Published on 22 December 2022

A GUIDE TO THE PAYMENT SERVICES ACT FOR E-WALLETS AND DIGITAL PAYMENT BUSINESSES

Part 1: General Restrictions and Anti-Money Laundering

[2022] SAL Prac 25

With the commencement of the Payment Services Act 2019 (2020 Rev Ed), payment service providers are now regulated under this overarching framework which encompasses the issuance of payment accounts and e-money, money transfers (both domestic and cross-border), merchant acquisition and cryptocurrencies. This two-part guide examines the key regulatory obligations in running a e-wallet and digital payment business in Singapore and offers some pointers on complying with these requirements.

Samson **LEO**[1]
LLB (Hons) (National University of Singapore);
Certified Anti-Money Laundering Specialist (ACAMS);
Co-founder and Chief Legal Officer, Xfers; Chief Legal Officer, Fazz.

I. Introduction

1 The Payment Services Act 2019[2] ("PSA") came into force on 28 January 2020 and provides an overarching regulatory framework to oversee and regulate payment services in Singapore. It takes the place of the repealed Payment Systems (Oversight) Act[3] and Money-changing and Remittance Businesses Act,[4] and addresses traditional payment activities while also providing

1 All views expressed in this article are the author's own, and the same goes for any errors herein. The author would like to thank Danielle Sim for her assistance and research.
2 2020 Rev Ed.
3 Cap 222A, 2007 Rev Ed.
4 Cap 187, 2008 Rev Ed.

a flexible modularised framework to regulate new forms of payment activities.

2 In particular, the PSA regulates payment services in seven broad categories[5] with the legislative intention to mitigate four key risks[6] identified in payment services: (a) loss of consumer moneys; (b) money laundering and terrorism financing ("ML/TF"); (c) fragmented payment systems without interoperability; and (d) technology and cyber risks.

3 The non-exhaustive table below sets out the seven payment services against some of the key obligations in the PSA and the accompanying notices and guidelines issued by the Monetary Authority of Singapore ("MAS") to address these four risks:

	Customer Protection	Anti-Money Laundering	Interoperability Powers	Technology Measures
Account Issuance Service	Major payment institutions are required to notify customers on transactions, provide a reporting channel for unauthorised transactions and reimburse customers for unauthorised transactions in certain cases.[7]	Payment service providers are required to comply with anti-money laundering measures,[8] in particular performing customer due diligence and ongoing monitoring.	MAS has powers to direct payment service providers to ensure interoperability with one another[9] or with common standards[10] and to impose common access regimes.[11]	As technology underpins the delivery of all digital payment services, MAS has set out six key cyber hygiene practices[12] as a baseline for all payment service providers to adhere to.

5 Payment Services Act 2019 (2020 Rev Ed) First Schedule.
6 *Parliamentary Debates, Official Report* (14 January 2019), vol 94 (Ong Ye Kung, Minister for Education).
7 Monetary Authority of Singapore, "E-Payments User Protection Guidelines" (last amended 5 September 2020).
8 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022)
9 Payment Services Act 2019 (2020 Rev Ed) s 25.
10 Payment Services Act 2019 (2020 Rev Ed) s 26.
11 Payment Services Act 2019 (2020 Rev Ed) s 51.
12 Monetary Authority of Singapore, "Notice PSN06 Cyber Hygiene" (5 December 2019).

Domestic Money Transfer Service	Major payment institutions are required to safeguard customers' funds in transit[13] – being any money they receive on account of their customers, and continue to hold at the end of each business day.[14]	Payment service providers are required to comply with anti-money laundering measures,[15] in particular the wire transfer obligations to collect and transmit the information on the payor and payee to the counterparty financial institution(s).	n/a	Additionally, MAS has set out some IT risk management principles and best practices in the form of guidelines[16] for all PSA licensees.[17]
Cross-border Money Transfer Service			n/a	

13 Payment Services Act 2019 (2020 Rev Ed) ss 23(1) and 23(2).

14 Payment Services Act 2019 (2020 Rev Ed) s 23(14), under the definition of "relevant money".

15 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022).

16 Monetary Authority of Singapore, "Technology Risk Management Guidelines" (January 2021).

17 While there is a corresponding "Notice PSN05 on Technology Risk Management", it currently only applies to operators and settlement institutions of designated payment systems, and not to Payment Services Act 2019 (2020 Rev Ed) licensees. However, the Monetary Authority of Singapore proposed in a recent "Consultation Paper on Proposed Regulatory Measures for Digital Payment Token Services" (26 October 2022) that this "Notice on Technology Risk Management" could be expanded to DPT service providers.

Merchant Acquisition Service		n/a	MAS has powers to direct payment service providers to ensure interoperability with one another[18] or with common standards[19] and to impose common access regimes.[20]	
E-money Issuance Service	Major payment institutions are required to safeguard the float[21] – being the money received from the customer and for which it is issued e-money (to a person in Singapore) in exchange.[22]	n/a	n/a	

18 Payment Services Act 2019 (2020 Rev Ed) s 25.
19 Payment Services Act 2019 (2020 Rev Ed) s 26.
20 Payment Services Act 2019 (2020 Rev Ed) s 51.
21 Payment Services Act 2019 (2020 Rev Ed) ss 23(3) and 23(4).
22 Payment Services Act 2019 (2020 Rev Ed) s 23(14) under the definition of "relevant money", as read with s 2 for the definition of "specified e-money".

Digital Payment Token ("DPT") Service	In the near future, payment service providers offering DPT will be required to safeguard customers' assets[23] (including DPTs), which may take the form of segregating customer assets from corporate assets. MAS will be setting these out in future subsidiary legislation and guidelines.	With ML/TF risk being a key concern for cryptocurrencies, all payment service providers offering DPT services are required to comply with anti-money laundering measures[24] starting from the first dollar worth of transfer – there is no "exempted" or "low-risk" DPT transaction unlike domestic/cross-border money transfers.	n/a	
Money-changing Service	n/a	Payment service providers are required to comply with anti-money laundering measures.[25]	n/a	

II. Scope – e-wallets and digital payment services

4 This two-part guide focuses on the typical e-wallet and digital payment services business models, which will encompass the following regulated activities:

23 Payment Services (Amendment) Act 2021 (Act 1 of 2021).

24 Monetary Authority of Singapore, "Notice PSN02 Prevention of Money Laundering and Countering the Financing of Terrorism – Digital Payment Token Service" (last updated 1 March 2022).

25 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022).

(a) Account issuance service: the e-wallet issued to the customer will likely fall within the definition of a "payment account" because the e-wallet is to be used to initiate a payment order or execute a payment transaction. For the avoidance of doubt, "e-wallets" is not a defined term in the PSA and is used in this guide interchangeably with payment account. E-wallet is the "container" holding the e-money.

(b) E-money issuance: the customer would "top up" his e-wallet (*ie*, the payment account) by sending money to the payment service provider, which will in turn issue the e-money to be reflected as a "balance" in the customer's e-wallet.

(c) Domestic money transfer: the customer "sends" his e-wallet "balance" to another user in Singapore (whether on the same e-wallet platform, or to another platform or bank account) or receives money from another user in Singapore (into his e-wallet or bank account).

(d) Cross-border money transfer: the customer "sends" his e-wallet "balance" to another person outside of Singapore (whether on the same e-wallet platform, or to another platform or bank account) or receives money from another user outside of Singapore (into his e-wallet or bank account).

(e) Merchant acquisition: a business customer (referred to as a "merchant") signs up with the payment service provider which will accept and process payment transactions for the merchant, enabling the merchant to receive payments through the e-wallet platform or through other payment platforms (*eg*, credit cards, bank transfers, other e-wallet platforms).

5 Cryptocurrency transactions involving dealing or exchanging cryptocurrencies (and soon custody and transfers of cryptocurrency) will fall under the Digital Payment Token ("DPT") service and are not discussed specifically in this guide, although some of the regulatory obligations highlighted in this

guide are applicable to all licensees, including those performing DPT services.

6 Additionally, this guide takes the point of view of a Major Payment Institution licensee under the PSA and does not seek to be a comprehensive guide for the PSA in general. A Standard Payment Institution licensee would have far fewer obligations under the PSA as compared to Major Payment Institutions, and payment service providers just starting out may wish to keep their payment transactions below the thresholds set out in s 6(5) of the PSA to enjoy lighter regulatory obligations, and to remain more agile in product ideation and product development. As a preliminary matter, payment service providers may wish to examine the various exemptions[26] under the PSA which they may be able to avail themselves of and to provide such services without having to apply for a PSA licence in the first place or to exempt themselves from specific PSA provisions.[27]

III. Key obligations and pointers

7 Expanding upon the table at para 3 above, the key obligations of a Major Payment Institution operating e-wallet and digital payment services are thematically grouped and discussed next.

26 For example, (a) exempted entities under s 13 of the Payment Services Act 2019 (2020 Rev Ed) ("PSA"); (b) transitional exemptions under ss 122–126 of the PSA and under the Payment Services (Exemption for Specified Period) Regulations 2019 (S 809/2019); (c) services designated as not "payment services" in the PSA First Schedule, Part 2; (d) limited purpose e-money/digital payment tokens as set out in the PSA First Schedule, Part 3; and (e) Payment Services Regulations 2019 (S 810/2019) rr 28–29.

27 For example, Payment Services Regulations 2019 (S 810/2019) rr 27 and 30–33.

A. General prohibitions and restrictions

(1) No lending out customer money or granting credit facilities

8 Licensees must not grant any credit facilities, such as advances or loans, to any individual in Singapore.[28] Furthermore, licensees providing an e-money issuance service must not lend out any customer money,[29] or use any customer money or interest earned on customer moneys, to finance – wholly or to any material extent— any of the licensee's business activities.[30]

9 In the author's experience, MAS has asked for a breakdown of the interest generated from the customer money and for an allocation of the interest revenue to specific business lines of the licensee. Licensees may consider including in their response to MAS what the interest revenue was used for (if it can be clearly earmarked), and to also compare the allocated interest revenue as a percentage of the operating expenditure of those business lines. As there is no guidance on what constitutes financing to a "material extent", licensees should consider against having interest revenue as their main source of revenue.

(2) No cash withdrawal from payment account e-money balance

10 Licensees providing a payment account to users who are resident in Singapore (or users whom the licensee has not determined as being resident outside of Singapore)[31] must not allow users to withdraw e-money from the user's payment accounts in the form of Singapore currency (*ie*, physical notes and coins). This withdrawal prohibition is regardless of whether it is directly at the licensee's places of business[32] or through agreements with a separate entity that exchanges e-money withdrawn for Singapore currency.[33] However, if the payment account is terminated, the licensee may allow withdrawal of the

28 Payment Services Act 2019 (2020 Rev Ed) s 20(1).
29 Payment Services Act 2019 (2020 Rev Ed) s 20(2)(*a*).
30 Payment Services Act 2019 (2020 Rev Ed) s 20(2)(*b*).
31 Payment Services Act 2019 (2020 Rev Ed) s 19(2).
32 Payment Services Act 2019 (2020 Rev Ed) s 19(1)(*a*).
33 Payment Services Act 2019 (2020 Rev Ed) s 19(1)(*b*).

remaining e-money in exchange for Singapore currency[34] as part of the account closure process.

11 In the author's opinion, this is generally not a major issue because this prohibition is highly targeted – it does not prevent foreign users from obtaining Singapore notes and coins for spending here, nor does it prevent Singapore residents from withdrawing foreign currency notes and coins for spending overseas. This "overseas withdrawal" is a common feature for international e-wallets to offer convenience to their users who are travelling – their users can easily head to an automated teller machine in the destination country to withdraw local currency for spending, instead of having to exchange the notes in their home country beforehand. In contrast, there is a much less compelling reason for a Singapore user withdrawing Singapore notes and coins and allowing this would go against the move towards encouraging cashless payments in Singapore.

(3) E-money load limits and transaction limits for payment accounts

12 A Major Payment Institution providing account issuance services must ensure that:

(a) the e-money balance contained in a user's personal payment account(s)[35] does not exceed the prescribed amount of S$5,000[36] (commonly referred to as the "stock cap"); and

(b) the total annual e-money transaction amount for a user's personal payment account does not exceed the prescribed amount of S$30,000[37] (commonly referred to as the "flow cap"). The author submits that this annual

34 Payment Services Act 2019 (2020 Rev Ed) s 19(4).

35 "Personal payment account" is defined in s 24(5) of the Payment Services Act 2019 (2020 Rev Ed) as being a payment account issued to (a) a user using it not in the course of business; and (b) a resident in Singapore or a user which the licensee has not determined to be resident outside of Singapore.

36 Payment Services Act 2019 (2020 Rev Ed) ss 24(1)(*a*) and 24(*c*)(i), read with Payment Services Regulations 2019 (S 810/2019) r 18(1).

37 Payment Services Act 2019 (2020 Rev Ed) ss 24(1)(*b*) & 24(1)(*c*)(ii) read with Payment Services Regulations 2019 (S 810/2019) r 18(2).

transaction limit should be interpreted as a rolling 365-day period because of the term "*any* period of one year" in s 24(1).

13 These limits are to be aggregated[38] across all personal payment accounts issued to each user, so simply issuing multiple accounts to the user will not sidestep this restriction. Only small payment accounts (capable of containing not more than S$1,000) and bearer payment accounts[39] would be excluded from the computation of such limits, but this likely would be quite cumbersome for both the user and the licensee to have to manage multiple such accounts if a licensee were to try to set it up just to circumvent the stock and flow caps. Additionally, there is a strong argument that doing so will go against the legislative intention of "protect[ing] customers by limiting a customer's potential loss from his e-money account" and "ensur[ing] continued stability of the financial system, by reducing the risk of significant outflows from banks deposits to non-bank e-money which can undermine the stability of our banks".[40]

14 Consequently, there have been continued industry efforts amongst the payment service providers to urge MAS to increase or to even do away with the stock and flow caps altogether.[41] In response, MAS has recently published a consultation paper[42] proposing to increase the stock cap from S$5,000 to S$20,000, and the flow cap from S$30,000 to S$100,000. This, in the author's opinion, is a step in the right direction in promoting cashless payments and reducing customer friction.

38 Payment Services Act 2019 (2020 Rev Ed) s 24(1)(*c*).

39 Payment Services Act 2019 (2020 Rev Ed) s 24(5) defines "small payment account" and "bearer payment accounts".

40 *Parliamentary Debates, Official Report* (14 January 2019), vol 94 (Ong Ye Kung, Minister for Education).

41 See, for example, Monetary Authority of Singapore, "Response to Feedback Received on the Proposed Payment Services Regulations" (December 2019) at para 5.3 and Natalie Choy, "UK-Singapore FTA May Loosen E-wallet Rules for UK Financial Firms Here" *The Business Times* (12 December 2020).

42 Monetary Authority of Singapore, "Consultation Paper on Proposed Amendments to Restrictions on Personal Payment Accounts that Contain E-Money" (18 October 2022).

15 Some exceptions to these stock and flow caps apply:

(a) These limits do not apply to payment accounts that are used in the course of business,[43] which means business users would be able to use e-money in their payment accounts to make larger business payments (as a recognition that businesses would generally load and spend more than what a consumer ordinarily would).

(b) These limits do not apply to payment accounts issued to users whom the Major Payment Institution (the account issuer and the e-money issuer) has determined are not residents in Singapore.[44] The author submits that obtaining the user's proof of residential address or tax domicile status should suffice for this purpose.

(c) The annual transaction limit does not apply to withdrawals of e-money from the user's personal payment account to his Singapore bank accounts[45] or overseas bank accounts.[46]

(d) The e-money balance in the personal payment account may exceed the prescribed S$5,000 if the excess is transferred out of the personal payment account at the end of the day on which the excess accrues.[47] MAS introduced this exemption in recognition of industry feedback that customers may make occasional large payment transactions[48] because it would otherwise just

43 Payment Services Act 2019 (2020 Rev Ed) s 24(5).

44 Consequently, such payment accounts issued to non-Singapore residents will fall outside the Payment Services Act 2019 (2020 Rev Ed) s 24(5) definition of a "personal payment account", and therefore the stock and flow caps in s 24 will not apply.

45 Payment Services Act 2019 (2020 Rev Ed) ss 24(1)(*b*) and 24(*c*)(ii) exclude transfers to a "personal deposit account" in the name of the user or designated by the user. Section 24(5) defines a "personal deposit account" as being a deposit account held with a bank in Singapore used other than in the course of business.

46 Payment Services Regulations 2019 (S 810/2019) rr 33(2) and 33(4) exclude transfers to an "overseas personal deposit account" in the name of the user or designated by the user. Rule 33(5) defines an "overseas personal deposit account" as being a deposit account held with a foreign entity.

47 Payment Services Regulations 2019 (S 810/2019) rr 33(1) and 33(3).

48 Monetary Authority of Singapore, "Response to Feedback Received on the Proposed Payment Services Regulations" (December 2019) at para 5.6.

be inconvenient for the user to break a larger transaction (*eg*, S$10,000) into multiple S$5,000 "top-ups and spend" cycles despite staying within the S$30,000 flow cap.

B. Anti-money laundering and countering financing of terrorism

16 With ML/TF being a key concern in ensuring that Singapore continues to be a responsible and trusted international financial centre, MAS has issued several notices setting out the requirements for licensees to exercise due diligence when dealing with its customers and to assist law enforcement to prevent ML/TF.

17 The MAS Notice PSN01[49] is the pertinent regulation for e-wallet and digital payment service providers, and is issued by MAS pursuant to its powers under s 27B of the Monetary Authority of Singapore Act 1970.[50]

(1) Risk assessment and mitigation

18 Payment service providers are expected to take appropriate steps to identify, assess and understand their ML/TF risks in their business – such steps include documenting and updating risk assessments, determining the appropriate mitigation to apply, and ensuring there are appropriate mechanisms to provide risk assessment information to MAS.[51]

19 After identifying these risks, payment service providers should then apply a risk-based approach in developing and implementing policies, procedures and controls.[52] These policies,

49 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022).

50 2020 Rev Ed.

51 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 5.2.

52 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 5.3.

procedures and controls are required to have been approved by senior management and, in practice, the anti-money laundering policy would generally be signed off by the CEO (or chief compliance officer or head of compliance), and corresponding procedures and controls will generally be signed off by the chief compliance officer or head of compliance.

20 This requirement to perform risk assessment and design mitigating measures also applies to payment service providers *before*: (a) launching new products and practices (including delivery mechanisms); or (b) using new technologies for either new or pre-existing products.[53]

(2) Customer due diligence

21 Carrying out customer due diligence ("CDD") is the cornerstone of mitigating ML/TF risks. Broadly, CDD encompasses several steps: identify[54] and verify[55] the customer, assigning a risk rating to the customer, screening the customer against ML/TF lists and sanctions lists,[56] performing enhanced due diligence measures for customers at higher risk of ML/TF[57] and conducting ongoing monitoring of the customer.[58]

53 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 6.1.

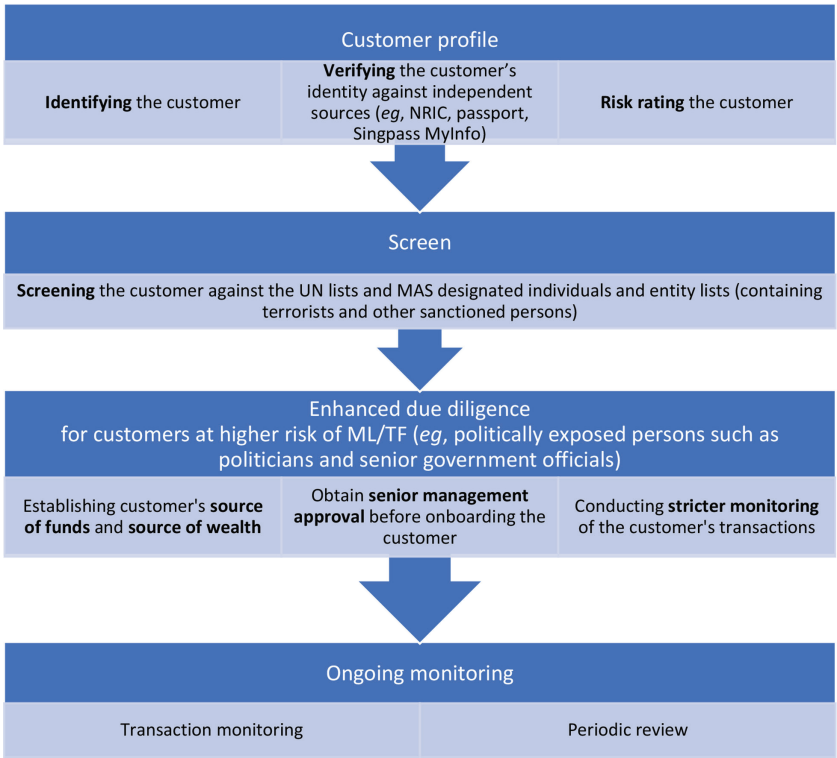
54 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at paras 7.5–7.8 and 7.10–7.17.

55 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 7.9.

56 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at paras 7.51–7.54.

57 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at paras 9.2–9.3 and 9.6.

58 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at paras 7.26–7.54.



22 Further operational guidance for each step can be found in the accompanying *Guidelines to Notice PSN01 on Prevention of Money Laundering and Countering the Financing of Terrorism* issued by MAS. In particular, these guidelines set out what type of CDD documentation should be collected from various types of customers,[59] measures for online onboarding customers,[60] and indicators of suspicious transactions.[61]

59 Monetary Authority of Singapore, *Guidelines to Notice PSN01 on Prevention of Money Laundering and Countering the Financing of Terrorism* (16 March 2020) at Appendix A.

60 Monetary Authority of Singapore, *Guidelines to Notice PSN01 on Prevention of Money Laundering and Countering the Financing of Terrorism* (16 March 2020) at para 7–12.

61 Monetary Authority of Singapore, *Guidelines to Notice PSN01 on Prevention of Money Laundering and Countering the Financing of Terrorism* (16 March 2020) at Appendix B.

23 Additionally, with the recent focus on offshore entities being used possibly abused for tax evasion and money laundering,[62] MAS in June 2019 also issued an additional guidance paper *Effective Practices to Detect and Mitigate the Risk from Misuse of Legal Persons*[63] setting out case studies, best practices and negative examples of conducting due diligence for customers who are companies, partnerships or trusts.

(3) Wire transfer obligations

24 When a payment service provider conducts domestic money transfer or a cross-border money transfer service via electronic means, it is required to collect information on the sender (known as the wire transfer originator) and recipient (known as the wire transfer beneficiary),[64] and to screen all the wire transfer originators and beneficiaries against the MAS lists of designated individuals and entities.[65]

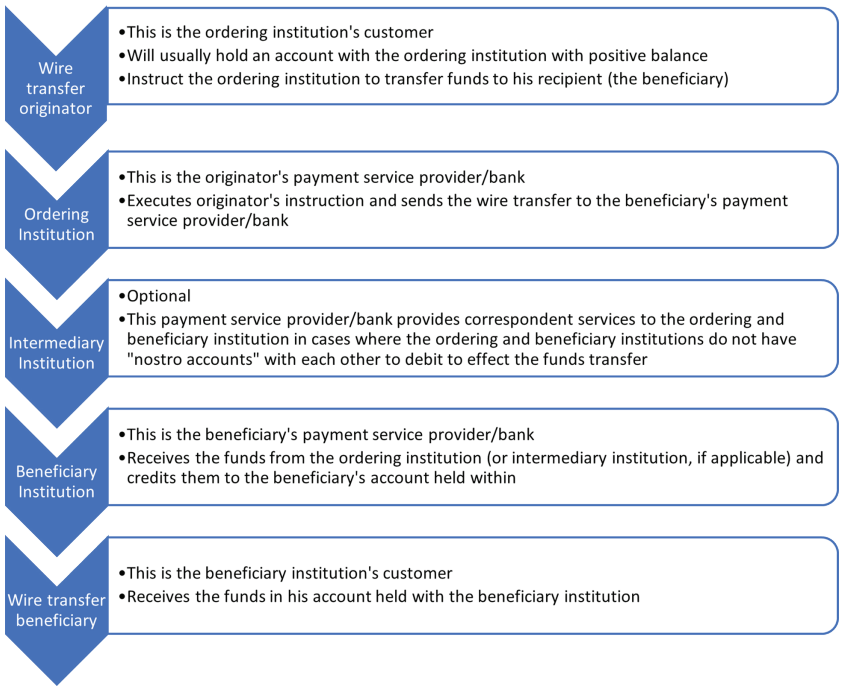
25 The process of transferring funds via wire transfers to a beneficiary holding an account with a different payment service provider is set out below:

62 Focus on offshore entities first started after the "Panama Papers" leak in 2016 and then the "Paradise Papers" leak in 2017: see, for example, Chong Koh Ping, "Panama Papers: Singapore Authorities Doing the 'Necessary Checks'" *The Straits Times* (5 April 2016) and Fabian Koh, "All's Not Well in Paradise: What You Need to Know about the Paradise Papers Leak" *The Straits Times* (7 November 2017).

63 <https://www.mas.gov.sg/regulation/guidance/effective-practices-to-detect-and-mitigate-the-risk-from-misuse-of-legal-persons> (accessed September 2022).

64 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 15.1.

65 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 7.53. The MAS lists of designated individuals and entities are available at <https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions/lists-of-designated-individuals-and-entities> (accessed September 2022).



26 The obligation of the ordering institution includes identifying the originator[66] and collecting information such as: (a) originator's name and account number;[67] (b) beneficiary's name and account number;[68] and (c) originator's address, unique identification number and date and place of birth[69] for cross-border money transfers above S$1,500. If the payment service provider is unable to comply with these obligations, it must not execute the wire transfer.[70]

66 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 15.3.

67 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 15.4.

68 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 15.4.

69 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 15.6.

70 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 15.11.

27 If the payment service provider is in the position of an intermediary institution, it shall onward transmit the information to the beneficiary institution[71] and retain all the information in the message from the ordering institution for a period of at least five years.[72] The intermediary institution shall implement risk-based policies and procedures on when it should suspend or reject wire transfers if it lacks the required information on the originator or beneficiary.[73]

28 For the payment service provider in the position of the beneficiary institution, it shall similarly implement risk-based policies and procedures on when it should suspend or reject wire transfers if it lacks the required information on the originator or beneficiary.[74]

29 In practice, banks and global payment service providers will generally use the SWIFT platform[75] to transmit and receive the information from one another for cross-border money transfers. For domestic money transfers in Singapore, banks and payment service providers use the FAST (or the older GIRO) electronic funds transfer network to transmit and receive the information.

(4) Payout restrictions

30 Payment service providers must not make payment to any recipient: (a) in the form of a bearer negotiable instrument;[76]

---

71 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 15.17.

72 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at paras 15.16 and 15.18.

73 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 15.20.

74 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 15.14.

75 SWIFT (Society for Worldwide Interbank Financial Telecommunication) is a global cooperative formed by banks in 1973 to solve inter-bank communications for cross-border transfers.

76 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 11.1.

or (b) in cash amounting to more than S$20,000[77] (aggregating multiple payment transactions where the payment service provider suspects are related or are deliberately restructured to avoid the S$20,000 limit[78]). This is in recognition that cash and bearer instruments pose a higher ML/TF risk because of their anonymity and ease of transfer.

31 In the context of e-wallets and digital payment services, this should similarly not pose any major business issues because these business models would generally move payments away from physical instruments and on to electronic transfers.

(5) Record-keeping and personal data

32 After having collected information and data on the customer and his transactions during the course of the customer due diligence process, the payment service provider must then keep these records and be ready to produce them to the relevant authorities for investigation or prosecution of criminal activities.[79] This is in line with the underlying principle of cooperating with law enforcement to prevent ML/TF.[80]

33 This record-keeping obligation extends to all other data, documents and information required to be produced under this MAS Notice PSN01[81] and the payment service provider must be

77 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 11.2.

78 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 11.3.

79 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 16.2.

80 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 4.1(c).

81 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 16.1.

ready to produce them to MAS and to its internal or external auditors[82] to demonstrate compliance with the notice.

34 Payment service providers will have to retain the data for at least five years after the customer closes the account or after the completion of the transaction, as the case may be.[83] The author submits that this legal retention obligation forms the justification for payment service providers to continue retaining customers' personal data despite s 25 of the Personal Data Protection Act 2012[84] ("PDPA").

35 The MAS Notice PSN01 also addresses certain intersections with the PDPA in relation to customers' personal data:

(a) Consent requirement (PDPA s 13): a payment service provider may collect, use or disclose personal data of a customer without consent[85] for the purpose of complying with the MAS Notice PSN01.

(b) Access requirement (PDPA s 21): a payment service provider shall provide to its customer access to the personal data[86] of that customer that is in the possession or under the control of the payment service provider.[87] It should be noted that while customers may also request under s 21(*b*) of the PDPA for payment service providers to explain how their personal data has

82 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 16.2(c).

83 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 16.3.

84 2020 Rev Ed.

85 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 17.4.

86 This includes the customer's full name, unique identification number (*eg*, NRIC, passport number), residential address, date of birth, nationality and any other personal data provided by the customer to the payment service provider: see para 17.3(a) of the Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022).

87 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 17.3(a).

been used or disclosed, the payment service provider must not inform the customer that it previously disclosed this customer's personal data to any prescribed law enforcement agency[88] (*eg*, Singapore Police Force[89] and Corrupt Practices Investigation Bureau[90]). This is also consistent that any suspicious transaction reports filed on a particular customer with the Suspicious Transaction Reporting Office of the Singapore Police Force should not be disclosed to that customer because it might prejudice any ongoing or future investigations, constituting the offence of tipping-off.[91]

(c) Correction requirement (PDPA s 22): a payment service provider shall correct any errors or omissions in the requesting customer's personal data as long as the payment service provider is satisfied that there are reasonable grounds for such request.[92]

(6) Suspicious transaction reporting

36 Payment service providers routinely collect and disburse money on behalf of their customers and if they have reasonable grounds to suspect that any money: (a) represents the proceeds; (b) was used in connection with; or (c) is intended to be used in connection with, any act which may constitute drug dealing or criminal conduct, they must file a suspicious transaction report with the Suspicious Transaction Reporting Office[93] via the SONAR platform.[94]

88 Personal Data Protection Act 2012 (2020 Rev Ed) s 21(4).
89 Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014 (S 368/2014) Schedule.
90 Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020 (S 272/2020) para 2.
91 Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 (2020 Rev Ed) ss 57(1) and 57(2).
92 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 17.3(b).
93 Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 (2020 Rev Ed) s 45.
94 Singapore Police Force, "STRO Online Notices and Reporting Platform" <https://eservices.police.gov.sg/content/policehubhome/homepage/stro-singpass.html> (accessed September 2022).

37 With a myriad of different customer profiles, account usage patterns, fund flows and business models, it is difficult to define what would constitute a suspicious transaction. Nevertheless, the guidelines to the MAS Notice PSN01 set out a non-exhaustive list of examples and situations which may indicate a transaction would require reporting, and they are broadly categorised as:

(a) transactions which do not make economic sense;

(b) transactions involving large amounts of cash or large transaction amounts;

(c) customer account transactions;

(d) transactions involving unidentified parties;

(e) tax crime;

(f) transactions relating to trade; and

(g) customer behaviour.[95]

Practically, it would be helpful to design the payment service provider's transaction monitoring programme around these indicators and to define various thresholds and variables according to the payment service provider's risk appetite and customer profiles.

38 This suspicion may arise at any stage of the customer relationship – before account opening, during customer due diligence, ongoing payment transactions, and account closure[96] – and the payment service provider should file a suspicious transaction report promptly.[97]

39 Payment service providers must establish internal policies, procedures and controls, designate a person or team

95 Monetary Authority of Singapore, *Guidelines to Notice PSN01 on Prevention of Money Laundering and Countering the Financing of Terrorism* (16 March 2020) at Appendix B.

96 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) para 18.3(b).

97 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 18.2.

for all employees to refer suspicious cases to, and keep records of all reports filed (along with all internal findings and analysis done).[98]

40 In practice, after filing a suspicious transaction report on a customer, the compliance team of financial institutions and payment service providers will recommend account closure and exiting the customer relationship due to the potentially increased ML/TF risk posed by the customer. Payment service providers would not want to be seen to be continuing to process or facilitate payment transactions which may potentially be linked to crime.

IV. Conclusion to Part 1 of this guide

41 In this first part of the guide, the regulatory principles of the PSA were explored and a common e-wallet and digital payment service business model was used to illustrate how certain activities are regulated payment services. Some general prohibitions and restrictions under the PSA were analysed, along with the author's personal opinions on the implications of such restriction on e-wallets and digital payment services. This first part ends off covering in detail the anti-money laundering requirements which are of critical importance to MAS and financial regulators worldwide.

42 The next part of this two-part guide will explore the other regulatory themes, such as customer protection, technology measures, outsourcing, human resource and regulatory reporting.

98 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services" (last updated 1 March 2022) at para 18.1(b).