Founding Partner
OPTUS

CLYDE&CO

Agmon & Co. Rosenberg Hacohen & Co.

MACQUARIE University

New Payment Products and Services – Potential anti-money laundering and counter-terrorist financing risks

DR DORON GOLDBARSHT

I gratefully acknowledge the support of the Optus Macquarie University Cyber Security Hub, Clyde & Co and Agmon & Co. Rosenberg Hacohen & Co. for funding this research.

CONTENTS

INTRODUCTION

New payment products and services (NPPSs) utilise innovations to initiate payments through, or to extend the reach of, traditional markets. They provide an alternative for clients to the products and services that are commonly offered by traditional regulated financial institutions, such as banks. Their development allows for increased access to financial services for a wider population, creating new markets. But NPPSs can also pose risks of money laundering (ML) and terrorist financing (TF) funds generation and transfer.[1] This whitepaper identifies different types of NPPSs, explains how they operate, and identifies some of the anti-money laundering and counter-terrorist financing (AML/CTF) risks that are associated with each type.

WHY ARE NEW PAYMENT PRODUCTS AND SERVICES IMPORTANT IN THE REALM OF AML/CTF?

NPPSs are increasingly interconnected, not only between themselves but also with traditional payment methods.[2] One of their greatest positive impacts has been the inclusion of individuals from developing countries in which basic financial services have not previously been sufficiently available.[3] Simultaneously, however, methods of ML and TF have also evolved to circumvent legal protections in this area. Many NPPSs are anonymous by design, rendering them vulnerable to exploitation for ML/TF, particularly in jurisdictions with weaker AML/CTF laws.[4] The further development of NPPSs requires monitoring, law reform, and enforcement, but in a way that does not stifle the benefits that these technologies bring.[5]

HOW NEW PAYMENT PRODUCTS AND SERVICES WORK AND THEIR POTENTIAL AML/CTF RISKS

NPPSs both enhance existing financial services and create entirely new ones. They may be used to co-mingle illicit cash with legitimate business takings, move illicit funds across borders, or conceal criminal proceeds and send them offshore.[6] This section will focus particularly on prepaid cards, mobile payment services, internet-based payment services and virtual currencies, internet-based loans, and alternative remittance services. It will first describe the payment system and explain how it works, the entities that are involved, and their roles or activities. It will then detail the potential risks involved with each of the NPPSs.

PREPAID CARDS

Prepaid cards, the value of which derives from money given to the card issuer, are increasingly utilised by small and medium enterprises and retail merchants.[7] The preloaded value is encoded on a magnetic strip or an electronic chip.[8] These are readily purchasable from retail stores and customers are not subject to the costs of opening a payment account.

The multiple types of prepaid cards available for purchase have different levels of associated risk. Closed-system prepaid cards fall on the lower end of the spectrum of AML/CTF risk.[9] These cards limit users to purchases of goods or services from the merchant issuing the card, such as is the case with gift cards. They can be purchased anonymously with cash and the end-users need not identify themselves. However, the cards cannot be redeemed for cash, which reduces their risk level.[10] Semi-closed prepaid cards, such as shopping centre gift cards, operate similarly, but can be used to pay multiple merchants or service providers. These are often issued by third parties, such as banks.[11] In

contrast, open-system prepaid cards can be used at most merchants that have the capacity for electronic funds transfer at point of sale (EFTPOS). These include charged travel cards, which are reloadable and can be used to retrieve cash from automated teller machines (ATMs).

Potential AML/CTF risks of prepaid cards

The AML/CTF risks of prepaid cards vary between closed, semi-closed and open-system cards. Among all systems, it can be difficult to identify the individual using the prepaid card, because providers do not necessarily need to comply with customer due diligence (CDD) requirements. If the purchaser of a prepaid card uses an account linked to a bank to originally acquire the card, this transaction can be traced back to them. Cards can, however, also be acquired anonymously with cash or other forms of NPPS.[12] Furthermore, third parties abroad can receive and utilise a shipped open-system card and access the value loaded onto it, provided they know the personal identification number.[13] The discreet size of the cards allows for easy transportation by mail or by being physically carried across borders.[14] Therefore, open-system cards in particular are vulnerable for use by money launderers or by terrorist organisations.

Examples of prepaid cards on the market[15]

I. **Australia Post**

Australia Post offers a range of prepaid card options in collaboration with Mastercard, consisting of both closed and open-system cards.[16] These include the Everyday Mastercard; the Travel Platinum Mastercard, which can store up to 11 currencies; and the Australia Post Gift Card by Mastercard, which can be loaded with between $20 and $500.

II. **Westfield**

Westfield offers gift cards that are redeemable at participating retailers in Australia with EFTPOS facilities – including, but not limited to, Myer, Coles, Woolworths Group, David Jones, Target, Kmart, JB Hi-Fi and Rebel Sport.[17] These are closed-system cards that are not refundable, exchangeable for cash, or reloadable. Therefore, they pose little to no AML/CTF risk.

III. **Universal Gift Card**

Universal Gift Card Pty Ltd offers open-loop prepaid cards issued by Heritage Bank Ltd. These cards can be used anywhere that Visa or Mastercard prepaid cards are accepted. The cards cannot be used for mail or telephone orders or, except for some reloadable cards, at an ATM. They are not linked to a bank account.[18]

MOBILE PAYMENT SERVICES

Mobile payment services encompass a range of transaction types in which a mobile phone is used in the payment process.[19] These transactions are facilitated by non-traditional financial institutions, such as telecom operators, as well as by traditional institutions, such as banks, working in conjunction with fintech companies. They utilise mobile telecommunication networks or proximity technologies in two main ways:[20] the bank-centric model and the mobile network operator-centric payment model.[21] In the bank-centric model, users can access money not tied to their payment account or they can access financial services through their phone with lower transaction limits. Here, mobile network operators merely facilitate the transfer of payment messages. Within the mobile network operator-centric model, there are two variations. First, in postpaid systems, the telecom operator allows the user to charge transactions

to their phone bill. Second, in prepaid systems, the customer uses the phone to authorise the deduction value from a prepaid account held by the operator.[22] Mobile payment services rely on several types of technologies, including text messaging, mobile internet access, near-field communication, programmed subscriber identity module (SIM) cards, and unstructured supplementary service data.[23] The user therefore does not need a bank account and, depending on the mobile network operator, may be able to access international payment services or withdraw cash from an ATM.[24]

Potential AML/CTF risks of mobile payments

Mobile payment services share the same main risks as prepaid cards. In both types of NPPS, the user can fund their transactions with cash so that the origin of the funds remains unidentified. Mobile payment services often also allow for transfers over long distances and sometimes internationally. These payments are particularly open to exploitation by terrorist organisations as different jurisdictions have varying levels of CTF controls and mechanisms, with those that have fewer restraints being more vulnerable.[25] Furthermore, mobile phones may be used by multiple people, rendering transactions highly elusive.[26] Lastly, mobile payment systems that allow for cash withdrawals at ATMs can add further complications to attempts at AML/CTF reform.[27]

Examples of mobile payment services on the market

I. **Google Pay**

Google Pay can be used across the web and in apps, without having to enter any payment information, as well as in-store.[28] When paying in-store with Google Pay, a customer's actual card number is not shared. In Sydney, Google Pay can also be used to pay for public transport by holding a phone to an Opal reader.

II. **Apple Pay**

Apple Pay operates in a very similar way to Google Pay. The user connects their cards with the app. When they make a purchase, Apple Pay uses a device-specific number and a unique transaction code. The card number is never stored on the device or on Apple servers and is never shared with merchants.[29] When paying with an eligible debit or credit card, Apple Pay does not keep transaction information that can be tied back to the user. The user can pay in-store via Face ID, which uses a specialised camera to create a depth map and an infrared image of the customer's face,[30] or Touch ID, which allows the customer to access their phone via fingerprint recognition.[31]

III. **Beem It**

This app is jointly owned by the Commonwealth Bank of Australia, the National Australia Bank and Westpac.[32] It was designed to allow users to track and share bills and group expenses. Users can make instant payments to anyone on their Beem It network using their in-app handle. They can transfer money between up to three debit cards and send up to $1,000 daily between them, without incurring fees.

IV. **Osko**

Osko is a product owned by BPAY, an electronic bill payment system based in Australia. It enables payments through a user's financial institution via online, mobile or phone banking facilities to organisations registered with BPAY. Osko also operates in conjunction with more than 60 banks and financial institutions within Australia.[33] It facilities person-to-person transfers and uses PayID (information unique to the customer that

is securely linked to their nominated bank account),[34] rather than Bank State Branch (BSB) and account numbers. Users can pay using a person's mobile number, email address or Australian Business Number (ABN). Osko functions through various bank apps, so it is implemented with the user's bank security standards.

INTERNET-BASED PAYMENT SERVICES AND VIRTUAL CURRENCIES

Internet payment services allow users to transfer electronic money to other individuals or to pay vendors. Some providers may require users to link their accounts with a bank account or a credit or debit card, while others allow for pre-funded transactions using a customer's direct account with the payment service provider.[35] When users remit digital currencies across borders, recipients can use these funds to make online purchases or they can withdraw the money at an ATM as cash in a national currency.

Internet-based payments through the use of virtual currency are common in the online gambling sphere, as well as in virtual worlds where users purchase this currency and can use it to make transactions within the system.[36] There is also a market for the purchase and sale of a digital representation of precious metals by paying intermediaries, who claim to hold the commodities on behalf of the online owner – all with little or no identity verification.[37] These derivatives can be exchanged between account holders.

In Australia, amendments in 2017 to the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) introduced new requirements in relation to digital currencies.[38] The definition of digital currency was drafted to cover a digital representation of value that meets several criteria, including that it must be interchangeable with money and may be used as consideration for the supply of goods or services.[39] In the revised explanatory memorandum for this amendment, however, it was stated explicitly that this criterion does not apply to loyalty or frequent flyer programs for which points may not be redeemed as money.[40] Therefore, by implication, loyalty or frequent flyer programs where a customer *can* exchange points for money fall under the scope of digital currency and are thus caught under the Act.

Potential AML/CTF risks of internet-based payment services and virtual currencies

Virtual currencies, unlike their national counterparts, do not have a central service provider and produce no records of transactions beyond the original purchase of the cryptocurrency.[41] In some cases, anonymous transfers and funding are possible, and customer relationships are typically not face-to-face.[42] The currency can then be transferred globally and converted to cash through a currency exchanger, rendering it vulnerable to use for TF – especially if it is transferred to banks in jurisdictions with fewer regulations in this area.[43]

These transactions happen quickly.[44] They are also able to be segmented and conducted pseudonymously (since, although a user's actual identity is not visible, information about their transactions is recorded publicly),[45] which raises issues for sufficient AML/CTF regulation.

Examples of internet-based payment services and virtual currencies on the market

I. **PayPal**

With PayPal, users create an account that is linked to their bank account or credit cards.[46] At the checkout for online purchases, the user chooses their preferred bank account or credit card and shipping address and PayPal pays the seller. The user's financial information is securely encrypted. The company offers a buyer protection service, which can be activated if items fail to arrive or are significantly different from their description, as well as refunded returns.[47]

II. **Amazon Pay**

After creating an account, users can select Amazon Pay as a payment method on Amazon and on the websites of other participating stores. Customers can then confirm the credit card and address details stored on their Amazon account during the checkout process. Amazon does not share the customer's full credit card, debit card or bank account number with participating merchants. Instead, it shares only the payment information required, which may include the last four digits of a card number and the card type.[48]

III. **Qantas**[49]

In 2018, the Qantas frequent flyer program had more than 12 million members and more than 200 partner organisations, including the four major banks, supermarkets and insurance companies.[50] In effect, Qantas acts as an unregulated bank, determining the value of points by deciding how many to issue, how many points are needed to purchase an upgrade or flight, and any additional fees or charges.[51] Members can use their points for a whole range of products and services, ranging from upgrading seats on flights, to gift cards with participating stores, to goods and services.[52]

IV. **KrisPay**

In 2018, Singapore Airlines launched a miles-based digital wallet, KrisPay.[53] This allows members to convert their KrisFlyer (frequent flyer) miles into KrisPay miles for everyday spending with merchants island-wide. Members can use their miles by scanning the Quick Response (QR) code provided at any participating outlet.

INTERNET-BASED LOANS

Internet-based loans are offered to customers by a range of companies working outside traditional financial institutions. These are generally small, short-term loans that are made either instantaneously or within a few business days. They are therefore subject to the same AML/CTF risk as the loans provided by traditional financial institutions. Over the past five years, more than 600 fintech lenders have emerged in the Australian market due to increased funding availability and demand from borrowers.[54]

Potential AML/CTF risks of internet-based loans[55]

The proceeds generated from criminal activity remain a source of funding for terrorist organisations. However, in the case of foreign terrorist fighters (FTFs), funds generated from criminal activity have typically involved petty crimes and are thus insufficient for greater activity. Three streams of funding for terrorist attacks have been identified. The first stream is funding to a network or organisation in amounts ranging from hundreds to millions of dollars. The second stream is funding to operations in amounts ranging from thousands to hundreds of thousands of dollars. The third stream is to individuals or cells in amounts ranging from hundreds to thousands of dollars.[56] It is therefore the first and third of these streams to which small-scale internet-based loans pose the most significant risk. One emerging trend in this area is suspected FTFs applying for small short-term loans from multiple providers while having no intention of repaying them.[57] These loans may be more easily facilitated by the emergence of online providers that offer fast personal or business loans with minimal turnaround time between the application and the receipt of funds. Terrorism microfinancing is made more difficult to detect when small transfers are varied and come from individuals whose accounts have not previously been noted for suspicious activity.[58] Self-funding from small-scale loans may be used for tactical short-term purposes, including lone-actor attacks, to fund travel for FTFs, or to finance military training.

Examples of internet-based loans on the market

I. **Afterpay**

Afterpay offers loans to consumers by splitting a purchase amount into four instalments, with the first paid at the time of purchase and the remaining three on a fortnightly basis.[59] These payments are interest free, but customers are charged relatively high fees for late payments. Purchases using Afterpay can be made both online and in-store by scanning a barcode on the app. An independent external audit of the company conducted in 2019, as ordered by the Australian Transaction Reports and Analysis Centre (AUSTRAC), found that the company had committed breaches of AML laws between February 2015 and November 2016 by failing to verify customer identities, but that the risks of ML and TF faced by the business were 'fairly low'.[60]

II. **Zip Pay**

Users make a purchase using Zip Pay and receive a statement of the amount owing on the first day of the next month.[61] The first payment for that purchase is then due on the last day of the next month, either in full or a minimum of $40 towards the purchase. The spending limit depends on the account type. With Zip Pay, the limit is $1,000 and with Zip Money users can borrow between $1,000 and $3,000, or they can apply through merchants for an account with a higher limit.[62]

III. **Prospa**

Prospa offers small business loans of up to $300,000. It can often provide a response within one hour if the application is lodged within standard business hours and the user allows utilisation of the bank verification system link.[63] If the applicant instead uses bank systems, response times are usually within just one business day. Prospa repayments are automatic, either daily or weekly.

IV. **Nimble**

Nimble provides a range of different loan types with small loans of between $300 and $2,000, medium loans of between $2,050 and $5,000, and personal loans of between $5,000 and $25,000.[64] Applications are solely online. For a successful application, payments can be made within 60 minutes of confirmation, depending on the loan type.

ALTERNATIVE REMITTANCE SERVICES

Alternative remittance services are financial systems in which value or funds are moved from one geographic location to another.[65] Money may be transferred within and between countries, including to locations that do not have modern formal banking services.[66] Transfers performed by these services often involve one or more intermediaries and they often function outside the conventional financial sector.[67] Alternative remittance systems are not traditionally classified as NPPSs. However, the online nature of most remittance services means that they are similar enough to include in this whitepaper.

Potential AML/CTF risks of alternative remittance services

Online remittance services are vulnerable to abuse in several ways. They carry a relatively high risk to AML/CTF due to the low costs associated with transfers and the ability to reach high-risk countries where formal financial channels

are less accessible or regulated. These services may be used for structuring to break down transactions into smaller amounts in order to avoid detection.[68] Increasingly, law enforcement agencies are detecting cases of remittance businesses being used as third parties to move funds or settle transactions involving two or more foreign countries.[69] It is common practice among overseas-based alternative remittance businesses to accept legitimate transfer instructions from parties and then send these instructions onto Australian counterparts, rather than conducting the transfer themselves. This is routinely done as part of the settlement of debts and to ease cash flow constraints. However, the practice is open to ML abuse. For example, FTFs are often required to pay for their own living expenses. Authorities in the Netherlands have found that this involves the transfer of several hundred or several thousand euros via regulated money and value transfer systems to agencies located near where terrorist organisations operate.[70] The remittance sector has relatively low detections of misuse compared to the banking sector, but this is a reflection of the lower total value of funds transferred via remittance. Alternative remittance services can assist in obscuring low-value transfers to finance terrorism.[71] They are, however, in a good position to assist in the detection of CTF if they comply with 'Know your Customer' practices.[72]

Examples of alternative remittance services

I. **OFX**

Once they have registered an account, whether for personal or business use, customers can transfer funds to OFX directly from their bank account by using BPAY or electronic funds transfer. The customer is given a quote and, if accepted, funds are transferred to another country. This will usually take one or two business days.[73] OFX boasts savings of up to 60% on the rates charged by banks. For transactions over A$10,000 or the equivalent, OFX does not charge fees. Like other foreign-exchange fintechs, OFX is subject to growing AML/CTF activism.[74]

II. **TransferWise**

TransferWise customers can open a foreign currency account as an alternative to a bank account abroad. These accounts can hold more than 50 currencies at once and allow for conversions between them almost instantly.[75] The rates are up to 16 times better than those offered by banks when sending money abroad. Customers with these accounts can receive free Mastercard debit cards to allow for cash withdrawals. TransferWise also offers business accounts that allow freelancers or sole traders to be paid by international clients. Businesses can also use these accounts to pay international employees or suppliers.

III. **XE**

Customers can open free personal accounts that attract no monthly charges. XE does not charge fees to receive money. It also does not apply transfer fees to foreign exchange transactions, although third-party banks may apply these fees when transferring the funds.[76] XE offers business accounts with services including currency data, international payments, and FX risk management solutions.[77]

CONCLUSION

Innovation in the fintech sphere allows for greater financial participation globally. It has the potential to open new markets and encourages the growth of pre-existing ones. Innovation is the main reason for the growth in NPPSs that we are experiencing today. NPPSs have made it much easier for start-ups and established companies to scale up their business by offering competitive payment products, services and prices. They offer payments through, or extend the reach of, traditional retail electronic payment systems, providing faster and more convenient services to users. By making use of rapidly advancing technology, NPPSs have the potential to foster stronger and more interconnected economies with robust competition. They allow for the inclusion of individuals from developing countries and areas in which traditional financial services may be insufficient or unavailable.

At the same time, NPPSs commonly involve anonymity, facilitate easier cross-border transactions, have faster turnaround times than traditional financial institutions, and allow for lower transactional amounts that may go undetected. These qualities mean that they carry risks of vulnerability to ML and TF as criminals and terrorist organisations may use these products and services to circumvent legal regimes that have not adapted quickly enough to changing technologies. Through monitoring, investigation and appropriate law reform, these risks can be better identified and mitigated so that innovative NPPS technologies can be used to their full positive potential.

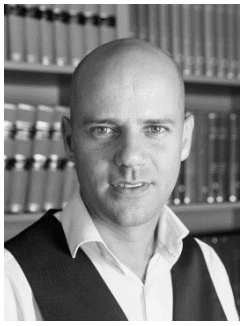
BIBLIOGRAPHY

[1] FATF, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (Paris, 2013) pp.13–20.
[2] FATF, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (Paris, 2013) p.10. See also Górka, J. (ed.), *Transforming Payment Systems in Europe* (Springer Heidelberg, 2016).
[3] Winn, J. and de Koker, L., 'Introduction to Mobile Money in Developing Countries: Financial Inclusion and Financial Integrity Conference Special Issue' (University of Washington School of Law Research Paper No. 2013-01, Seattle, 2013); Malady, L., Buckley, R.P. and Arner, D.W., 'Developing and Implementing AML/CFT Measures Using a Risk-Based Approach for New Payments Products and Services' (CIFR Paper No. 028/2014 and University of Hong Kong Faculty of Law Research Paper No. 2014/021, 2014).
[4] FATF, *Emerging Terrorist Financing Risks* (Paris, 2015) pp.20–21.
[5] Zerzan, A., 'New Technologies, New Risks? Innovation and Countering the Financing of Terrorism' (World Bank Working Paper No. 174, Washington DC, 2009) pp.1–2.
[6] https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/money-laundering-australia-2011.
[7] Gurung, J., Wijaya, M. and Rao, A., 'AML/CTF Compliance and SMEs in Australia: A Case Study of the Prepaid Card Industry' (2010) 13(3) *Journal of Money Laundering Control* 184 at p.193; Sienkiewicz, S., 'Prepaid Cards: Vulnerable to Money Laundering?' (Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper No. 07-02, Philadelphia, 2007) pp.1–4.
[8] FATF, *Money Laundering Using New Payment Methods* (Paris, 2010) p.16. See also Choo, K.-K.R., 'New Payment Methods: A Review of 2010–2012 FATF Mutual Evaluation Reports' (2013) 36 *Computers & Security* pp.12–26.
[9] FATF, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (Paris, 2013) p.5; Sienkiewicz, S., 'Prepaid Cards: Vulnerable to Money Laundering?' (Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper No. 07-02, Philadelphia, 2007) pp.9–16.
[10] Linn, C.J., 'Regulating the Cross-Border Movement of Prepaid Cards' (2008) 11(2) *Journal of Money Laundering Control* 146 at p.147.
[11] Choo, K.-K. R., 'Money Laundering Risks of Prepaid Stored Value Cards' (Trends and Issues in Crime and Criminal Justice No 363, Canberra, 2008) pp.2–4.

[12] FATF, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (Paris, 2013) p.20.
[13] Sienkiewicz, S., 'Prepaid Cards: Vulnerable to Money Laundering?' (Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper No. 07-02, Philadelphia, 2007) pp.36–37.
[14] The FATF has evidenced in particular that ISIL has used prepaid cards to receive funds. See FATF, *Financing of the Terrorist Organization Islamic State in Iraq and the Levant (ISIL)* (Paris, 2015) p.24.
[15] The examples below, and later in this whitepaper, are not offered to suggest that they have been used for the purpose of ML/TF or that the companies issuing them are not complying with the relevant regulations.
[16] https://auspost.com.au/money-insurance/prepaid-cards.
[17] https://www.westfieldgiftcards.com.au/Online/Information/FAQ.
[18] https://universalgiftcard.com.au/terms.aspx.
[19] Krueger, M., 'Mobile Payments: The Second Wave' in Górka, J. (ed.), *Transforming Payment Systems in Europe* (Springer, Heidelberg, 2016) pp.214–235.
[20] Dahlberg, T., Mallat, N., Ondrus, J. and Zmijewska, A., 'Past, Present and Future of Mobile Payments Research: A Literature Review' (2008) 7(2) *Electronic Commerce Research and Applications* 165.
[21] FATF, *Report on New Payment Methods* (Paris, 2006) pp.6–8.
[22] FATF, *Report on New Payment Methods* (Paris, 2006) pp.6–8; FATF, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (Paris, 2013) p.9.
[23] Merritt, C., 'Mobile Money Transfer Services: The Next Phase in the Evolution in Person-to-Person Payments' (Retail Payments Risk Forum White Paper, Federal Reserve Bank of Atlanta, 2010) pp.13–14; FATF, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (Paris, 2013) p.9.
[24] FATF, *Report on New Payment Methods* (Paris, 2006) p.9; Chatain, P.L. et al, *Protecting Mobile Money against Financial Crimes: Global Policy Challenges and Solutions* (World Bank Publications, Washington DC, 2011) p.28.
[25] FATF, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (Paris, 2013) pp.6–9.
[26] Chatain, P. et al, 'Integrity in Mobile Phone Financial Services Measures for Mitigating Risks from Money Laundering and Terrorist Financing' (World Bank Working Paper No 146, Washington DC, 2008) pp.12–13.
[27] FATF, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (Paris, 2013) p.9.
[28] https://pay.google.com/intl/en_au/about/.
[29] https://www.apple.com/au/apple-pay/.
[30] https://support.apple.com/en-us/HT208108.
[31] https://support.apple.com/en-gb/HT201371.
[32] https://www.beemit.com.au/.
[33] https://osko.com.au/home.
[34] https://payid.com.au/.
[35] FATF, *Report on New Payment Methods* (Paris, 2006) pp.15–16.
[36] FATF, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (Paris, 2013) p.10.
[37] Hett, W., 'Digital Currencies and the Financing of Terrorism' (2008) 15(2) *Richmond Journal of Law and Technology* 4 at pp.4–9; FATF, *Report on New Payment Methods* (Paris, 2006) p.9.
[38] *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017* (Cth).
[39] https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5952_ems_ab6b819a-b113-4f6e-b9ed-ab37f596154e/upload_pdf/Anti-Money%20Laundering%20and%20Counter-Terrorism%20Financing%20Amendment%20Bill%202017_Revised%20EM.pdf;fileType=application%2Fpdf pp.16–17.
[40] https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5952_ems_ab6b819a-b113-4f6e-b9ed-ab37f596154e/upload_pdf/Anti-Money%20Laundering%20and%20Counter-Terrorism%20Financing%20Amendment%20Bill%202017_Revised%20EM.pdf;fileType=application%2Fpdf p.17.
[41] Hett, W., 'Digital Currencies and the Financing of Terrorism' (2008) 15(2) *Richmond Journal of Law and Technology* 4 at pp.6–13.
[42] FATF, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks* (Paris, 2014) pp.7–8.
[43] Hett, W., 'Digital Currencies and the Financing of Terrorism' (2008) 15(2) *Richmond Journal of Law and Technology* 4 at pp.6–13.
[44] Brantly, A., 'Financing Terror Bit by Bit' (2014) 7(10) *Combating Terrorism Center at West Point* 1 at pp.3–5.

[45] Keatinge, T., Carlisle, D. and Keen, F., 'Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses' (European Parliament, PE 604.970, Brussels, 2018) pp.30–31.
[46] https://www.paypal.com/au/home.
[47] https://www.paypal.com/au/smarthelp/article/what-is-paypal-buyer-protection-faq1269.
[48] https://pay.amazon.com/using-amazon-pay.
[49] https://www.qantaspoints.com/home.
[50] https://www.abc.net.au/news/2018-07-11/frequent-flyer-program-helping-airlines-more-than-customers/9977272.
[51] https://www.abc.net.au/news/2018-07-11/frequent-flyer-program-helping-airlines-more-than-customers/9977272.
[52] https://www.qantasstore.com.au/.
[53] https://www.singaporeair.com/en_UK/sg/ppsclub-krisflyer/use-miles/krispay/.
[54] https://www.afr.com/companies/financial-services/small-business-is-dumping-the-big-four-banks-for-fintech-lenders-20191213-p53jpi.
[55] https://www.austrac.gov.au/sites/default/files/2019-07/regional-risk-assessment-SMALL_0.pdf p 23.
[56] http://www.acams.org/wp-content/uploads/2015/08/Big-Problems-in-Small-Transactions-D-Hitzeroth.pdf p 2.
[57] https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf p 26.
[58] http://www.acams.org/wp-content/uploads/2015/08/Big-Problems-in-Small-Transactions-D-Hitzeroth.pdf p 4.
[59] https://www.afterpay.com/en-AU.
[60] https://www.abc.net.au/news/2019-11-25/afterpay-audit-austrac-low-risk-money-laundering/11734602.
[61] https://zip.co/.
[62] https://zip.co/how-zip-works.
[63] https://www.prospa.com/.
[64] https://nimble.com.au/.
[65] https://www.fatf-gafi.org/media/fatf/BPP%20SRVI%20June%202003%202012.pdf p.1.
[66] https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/money-laundering-australia-2011.
[67] https://www.fatf-gafi.org/media/fatf/BPP%20SRVI%20June%202003%202012.pdf pp.1–2.
[68] https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/money-laundering-australia-2011.
[69] https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/money-laundering-australia-2011.
[70] http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf p.22.
[71] https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/terrorism-financing-australia-2014.
[72] https://www.fatf-gafi.org/media/fatf/BPP%20SRVI%20June%202003%202012.pdf p.2.
[73] https://www.ofx.com/en-au/.
[74] https://www.afr.com/companies/financial-services/money-laundering-is-achilles-heel-of-forex-fintechs-ofx-boss-warns-20191126-p53e4w.
[75] https://transferwise.com/au/borderless/#borderless-explainer-video.
[76] https://www.xe.com/mt/au-money-transfer.
[77] https://www.xe.com/mt/au-business.

ABOUT THE AUTHOR



Doron Goldbarsht (doron.goldbarsht@mq.edu.au) is a lecturer in the School of Law at Macquarie University in Sydney, Australia and a member of the Optus Macquarie University Cyber Security Hub. He holds a Bachelor's degree and a Master's degree in law, specialising in commercial law, from the Hebrew University of Jerusalem, and a PhD from the University of New South Wales. His research focuses on managing the relationship between financial inclusion and anti-money laundering and counter-terrorist financing objectives, and state compliance with soft law. He has partnered with the Optus Macquarie University Cyber Security Hub, Clyde & Co and Agmon & Co. Rosenberg Hacohen & Co. on his current project, revolving around the anti-money laundering and counter-terrorist financing risks of new payment products and services, which are an alternative to the traditional financial services that are typically offered by regulated financial institutions.

ACKNOWLEDGEMENTS

The author wishes to thank Ms Pelin Ersoy for excellent research assistance. Parts of this whitepaper are based on a previous publication: Doron Goldbarsht, 'New Payment Systems, Potential Counter-Terrorist Financing Risks and the Legal Response in the United Kingdom' in Katie Benson, Colin King and Clive Walker (eds), *Assets, Crimes and the State: Innovation in 21st Century Legal Responses* (Routledge, 2020).

OPTUS

MACQUARIE University

OPTUS MACQUARIE UNIVERSITY

Cyber Security Hub

CRICOS Provider 00002J

This white paper is part of an insight and knowledge-sharing series from the Optus Macquarie University Cyber Security Hub.

The Cyber Security Hub relies on a network of experts across business, government and higher education. It promotes an interdisciplinary understanding of cyber security by bringing together technology, business, legal, policy, security intelligence and psychology perspectives.

The Cyber Security Hub offers a range of services and collaborative opportunities. This includes professional education, hosting events to promote up-to-date knowledge, publishing key insights and updates, and working with partners on their business challenges.

If your organisation would benefit from being a part of a cross-sector network and have a greater understanding of the complex issues surrounding cyber security, please contact us to discuss opportunities for collaboration at cybersecurityhub@mq.edu.au

For more information visit mq.edu.au/cyber-security-hub