre for Governance and Public Policy, Griffith University, 2012, p. 21.
[11] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 29, 43.
[12] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 21.

Costa Rican company provided its with what it described as "instant, real-time currency for international commerce", which could be used to "send and receive payments from anyone, anywhere on the globe". The US authorities allege that people behind Liberty Reserve:[13]

> *…intentionally created, structured, and operated Liberty Reserve as a criminal business venture, one designed to help criminals conduct illegal transactions and launder the proceeds of their crimes. Liberty Reserve was designed to attract and maintain a customer base of criminals by, among other things, enabling users to conduct anonymous and untraceable financial transactions.*
>
> *Liberty Reserve emerged as one of the principal means by which cyber-criminals around the world distributed, stored and laundered the proceeds of their illegal activity. Indeed, Liberty Reserve became a financial hub of the cyber-crime world, facilitating a broad range of online criminal activity, including credit card fraud, identity theft, investment fraud, computer hacking, child pornography, and narcotics trafficking. Virtually all of Liberty Reserve's business derived from suspected criminal activity.*
>
> *The scope of Liberty Reserve's criminal operations was staggering. Estimated to have had more than one million users worldwide, with more than 200,000 users in the United States, Liberty Reserve processed more than 12 million financial transactions annually, with a combined value of more than $1.4 billion. Overall, from 2006 to May 2013, Liberty Reserve processed an estimated 55 million separate financial transactions and is believed to have laundered more than $6 billion in criminal proceeds.*

It was further alleged by US authorities that for an additional "privacy fee" of 75 cents per transaction, a user could hide their own Liberty Reserve account number when transferring funds, effectively making the transfer completely untraceable, even within Liberty Reserve's already opaque system.[14]

US authorities alleged defendant Arthur Budovsky used Technocash to receive funds from exchangers. Mr Budovsky, the alleged principal founder of Liberty Reserve,[15] allegedly used his bank to wire funds to Technocash bank accounts held by Westpac.[16] He is also alleged to be the registered agent for Webdata Inc which held an account with SunTrust. Technocash records allegedly showed deposits into the SunTrust account from Technocash accounts associated with Liberty Reserve between April 2010 and November 2012 of more than $300,000.[17]

Arthur Budovsky is allegedly listed as the president for Worldwide E-commerce Business Sociedad Anonima (WEBSA) and defendant Maxim Chukharev as the secretary. Maxim Chukharev is alleged to have helped design and maintain Liberty Reserve's technological infrastructure.[18] WEBSA allegedly served to provide information technology support services to Liberty Reserve and to serve as a vehicle for distributing Liberty Reserve profits to Liberty Reserve principals and employees.[19] It is alleged bank records showed that from July 2010

[13] US Attorney for the Southern District of New York, 13 Civ 3565, 28 May 2013, pp. 4-5.
[14] US Attorney for the Southern District of New York, 13 Civ 3565, 28 May 2013, p. 6.
[15] US Department of Justice, 'One of the World's Largest Digital Currency Companies and Seven of Its Principals and Employees Charged in Manhattan Federal Court and Running Alleged $6 Billion Money Laundering Scheme', 28 May 2013.
[16] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 29.
[17] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.
[18] US Department of Justice, 'One of the World's Largest Digital Currency Companies and Seven of Its Principals and Employees Charged in Manhattan Federal Court and Running Alleged $6 Billion Money Laundering Scheme', 28 May 2013.
[19] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 37.

to January 2013, the WEBSA account in Costa Rica received more than $590,000 from accounts at Technocash associated with Liberty Reserve.[20]

It is alleged Arthur Budovsky was the president of Grupo Lulu Limitada which was allegedly used to transfer and disguise Liberty Reserve Funds.[21] Records from Technocash allegedly indicate that from August 2011 to November 2011 a Costa Rican bank account held by Grupo Lulu received more than $83,000 from accounts at Technocash associated with Liberty Reserve.[22]

Further, defendant Azzeddine El Amine, manager of Liberty Reserve's financial accounts,[23] was the Technocash account holder for Swiftexchanger. It is alleged e-mails showed that exchangers wishing to purchase Liberty Reserve currency wired funds to Swiftexchanger. When Swiftexchanger received funds in its Technocash account, an e-mail alert was sent to El Amine, notifying him of the transfer. Based on these alerts, it is alleged between 12 June 2012 and 1 May 2013, exchangers doing business with Liberty Reserve send approximately $36,919,884 to accounts held by Technocash at Westpac.[24]

The defendants are alleged to have used Technocash services to transfer funds to nine Liberty Reserve controlled accounts in Cyprus.[25]

Technocash Limited was reported to have been forced out of business in Australia following the action by US authorities, when it was denied the ability to establish accounts in Australia by financial institutions.[26] Technocash stated that it "complied with Australia's comprehensive AML regime, verified customers and has an AFSL licence since 2003. Technocash denied any wrong doing."[27]

Another example of where a company service provider appears to have failed to carry out appropriate due diligence is that of Danial Kalaja. Unemployed Daniel Kalaja, with a history of drug offences was found to be the leader of a Australian drug network empire subsequent known to the law enforcement operation -'Warrior'. Kalaja pleaded guilty in 2013 to numerous serious criminal offences including trafficking in dangerous drugs and received a 14-year prison sentence.

In 2014 Kalaja forfeited $3.188 million in assets to the State of Queensland subject to a six year investigation. Court documents reveal the extent that Kalaja went to legitimise his drug wealth using property development.

Kalaja registered an Australian proprietary company in December 2003 called 'GDK Developments Pty Ltd' (GDK) with Kalaja as sole shareholder and his uncle as director. In March 2004 GDK purchased a $385,000 development land block in Lowood, Queensland which was ultimately paid for with cash.

---

[20] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.
[20] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 38.
[21] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.
[21] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 40.
[22] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.
[22] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 41.
[23] US Department of Justice, 'One of the World's Largest Digital Currency Companies and Seven of Its Principals and Employees Charged in Manhattan Federal Court and Running Alleged $6 Billion Money Laundering Scheme', 28 May 2013.
[24] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 30.
[25] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 31.
[26] Technocash, 'Opportunity: Own the Technocash Payment Platform', Media Release, 5 July 2013.
[27] http://www.technocash.com/pages/press-release.cfm

Initially, cash was 'structurally deposited' (multiple cash deposit amounts lower than the AML/CTF Act reporting limit of $10,000) into Kalaja's bank accounts, then transferred to GDK's bank account where structured deposits also took place. The law firm completing the property conveyance also receipted 11 structured cash deposits (which avoided the reporting obligation under the FTR Act) and telegraphic deposits from the company's bank accounts.

Subsequent to the land purchase, the company's bank account statements were given to a 'Jim's Bookkeeping' franchisee who was instructed to create the first set of accounts for GDK showing the purchase of the land. Instructions to the bookkeeper, given by Kalaja's uncle, was that the GDK deposits belonged to Daniel Kalaja and were to be credited to a loan account in his name.

Jim's bookkeeping created the accounts and handed them to Kalaja's uncle who then provided them to another accountancy firm. However, the account history of the account's financial balances was not transferred to this later accountancy firm and thus reconstruction of balances was not possible without the information from the bookkeeper.

GDK developed the Lowood land and subsequent sale of developed lots eventually exceeding $2.5 million. Prior to the sale of all Lowood land, the apparent development profitability led to a loan approval from a major bank for GDK to enable purchase of another development, a $1.2 million development land block in Upper Caboolture in 2007.

Confiscation investigations commenced in 2008 prior to both developments being completed.

2. Do any of the services provided by TCSPs, and identified by the FATF as requiring regulation, pose a demonstrated low ML/TF risk in the Australian context?

3. What are the benefits of requiring TCSPs to comply with AML/CTF obligations when performing services that may pose an ML/TF risk?

The benefits include compliance with FATF AML/CTF international standards which will also likely impede the activity of Australian-based and overseas-based crime groups who, according to AUSTRAC, use professionals, including TCSPs, to help undertake transactions to:[28]

- obscure ultimate ownership through complex layers and structures;
- conceal proceeds of crime;
- legitimise illicit funds;
- avoid tax;
- avoid regulatory controls;
- provide a veneer of legitimacy to criminal activity;
- avoid detection and confiscation; and
- frustrate law enforcement investigations.

The FATF found that reporting entities are the best source of information with respect to beneficial ownership for law enforcement investigations with the TCSP analysis concluding that "prevention of corporate vehicle misuse for ML purposes could be improved by knowing or being in a position to determine in a timely fashion who are the ultimate beneficial owners of a company and who are the trustees, settlors, beneficiaries involved with a trust. It would also be important to find out for what purpose the corporate vehicle was formed, why foreign

[28] AUSTRAC, 'Money laundering in Australia 2011', 2011, p. 28.

jurisdictions are being used for creation/administration of the entity, and why complex structures are being built". [29]

4. To what extent are the FATF's CDD obligations already reflected in existing regulation (including self-regulation) for Australian TCSPs?

5. To what extent do existing mechanisms that allow for regulatory oversight of TCSPs mitigate any ML/TF risks that may be posed by the services TCSPs provide?

6. What lessons can be learned from the experience of regulating TCSPs under AML/CTF regimes in other jurisdictions?

In their assessment of the UK anti-money laundering system, Transparency International UK concluded:[30]

> *The current regulatory system for these sectors relies on a patchwork of 22 different supervisors – mostly private sector institutions – to ensure that firms abide by the rules. It is this system that is structurally unsound.*
>
> *The UK has experimented with a low-cost model of supervision that relies on outsourcing responsibility for regulatory oversight to a wide range of private sector bodies. This approach, unique to the UK, has led to an environment where standards of supervision vary widely. Ineffective supervision – where it occurs – leads to inadequate compliance with the rules by firms within the sector, low reporting of suspicions and poor quality reporting.*

This is not a path the Australian Government should seek to follow and a properly resourced AUSTRAC should regulate the DNFBP sectors.

7. What services provided by TCSPs should be regulated under the AML/CTF regime?

8. Do any of the services provided by TCSPs as defined by the FATF pose a low ML/TF risk in the Australian context? If so, what evidence is there of this?

9. What should be done if there is an overlap of regulation of DNFBPs?

10. What impact would the costs associated with complying with the AML/CTF regime have on TCSPs?

11. What additional administrative structures will legal practitioners need to put in place to comply with the requirements of the AML/CTF regime?

12. How would regulating TCSPs for AML/CTF purposes impact on the delivery of services to clients?

13. How would AML/CTF obligations impact on the client confidentiality obligations of TCSPs?

6.1 Enrolment and scope of services

• What professional activities undertaken by TCSPs should be regulated under the AML/CTF Act?

---

[29] FATF, 'The Misuse of Corporation Vehicles, including Trust and Company Service Providers', October 2006, p. 17.

[30] Kevin Bridgewater, 'Don't Look, Won't Find. Weaknesses in the Supervision of the UK's Anti-Money Laundering Rules', Transparency International UK, November 2015, p. 5.

The FATF Recommendation 22 sets out the customer due diligence and record-keeping requirements set out in Recommendations 10, 11, 12, 15, and 17, for TCSPs which are outlined below at CDD question 6.2.

The FATF states that "DNFBPs should be required to take appropriate steps to identify and assess their money laundering and terrorist financing risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels). They should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities and self-regulatory bodies. The nature and extent of any assessment of money laundering and terrorist financing risks should be appropriate to the nature and size of the business."[31]

The FATF Recommendations 24 and 25 outline measures countries should take to ensure the availability of adequate, accurate and timely information on the beneficial ownership and control of legal persons and arrangements.[32] Countries, such as Australia, that allow nominee shareholders or nominee directors, should take effective measures to ensure that they are not misused for money laundering or terrorist financing.

• Should TCSPs be required to enrol with AUSTRAC?
The Synod believes that it would be appropriate for TCSPs to be enrolled with AUSTRAC so there is a greater ability of AUSTRAC to provide education and oversight to TCSPs in relation to their AML/CTF obligations.

6.2 Customer due diligence (CDD)
• What CDD obligations should TCSPs have?
The FATF Recommendation 22 (DNFBPs CDD) advise that customer due diligence and record-keeping requirements set out in Recommendations 10, 11, 12, 15, and 17, apply to DNFBPs including TCSPs when they prepare for or carry out transactions for a client concerning the following activities:[33]

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement; and
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

• When should the obligation for TCSPs to conduct CDD on clients commence?
As per FATF Recommendation 22 (DNFBPs CDD).[34]

6.3 Ongoing customer due diligence

[31] FATF, 'International Standards on Combating ML and FT & Proliferation; The FATF Recommendations', p. 33.
[32] FATF, International Standards on Combating ML and FT & Proliferation; The FATF Recommendations, p 22
[33] FATF, 'International Standards on Combating ML and FT & Proliferation; The FATF Recommendations', p. 19-20.
[34] FATF, 'International Standards on Combating ML and FT & Proliferation; The FATF Recommendations', p. 19-20.

• What ongoing due diligence obligations should apply to TCSPs?
As per FATF Recommendation 22 (DNFBPs CDD) which incorporates requirements from Recommendations 10 and 12.[35]

6.4 Reporting obligations
• If TCSPs have suspicious matter reporting obligations, should such reports be lodged with AUSTRAC or an industry body?
Suspicious matter reports from TCSPs should be required to be lodged with AUSTRAC so that AUSTRAC can assess and act on the intelligence provided and also is able to assess the extend to which the TCSP sector is being compliant with the AML/CTF obligations.

• Should TCSPs be able to voluntarily report suspicious matters to the AML/CTF regulator that relate to a service that is not a designated service?
This would seem to be required as per FATF Recommendation 23 for all DNFBPs.[36] Thus the Synod strongly supports TCSPs being able to make additional voluntary suspicious transaction reports beyond any legal obligations they would have to do so under AML/CTF requirements.

6.5 Internal controls– AML/CTF programs
• Should TCSPs have an obligation to develop and maintain an AML/CTF program?
The Synod believes that TCSPs should have an obligation to have an AML/CTF program that outlines what procedures they will take to ensure that they meet any AML/CTF obligations introduced that apply to them.

• What are the implications of a risk-based approach for TCSPs?
A rick-based approach for TCSPs would be consistent with the FATF Recommendations and complements Australia's existing AML/CTF approach.

6.6 Record-keeping
• What records should TCSPs be required to keep?
TCSPs should be required to keep information on the directors and ultimate beneficial owners of the legal entities they establish, which should include name and address. It should also include what documents were used to verify the identity of the directors and ultimate beneficial owners.

• To what extent can record-keeping obligations for AML/CTF purposes leverage off other record-keeping obligations that TCSP have (for example, under taxation or corporations law, and laws governing the use of trust accounts)?
Various requirements are legislated by the *Income Tax Assessment Act 1936*, *Corporations Act 2001* and *Australian Charities and Not for Profit Commission Act 2012* with seven years the maximum retention period which is also that required by AML/CTF and the FTR Acts.

6.7 Monitoring and supervision
• Should AUSTRAC monitor and supervise TCSPs for compliance with AML/CTF obligations?
The FATF recommends the extension of supervision of the DNFBPs for AML/CTF compliance beyond casinos and bullion dealers to include services offered by other DNFBPs including TCSPs (among others).[37]

[35] FATF, 'International Standards on Combating ML and FT & Proliferation; The FATF Recommendations', p. 19-20.
[36] FATF, 'International Standards on Combating ML and FT & Proliferation; The FATF Recommendations', p. 20.
[37] FATF, 'AML and CTF measures Australia Mutual Evaluation Report', April 2015, p. 103.

Dr Mark Zirnsak
Director
Justice and International Mission Unit
Synod of Victoria and Tasmania
Uniting Church in Australia
Phone: (03) 9251 5265

Acknowledgement: The Synod thanks Gillian Donnelly from Just Integrity Solutions for the assistance with this submission.