LA TROBE UNIVERSITY

COLLEGE OF ARTS, SOCIAL SCIENCES AND COMMERCE
LA TROBE LAW SCHOOL

Mailing address
La Trobe University
Victoria 3086 Australia

latrobe.edu.au/law

CAMPUSES
Melbourne (Bundoora)
Albury-Wodonga
Bendigo
City (Collins Street)
Franklin Street (CBD)
Mildura
Shepparton
Sydney

Email: to: fintech.sen@aph.gov.au

30 June 2021

The Chair
Select Committee on Financial Technology and Regulatory
PO Box 6100
Parliament House
Canberra ACT 2600

Dear Senator Bragg,

Third Issues Paper: Submission on Debanking of the FinTech Sector

1 We thank you for the opportunity to make a submission on debanking and the FinTech sector.

La Trobe LawTech researchers have been investigating debanking practices since 2014. A study undertaken by Louis de Koker (La Trobe), Supriya Singh (RMIT) and Jonathan Capal (Developing Markets Associates) of the impact of debanking on Horn of Africa remittance communities in Melbourne, produced the following recommendations:

(i) recognising a legal right to access a payment account;
(ii) increased public-private partnerships between regulators and banks, including in relation to utilities, to enable them to manage integrity risks relating to remittance providers effectively and efficiently; and
(iii) improved risk-based regulation and supervision of remittance service providers.

(Louis de Koker, Supriya Singh and Jonathan Capal, 'Closure of Bank Accounts of Remittance Service Providers: Global Challenges and Community Perspectives in Australia' (2017) 36(1) *University of Queensland Law Journal* 119)

Our researchers have also been actively engaged in submissions and discussions regarding the virtual asset service provider standards adopted by the Financial Action Task Force, the global standard-setting body for anti-money laundering and counter terrorist financing.

Our research and global engagement of the issues relating to denial of financial services inform our submission.

2 Australian banks generally justify their de-banking decisions based on the risks posed by FinTech companies. We have however encountered little evidence of consistent and appropriate appraisals of money laundering or terrorist financing risks posed by an affected customer. An appropriate assessment of that risk requires the bank to consider the customer's risk management processes. In very few cases do Australian banks actually collect such information before banking services are denied. International anti-money laundering and counter terrorist financing standards require banks to undertake

LA TROBE UNIVERSITY

COLLEGE OF ARTS, SOCIAL SCIENCES AND COMMERCE
La Trobe Law School

individual assessments and not to engage in large-scale denials of service to industry sectors. While banks often cite these standards to support their denials of service there is therefore no clear evidence that Australian banks actually comply with the standards in relation to their debanking decisions.

We detail the global standards regarding appropriate risk assessment practices in Attachment A to this letter ('Debanking' of Australian FinTechs: International Standards and Practice).

3 We further note that the Australian Competition and Consumer Commission investigated debanking of non-bank providers of International Money Transfers (IMTs) and acknowledged competition concerns relating to debanking of competitors:

> "From a commercial perspective, there can be little incentive for a bank to supply banking services to an IMT supplier who is possibly going to win IMT business from that bank. HiFX alludes to this in its submission: '…. a residual risk to larger non-bank providers that banks look to secure a larger % [share] of the overall market by making it harder for, or refusing to provide services to, non-bank providers.'" (ACCC in Foreign Currency Conversion Services Inquiry: Final Report (2019) p. 57)

4 The practices experienced by FinTechs reflect those captured by the Australian Small Business and Family Enterprise Ombudsman in their May 2020 *COVID-19 Recovery Plan*:

> "The greatest volume of denied service issues dealt with by the Ombudsman is in the banking sector, where there has been denial or withdrawal of service to small businesses in industries including adult service (brothels, individual sex workers and sex shops), tattoo parlours, cryptocurrency traders, precious metal traders and newsagencies providing Western Union remittance services. This 'de-banking' includes refusing access to a bank account, access to internet banking, and point of sales hardware. In de-banking customers, banks commonly provide businesses with only a small amount of information, usually a letter outlining a change to the bank's 'risk profile'. This may suggest a concern within the bank regarding anti-money laundering/counter terrorism financing (AML/CTF) issues. However, some businesses have had their bank's decision reversed suggesting that banks may not be conducting due diligence before their decision. The Ombudsman has also seen the practice of de-banking extended to personal accounts of family members not even involved in the operation of the business. In discussion with the banks, it appears that decisions are being made on arbitrary perceptions of morality. …" (own emphasis) (Australian Small Business and Family Enterprise Ombudsman, COVID-19 Recovery Plan (May 2020) 23-24)

5 We also note that Australian financial supervisors responded to debanking concerns by recognising the right of banks to make commercial decisions to manage their risk. These supervisors have however not provided sufficient information about the supervisory processes they follow to ensure that the debanking decisions comply with the relevant

LA TROBE UNIVERSITY

COLLEGE OF ARTS, SOCIAL SCIENCES AND COMMERCE
La Trobe Law School

international standards and are informed by appropriate assessments of actual risks posed by each customer rather than by ulterior factors.

6 We furthermore highlight the recommendation in our earlier paper that Australia should consider following the example of a growing number of countries that recognise a legal right to access the payment services of a bank. There are tried and tested examples of how to structure and implement such a right to balance the interests of society and the banks.[1]

7 We also note that the Australian Competition and Consumer Commission's *Foreign Currency Conversion Services Inquiry - Final Report* (2019) identified the risk that de-banking poses to competition in the supply of international money transfers (IMTs) and recommended as follows:[2]

> "The Australian Government should form a working group tasked with consulting on the development of a scheme through which IMT suppliers can address the due diligence requirements of the banks or providers of payment system infrastructure, including in relation to AML/CTF requirements. The Working Group should begin a public consultation process on the merits and design of such a scheme by 31 December 2019 and conclude that process by 30 June 2020. The Working Group should consider any alternative solutions to address the issue of de-banking that are raised by stakeholders during the public consultation process. By 31 December 2020, the scheme should be operational or the Working Group should have set out any alternative approach it will initiate to ensure that non-bank IMT suppliers are able to obtain efficient access to the banking and payment services they need to compete in the supply of IMT services to Australian consumers."

8 We therefore call for:

8.1 An investigation of supervisory practices that have been implemented to ensure that debanking decisions comply with global standards and with Australian law, especially in relation to discrimination;

8.2 a consideration of the progress made with the Australian Competition and Consumer Commission's proposed course of debanking action and the applicability of any emerging solutions to FinTechs; and

---

[1] Louis de Koker, Supriya Singh and Jonathan Capal, 'Closure of Bank Accounts of Remittance Service Providers: Global Challenges and Community Perspectives in Australia' (2017) 36(1) *University of Queensland Law Journal* 151-3.

[2] Australian Competition and Consumer Commission, *Foreign Currency Conversion Services Inquiry - Final Report* (2019) 11.

COLLEGE OF ARTS, SOCIAL SCIENCES AND COMMERCE
La Trobe Law School

8.3 a consideration of the implication of following the example of other countries by recognising a right to a payment account. [3]

Thank you for the opportunity to make a submission.

Yours sincerely

Professor Louis de Koker
B.Iuris, LLB, LLM, LLD (UFS), LLM (Cantab)
La Trobe LawTech
La Trobe Law School

Research Professor Pompeu Casanovas
UAB Director of Advanced Research
La Trobe LawTech
La Trobe Law School

[3] Louis de Koker, Supriya Singh and Jonathan Capal, 'Closure of Bank Accounts of Remittance Service Providers: Global Challenges and Community Perspectives in Australia' (2017) 36(1) *University of Queensland Law Journal* 151-3.

LA TROBE UNIVERSITY

COLLEGE OF ARTS, SOCIAL SCIENCES AND COMMERCE
La Trobe Law School

Attachment A

'Debanking' of Australian FinTechs: International Standards and Practice

1 Australian banks are reluctant to provide services to Australian FinTechs that operate in the crypto space. Large banks have adopted policies not engage or retain such businesses as customers. These policies are presented as positions taken after an assessment of money laundering, terrorist financing and proliferation financing risk posed by the sector.

There is however no convincing evidence that appropriate risk assessments are consistently undertaken as required by international standards adopted by the Australian government.

International standards: No generalized de-banking but customer-specific risk assessment

2 The Financial Action Task Force (FATF) is the global inter-governmental body that sets international regulatory and supervisory standards of money laundering, terrorist financing and proliferation financing risk. Australia is a member and the Australian government is committed to ensure that Australian laws and practices meet the FATF standards. These standards require banks to perform risk assessments, but they have also warned consistently, after de-banking practices became evident, that:[4]

> "Regulators and supervisors should also ensure that financial institutions are taking a risk-based approach to implementing AML/CFT measures, without prejudice to rules-based measures such as targeted financial sanctions. Implementation by financial institutions should be aimed at managing (not avoiding) risks. What is not in line with the FATF standards is the wholesale cutting loose of entire countries and classes of customer, without taking into account, seriously and comprehensively, their level of money laundering and terrorist financing risk and applicable risk mitigation measures for those countries and for customers within a particular sector." (own emphasis)

Also see the similar remarks were made in their 2014 statement entitled "FATF clarifies risk-based approach: case-by-case, not wholesale de-risking".[5]

3 FATF stated similarly in its 2016 *Guidance for a Risk-Based Approach: Money or Value Transfer Services (MVTs)*:[6]

> "When assessing the risks associated with … providers, different risk factors (types of products and services" offered, types of customers, distribution channels, and jurisdictions they are exposed to, experience of the provider, purpose of the account, anticipated account activity etc.) should be weighed; as

[4] FATF, FATF Takes Action to Tackle De-Risking, Statement, Paris, 23 October 2015.
[5] FATF, FATF Clarifies Risk-based Approach: Case-by-case, Not Wholesale De-risking, Statement, Paris, 23 October 2014.
[6] FATF, Guidance for a Risk-Based Approach: Money or Value Transfer Services (2016) [128].

LA TROBE UNIVERSITY

COLLEGE OF ARTS, SOCIAL SCIENCES AND COMMERCE
La Trobe Law School

> MVTS providers will not present the same levels of ML/TF risk. While some will pose a higher risk, there are others that will not." (own emphasis)

4 In par 25 of their *Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers*, FATF stated the following:

> "The FATF Recommendations do not predetermine any sector as higher risk. The standards identify sectors that may be vulnerable to ML and TF; however the overall risk should be determined through an assessment of the sector—in this case, the VASP sector—at a national level. Different entities within a sector may pose a higher or lower risk depending on a variety of factors, including products, services, customers, geography, and the strength of the entity's compliance program**.** (own emphasis)

5 The FATF approach is mirrored in the practices of other national regulators too. Thomas J Curry, the then-Comptroller of the Office of the Comptroller of the Currency of the United States stated in a 2014 address to the Association of Certified Anti-Money Laundering Specialists:[7]

> Money transmitters, as a business, are more risky than, say, your local movie theater. But that doesn't mean that all money transmitters are high risk, nor does it mean that other types of businesses couldn't be used for illicit purposes. The point is, one size doesn't fit all. No matter what type of business you are dealing with, you have to exercise some sound judgment, conduct your due diligence, and evaluate customers individually. Even in areas that traditionally have been viewed as inherently risky, you should be able to appropriately manage the risk. This is basic risk management, and that's a business that the institutions we at the OCC supervise excel at. You shouldn't feel that you can't bank a customer just because they fall into a category that on its face appears to carry an elevated level of risk. Higher-risk categories of customers call for stronger risk management and controls, not a strategy of total avoidance. Obviously, if the risk posed by a business or an individual is too great to be managed successfully, then you have to turn that customer away. But you should only make those decisions after appropriate due diligence." (own emphasis)

6 The FATF has also provided guidance on the contents of such a risk assessment. In its *Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers,* it stated that risk assessments should consider aspects such as [par 31]:

> "a) The potentially higher risks associated both with VAs that move value into and out of fiat currency and the traditional financial system and with virtual-to-virtual transactions;
>
> b) The risks associated with centralised and decentralised VASP business models;

[7] https://www.occ.gov/news-issuances/speeches/2014/pub-speech-2014-39.pdf.

LA TROBE UNIVERSITY

COLLEGE OF ARTS, SOCIAL SCIENCES AND COMMERCE
La Trobe Law School

> c) The specific types of VAs that the VASP offers or plans to offer and any unique features of each VA, such as AECs, embedded mixers or tumblers, or other products and services that may present higher risks by potentially obfuscating the transactions or undermining a VASP's ability to know its customers and implement effective customer due diligence (CDD) and other AML/CFT measures;
>
> d) The specific business model of the VASP and whether that business model introduces or exacerbates specific risks;
>
> e) Whether the VASP operates entirely online (e.g., platform-based exchanges) or in person (e.g., trading platforms that facilitate peer-to-peer exchanges or kiosk-based exchanges);
>
> f) Exposure to Internet Protocol (IP) anonymizers such as The Onion Router (TOR) or Invisible Internet Project (I2P), which may further obfuscate."

7 The experience of smaller FinTechs in Australia is that Australian banks do not comply with these standards. The banks, when pressed, generally refer to standing policy decisions that they will not engage with businesses involved in crypto. Individual risk assessments may be undertaken in relation to large FinTechs but in the majority of cases FinTechs are not even given an opportunity to provide information about their business model and risk control measures. The lack of appropriate consideration of the risk and risk management information of an individual applicant does not meet the FATF standards.

8 De-banking decisions that are not informed by appropriate due diligence and risk assessment but may be informed by alternative considerations are also evident in the USA in practices of some banks. In 2020 the US Office of the Comptroller of the Currency (OCC) stated: [8]

> "Despite the OCC's statements and guidance over the years about the importance of assessing and managing risk on an individual customer basis, some banks continue to employ category-based risk evaluations to deny customers access to financial services. This happens even when an individual customer would qualify for the financial service if evaluated under an objective, quantifiable risk-based analysis. These banks are often reacting to pressure from advocates from across the political spectrum whose policy objectives are served when banks deny certain categories of customers access to financial services."

[8] Office of the Comptroller of the Currency, 'Fair Access to Financial Services' RIN 1557-AF05 (2020) at https://www.occ.treas.gov/news-issuances/federal-register/2020/nr-occ-2020-156a.pdf 4-5.