

GUIDANCE FOR CREDIT INSTITUTIONS, PAYMENT INSTITUTIONS AND ELECTRONIC MONEY INSTITUTIONS OPENING ACCOUNTS FOR FINTECHS

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

FOREWORD

Technology is becoming ever more prevalent in our everyday lives, bringing with it a number of advantages, particularly in relation to automation and simplification. This has seen the development of numerous new products and services in a number of sectors, with the financial services sector being no exception.

The Financial Intelligence Analysis Unit ('FIAU') and the Malta Financial Services Authority ('MFSA') (hereinafter collectively referred to as 'the Authorities') are cognisant of risks which technological innovation may bring about, as well as the potential challenges for subject persons to assess the actual ML/FT risks they may be exposed to when considering whether to service any person whose activities are heavily reliant on technology.

It is for this reason that the Authorities are issuing this joint Guidance Document for Credit Institutions, Payment Service Providers and Electronic Money Institutions (hereinafter collectively referred to as 'Institutions') opening accounts for FinTechs.

This Guidance Document is designed to assist Institutions to acquire a better risk understanding of any such prospective customers, active in technology reliant areas, prior to servicing them, and is not intended to provide any explanations of how the respective technologies function.

While it is not intended for this Guidance Document to be binding, consideration thereof in the formulation of one's risk assessment measures, controls, policies and procedures is encouraged. It is important that it is read together with the Implementing Procedures and any other relevant guidance document issued by the FIAU, as well as within the more general context provided by the Prevention of Money Laundering and Funding of Terrorism Regulations ('PMLFTR'). This document does not provide for any derogation from any obligations that a subject person has to fulfil in terms of the PMLFTR but rather seeks to provide additional assistance as to how adherence thereto can be achieved when a prospective customer carries out particular activities.

It is emphasised that this document is solely intended for its users' general guidance and should neither be considered nor construed as advice or in any way a commitment on the part of the MFSA or the FIAU. Should a conflict arise between this document and the applicable laws, regulations or rules, the respective laws, regulations or rules are to prevail.

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

CONTENTS

TITLE 1 - SCOPE AND APPLICATION	1
SECTION 1- SCOPE.....	1
SECTION 2 - APPLICATION	2
SECTION 3 - DEFINITIONS.....	3
 TITLE 2 - GUIDANCE FOR CREDIT INSTITUTIONS, PAYMENT INSTITUTIONS AND ELECTRONIC MONEY INSTITUTIONS OPENING ACCOUNTS FOR FINTECHS	5
SECTION 1 - SCOPE AND APPLICATION	5
SECTION 2 - GENERAL GUIDANCE.....	5
SECTION 3 - SUPPLEMENTARY GUIDANCE FOR CREDIT INSTITUTIONS, PAYMENT INSTITUTIONS AND ELECTRONIC MONEY INSTITUTIONS OPENING ACCOUNTS FOR DLT EXCHANGES.....	9
 TITLE 3 - SUPPLEMENTARY GUIDANCE FOR CREDIT INSTITUTIONS, PAYMENT INSTITUTIONS AND ELECTRONIC MONEY INSTITUTIONS OPENING ACCOUNTS FOR ISSUERS OF DLT ASSETS	11
SECTION 1 - SCOPE AND APPLICATION	11
SECTION 2 - SUPPLEMENTARY GUIDANCE FOR CREDIT INSTITUTIONS, PAYMENT INSTITUTIONS AND ELECTRONIC MONEY INSTITUTIONS OPENING ACCOUNTS FOR ISSUERS OF DLT ASSETS.....	11
SECTION 3 - FURTHER SUPPLEMENTARY GUIDANCE FOR CREDIT INSTITUTIONS, PAYMENT INSTITUTIONS AND ELECTRONIC MONEY INSTITUTIONS OPENING ACCOUNTS FOR ISSUERS OF DLT ASSETS RAISING FUNDS IN DLT ASSETS.....	13
 TITLE 4 - SUPPLEMENTARY GUIDANCE FOR CREDIT INSTITUTIONS, PAYMENT INSTITUTIONS AND ELECTRONIC MONEY INSTITUTIONS OPENING ACCOUNTS FOR FINTECHS, SPECIFICALLY THOSE WHICH ARE AUTHORISED OR SEEKING TO BE AUTHORISED, BY THE MFSa, AS VFA SERVICE PROVIDERS	14
SECTION 1 - SCOPE AND APPLICATION	14
SECTION 2 - SUPPLEMENTARY GUIDANCE FOR CREDIT INSTITUTIONS, PAYMENT INSTITUTIONS AND ELECTRONIC MONEY INSTITUTIONS OPENING ACCOUNTS FOR FINTECHS WHICH ARE AUTHORISED OR SEEKING TO BE AUTHORISED BY THE MFSa	14

TITLE 5 - GUIDANCE FOR CREDIT INSTITUTIONS, PAYMENT INSTITUTIONS AND ELECTRONIC MONEY INSTITUTIONS OPENING ACCOUNTS FOR FINTECHS ACCEPTING DLT ASSETS AS A MEANS OF PAYMENT 16

SECTION 1 - SCOPE AND APPLICATION 16

SECTION 2 - GUIDANCE FOR CREDIT INSTITUTIONS, PAYMENT INSTITUTIONS AND ELECTRONIC MONEY INSTITUTIONS OPENING ACCOUNTS FOR FINTECHS ACCEPTING DLT ASSETS AS A MEANS OF PAYMENT 16

REVISIONS LOG

VERSION	DATE ISSUED	DETAILS
1.00	27 MARCH 2019	GUIDELINES ISSUED FOR CONSULTATION
1.01	18 JUNE 2019	GUIDELINES ISSUED

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

Title 1 Scope and Application

Section 1 Scope

G2-1.1.1 This document provides guidance to Credit Institutions, Payment Institutions and Electronic Money Institutions ('Institutions') opening accounts for those persons operating within the financial services sector and harnessing technological advancements (including *inter alia* artificial intelligence, distributed ledger technology, the internet of things and cloud technologies) for the development of a financial product or provision of a financial service ('FinTech Operators' or 'FinTechs'):

This would, for example, include but not be limited to:

- i. Issuers of Virtual Financial Assets ('VFAs') and VFA service providers;
- ii. The use of Distributed Ledger Technology ('DLT') for the carrying out and settlement of payment transactions as well as for the custody, clearing and settlement of securities-related transactions;
- iii. The use of smart contracts and/or the internet of things within the insurance industry when it comes to determinate types of insurance policies;
- iv. The use of Artificial Intelligence within the traditional financial services sector.

G2-1.1.2 For the purposes of this document, the term 'FinTechs' does not include:

- i. persons providing consultancy or advisory services to FinTechs; and
- ii. persons whose activity in relation to FinTech is solely limited to the development of software or other technological solutions used for, or being ancillary to, the provision of financial services and/or financial products but not the provision of the said service or product;

G2-1.1.3 This Title outlines the scope and application of this document.

G2-1.1.4 Title 2 provides guidance for Institutions opening accounts for FinTechs in general.

- G2-1.1.5 Title 3 provides supplementary guidance for Institutions opening accounts for FinTechs, specifically those persons offering their DLT Assets either to the public or through a private placement ('Issuers').
- G2-1.1.6 Title 4 provides supplementary guidance for Institutions opening accounts for FinTechs, specifically those which are authorised or seeking to be authorised, by the MFSA, as VFA service providers.
- G2-1.1.7 Title 5 provides supplementary guidance for Institutions opening accounts for FinTech accepting DLT Assets as a means of payment

Section 2 *Application*

- G2-1.2.1 This document is addressed to the Institutions opening accounts for FinTechs.

- G2-1.2.2 These Guidelines are neither intended to replace Institutions' internal procedures nor as an obligation for them to modify their risk appetite, but rather to:

- i. assist Institutions in acquiring a better understanding of the sector-specific risks involved; and
- ii. complement their due diligence procedures, *inter alia* by providing guidance on which information and documentation can be requested to assist them in reaching a decision as to whether to on board a customer or otherwise;

and this in line with the risk based approach which Institutions have to implement in terms of the PMLFTR and the Implementing Procedures - Part I.

- G2-1.2.3 This document is solely intended for its users' general guidance and should neither be considered nor construed as advice or in any way a commitment on the part of the Authorities. Unless otherwise stated, the omission of any reference in this document to particular obligations emanating from applicable laws, regulations or rules is not to be construed as tantamount to the inapplicability of the same to the Institutions. Furthermore, should a conflict arise between this document and the applicable laws, regulations or rules, the laws, regulations or rules are to prevail.

It is equally important to note that this document is non-binding in nature and that Institutions may make use of information and/or documentation

that is not referred to in this document to inform their risk understanding and assessment of a (prospective) customer. Needless to say that any such other information and documentation would have to be sufficiently reliable so as to allow the Institutions to make an independent assessment of the ML/FT risks inherent in servicing a give (prospective) customer.

G2-1.2.4 Further to G2-1.2.3, these guidelines do not provide any person with any claim to the opening of an account.

G2-1.2.5 Further to G2-1.2.3, these guidelines are to be read together with the Implementing Procedures and other relevant guidance issued by the FIAU, as well as within the more general context provided by the Prevention of Money Laundering and Funding of Terrorism Regulations ('PMLFTR'). This document does not provide for any derogation from any obligations that a subject person has to fulfil in terms of the PMLFTR but rather seeks to provide additional assistance as to how adherence thereto can be achieved.

In addition, the Institutions are to note that the document does in some cases propose for information to be obtained from the Fintech Operator or for undertakings to be obtained from the same. Institutions are to note that this is not a derogation from considering for risk assessment and on-going monitoring obligations any information which they may become aware of or may otherwise be publicly available, even though it contrasts with the information provided by the FinTech Operator. Moreover, the Institutions remain at all times responsible to ensure on a risk sensitive basis that any information, documentation and data provided by their customers is still relevant and up-to-date.

Section 3

Definitions

G2-1.3.1 (1) "Distributed Ledger Technology" or "DLT" means a database system in which information is recorded, consensually shared, and synchronised across a network of multiple nodes as further described in the First Schedule of the Innovative Technology Arrangements and Services Act, 2018, whether the same is certified under that Act or otherwise;

(2) "DLT asset" means (a) a virtual token; (b) a virtual financial asset; (c) electronic money; or (d) a financial instrument; that is intrinsically dependent on, or utilises, Distributed Ledger Technology;

(3) "DLT exchange" means any trading and, or exchange platform or facility, whether in Malta or in another jurisdiction, on which any form of DLT asset may be transacted in accordance with the rules of the platform or facility;

(4) "electronic money" has the same meaning assigned to it under the Third Schedule to the Financial Institutions Act;

(5) "financial instrument" has the same meaning assigned to it under the Second Schedule to the Investment Services Act, whether or not issued in Malta;

(6) "FinTech" means technologically enabled financial innovation that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services;

(7) "virtual financial asset" or "VFA" means any form of digital medium recordation that is used as a digital medium of exchange, unit of account, or store of value and that is not (a) electronic money; (b) a financial instrument; or (c) a virtual token;

(8) "virtual token" means a form of digital medium recordation whose utility, value or application is restricted solely to the acquisition of goods or services, either solely within the DLT platform on or in relation to which it was issued or within a limited network of DLT platforms: Provided that the term "DLT platform" referred to in this definition shall exclude DLT exchanges: Provided further that a virtual token which is or may be converted into another DLT asset type shall be treated as the DLT asset type into which it is or may be converted;

G2-1.3.2

Words and expressions used in this document, which are also used in the Virtual Financial Assets Act (Chapter 590 of the Laws of Malta) (the 'VFA Act') are, unless otherwise specified, to have the same meaning as in the said Act:

Provided that where there exists any inconsistency between the definitions provided in G2-1.3.1 above and those provided by the VFA Act, the definitions provided by the said Act shall prevail.

Title 2 Guidance for Credit Institutions, Payment Institutions and Electronic Money Institutions opening accounts for FinTechs

Section 1 Scope and Application

G2-2.1.1 Section 2 of this title provides guidance for Institutions opening accounts for FinTechs in general whereas Section 3 provides for supplementary guidance for instances where the FinTech in question is a DLT Exchange.

Section 2 General Guidance

G2-2.2.1 The risks inherent in establishing a business relationship with a FinTech should be assessed in line with any applicable regulatory requirements and on the basis of the methodology adopted by subject persons to risk assess other customer segments.

G2-2.2.2 Thus, in order to assess the risks inherent to establishing a business relationship with a FinTech Operator, the Institutions should consider the risk factors referred to in the Implementing Procedures Part I and any other Guidance issued by the FIAU, and, when considering the customer risk and the geographical risk, should have regard to the Operator's:

- i. Regulatory Status;
- ii. Activities; and
- iii. Use of Technology.

G2-2.2.2.1 Regulatory Status

FinTechs are likely to be subject to regulatory requirements, not least in the areas of AML/CFT. Not only is it usual to have conduct of business rules applicable thereto but very often there are licensing or authorisation requirements which act as a barrier to potential criminals. Moreover, being subject to AML/CFT requirements and to a level of supervision equivalent to what is provided for under Directive (EU) 2015/849 should lower the risk that the activity being carried out by the FinTech is abused for ML/TF purposes.

G2-2.2.2.1.1 To determine the regulatory status of the FinTech, Institutions should obtain a declaration from the FinTech Operator as to whether the Operator is:

- i. authorised or intends to apply for authorisation with a national, European or overseas regulatory authority (identifying such authority); and
- ii. a subject person under the Prevention of Money Laundering and Funding of Terrorism Regulations (S.L. 373.01 of the Laws of Malta) (the 'PMLFTR') or subject to AML/CFT requirements and to a level of supervision equivalent to what is provided under Directive (EU)2015/849.

Consideration has to be given to the standing of the jurisdiction the authorities of which would have authorised the Fintech Operator and/or would be responsible for supervising the said Operator for compliance with its obligations at law. If the jurisdiction results to be a high risk or non-reputable one, the regulatory status of the Operator would not be expected to decrease the risk associated with the same and may even increase the risk associated therewith.

G2-2.2.2.1.2 Notwithstanding G2-2.2.2.1.1, the Institution may also obtain information from public registers, where these are available.

G2-2.2.2.1.3 Where, pursuant to point G2-2.2.2.1.1 (i) above, the FinTech Operator is authorised or intends to apply for authorisation with a national, European or overseas regulatory authority, the Institution may also seek to obtain a copy of the authorisation held, or details of type of authorisation applied for, by the FinTech Operator unless this information is available through public registers as referred to in G2-2.2.2.1.2.

Provided that, where the FinTech Operator has applied for authorisation, the Institution should keep up to date with the progress of this application.

G2-2.2.2.1.4 Pursuant to G2-2.2.2.1.1 above, the Institution should also take into consideration, as part of its risk assessment, any supervisory or regulatory action taken against the FinTech Operator, as well as any publically available information as to any questionable activities/business practices undertaken.

This should not only be done when considering whether to establish a business relationship with a FinTech Operator but on an on-going basis throughout the said relationship. Where the Institution becomes aware of any such information following the establishment of the business relationship, the Institution should review its customer risk assessment to

determine whether the said information has any influence on the customer's risk assessment.

In addition, it is to be noted that FinTech Operators may either be subject to a regulatory requirement to carry out periodical reviews and audits of their compliance with the AML/CFT framework, or they may choose to do so out of their own free will. Where such audit or review is carried out, Institutions may, on a risk-sensitive basis, consider requesting copies of the same to better understand how the said operator is seeking to mitigate any ML/FT risk it is exposed to and the adequacy of the measures taken to do so.

Notwithstanding the above, the Institution should also appreciate the sensitivity of any such review or audit and that there is no obligation on the FinTech operator to disclose the same.

G2-2.2.2.2 *Activities*

G2-2.2.2.2.1 In order to understand the activity of the FinTech Operator, Institutions should obtain, from the FinTech Operator:

- i. a detailed description of the organisational setup and proposed activities of the FinTech Operator. This should inter alia include:
 - a. information on the business activity including the volume of business which the FinTech Operator has or is projecting to have, and the value and volume of activity that will be transacted using the products and services to be provided; and
 - b. an organisational chart listing at least the key individuals, and where such individuals will be based;
- ii. a confirmation from the FinTech Operator as to whether the Operator will have substance in Malta and whether it will be operating in or from Malta;
- iii. where a FinTech Operator is undertaking or intends to undertake activities in other jurisdictions, a list of the jurisdictions where the Operator is/will be undertaking its activity, and a declaration from the FinTech Operator's Board that the Operator will comply with the applicable laws of the respective jurisdiction/s; and

- iv. a declaration from the FinTech Operator that they have assessed the risks involved in their business and that they have taken appropriate measures to mitigate such risks:
- G2-2.2.2.2.2 Information collected pursuant to point (i) of G2-2.2.2.2.1 will allow the subject person to better perform its risk assessment, as the volume, frequency and value of transactions to be undertaken will inevitably influence risk, and will allow it to effectively carry out on-going monitoring and detect any unusual variations in activity which would merit further consideration.
- G2-2.2.2.2.3 Information collected pursuant to point (iii) of G2-2.2.2.2.1 will provide the Institution with the geographical location/s of where funds will be effectively generated. The higher the risks associated with these jurisdictions the higher the risk of ML/FT that it will be exposed to.
- G2-2.2.2.2.4 Notwithstanding G2-2.2.2.2.1, the Institution may supplement or substantiate any information obtained through publically available information and/or financial statements, where these are available.
- G2-2.2.2.2.5 In addition, the nature and extent of the activities carried out by the FinTech operator may also be of assistance when considering source of wealth and source of funds requirements. The said requirements should be understood and construed in terms and as provided for by the Implementing Procedures - Part I.
- G2-2.2.2.3 *Use of Technology*
- G2-2.2.2.3.1 Whilst it is not expected for a subject person to understand all the different forms of technology that may be used to provide financial services and/or products, it is also true that risk assessing prospective areas of activity or customers would require an understanding of the same.
- G2-2.2.2.3.2 In assessing this risk, Institutions should, at least, consider:
- i. whether the technology being used was subject to any systems audit; and
 - ii. the background of individuals responsible for the development and implementation of the technology.
- G2-2.2.2.3.3 Information collected pursuant to point (i) of G2-2.2.2.3.2 would indicate whether the technology was audited (voluntarily or as part of an authorisation process) or otherwise. To the extent that the systems audit

concludes that the technology used can actually deliver what the customer states, the risk from the technological side would be considered to be low.

- G2-2.2.2.3.4 Pursuant to point (ii) of G2-2.2.2.3.2, having individuals involved in the FinTech with expertise in both technology and financial services should provide additional comfort as to the technology's reliability. Information thereon may be obtained from the FinTech Operator or from public sources.
- G2-2.2.3 Institutions should oblige FinTechs to notify them of any material changes to any of the information submitted to them.
- G2-2.2.4 Institutions are reminded of their obligations under Regulation 5(5)(e) of the PMLFTR in terms of which they are to 'provide employees from time to time with training in the recognition and handling of operations and transactions which may be related to proceeds of criminal activity, money laundering or the funding of terrorism.' In this light Institutions are to provide their employees with training in relation to FinTech related activities.

Section 3 *Supplementary Guidance for Credit Institutions, Payment Institutions and Electronic Money Institutions opening accounts for DLT Exchanges*

- G2-2.3.1 In view of the particular nature of DLT Exchanges, additional guidance is being provided as to the sources of information that can be used to better understand their activities. Further to Section 2 above, where the FinTech in question is a DLT Exchange, Institutions should ensure that they are also provided with details on:
- i. the DLT Exchange's operational set-up, including its custodial arrangements and whether it is a centralised or decentralised exchange; and
 - ii. whether the DLT Exchange is linked to other exchanges; and
 - iii. a copy of the bye-laws of the DLT Exchange. Obtaining a copy of the bye-laws of the DLT Exchange can also provide Institutions with relevant information on the activities carried out by the said exchange as this document may explain which assets are admitted to trading and under what conditions, as well as who and under what conditions is allowed to trade on the same. Understanding the potential composition of the DLT Exchange's customer-base as well as how trading on the same is to take place should allow Institutions

to better understand and appreciate the ML/FT risks arising from servicing such an operator.

Title 3 Supplementary guidance for Credit Institutions, Payment Institutions and Electronic Money Institutions opening accounts for Issuers of DLT Assets

Section 1 Scope and Application

G2-3.1.1 Section 2 of this Title provides supplementary guidance for Institutions opening accounts for FinTechs, specifically those Issuers offering their DLT Assets either to the public or through private placements, whereas Section 3 provides supplementary guidance for Institutions opening accounts for Issuers of DLT Assets raising funds in DLT Assets, in whole or in part.

Section 2 Supplementary Guidance for Credit Institutions, Payment Institutions and Electronic Money Institutions opening accounts for Issuers of DLT Assets

G2-3.2.1 Pursuant and further to G2-2.2.2, in assessing the risk presented by the customer's activities, Institutions should *inter alia* consider the following:

- i. Regulatory Status – apart from the regulatory status of the Issuer, Institutions should also consider what is the status of the market on which the assets may be traded and the extent of disclosure obligations that any such listing entails;
- ii. The nature and features of the DLT Asset being offered. Certain features may render a DLT Asset riskier from a ML/FT point of view;
- iii. Target investors – issuers may target specific investor categories and/or specific jurisdictions. These aspects, together with any capping that may be applicable to each single investor, will also influence the ML/FT risk associated with the issue;
- iv. Reliability of the Issue and of the project financed through the Issue – subject persons should consider what the funds collected through the issue of DLT Assets are to be used for;
- v. Technology used – As already highlighted in G2-2.2.2.3, the technology used may present additional risks to the subject person.

G2-3.2.2 Further to G2-2.2.2 and to the extent that may be applicable in the case of the specific issue, Institutions should therefore seek to obtain the following information:

- i. the details of the functionaries appointed by the Issuer;
- ii. financial projections;
- iii. how funds will be refunded to investors in the event that an offering is cancelled for any reason whatsoever as per the applicable legislation;
- iv. declarations from the Issuer:
 - a. on how they intend to use the proceeds of the offering;
 - b. that the Issuer is aware of its regulatory obligations under the applicable regulatory framework; and
 - c. that the Issuer is aware of its obligations as a subject person under the PMLFTR;
- v. Further to point (iv) (c) above, a description of the systems which the Issuer has in place to satisfy any applicable AML/CFT requirements:

This information may *inter alia* be obtained by obtaining a copy of the admission document (whitepaper or prospectus, as applicable), drawn up in accordance with the applicable regulatory framework, as soon as this is available.

G2-3.2.3 Further to G2-3.2.1, the information collected in terms of G2-3.2.2 will also assist the subject person when:

- i. Establishing the nature and purpose of the business relationship; and
- ii. Carrying out ongoing monitoring

G2-3.2.4 In carrying out their ongoing monitoring obligations, Institutions should follow any updates published by the Issuer and which may have a bearing on the risk assessment of the business relationship, and may consider requesting the said Issuer to provide any information with respect to the project financed through the issue as they may deem necessary.

Section 3 ***Further Supplementary Guidance for Credit Institutions, Payment Institutions and Electronic Money Institutions opening accounts for Issuers of DLT Assets raising funds in DLT Assets***

G2-3.3.1 Further to Section 2 of this Title, G2-5.2.2 and G2-5.2.3 should also be considered in the case of Institutions opening accounts for Issuers of DLT Assets raising funds in DLT Assets, in whole or in part.

Title 4 Supplementary guidance for Credit Institutions, Payment Institutions and Electronic Money Institutions opening accounts for FinTechs, specifically those which are authorised or seeking to be authorised, by the MFSA, as VFA Service Providers

Section 1 Scope and Application

G2-4.1.1 Section 2 of this title provides supplementary guidance for Institutions opening accounts for FinTechs, specifically those which are authorised or seeking to be authorised, by the MFSA, as VFA service providers.

This notwithstanding, Institutions opening accounts for FinTechs providing services equivalent to VFA services (not provided in or from Malta) should refer to Title 2 of this Guidance and consider whether any of the following may also be applicable thereto.

Section 2 Supplementary Guidance for Credit Institutions, Payment Institutions and Electronic Money Institutions opening accounts for FinTechs which are authorised or seeking to be authorised by the MFSA

G2-4.2.1 Pursuant and further to G2-2.2.2, in assessing the risk presented by the customer's activities, Institutions should also consider the following:

- i. The VFAs that the service provider is willing to deal/transact in – some VFAs have features which increase the risk associated therewith;
- ii. The dependence on other VFA service providers in the course of providing the service/s for which it is licenced – where reliance is made on third parties this will inevitably also impact the service provider's overall risk.

G2-4.2.2 Further to G2-2.2.2, Institutions should therefore seek to obtain the following information:

- i. details of any material outsourcing arrangements entered into by the FinTech Operator;

- ii. financial projections;
- iii. details of services provided/to be provided by the FinTech Operator;
- iv. a list of VFA Assets the FinTech Operator provides/will provide services in relation thereto;
- v. where the FinTech Operator holds clients' monies or assets, details of the arrangements it has in this regard, particularly the reconciliations being conducted and the frequency thereof;
- vi. declarations from the FinTech Operator:
 - a. that the FinTech Operator is aware of its regulatory obligations under the applicable regulatory framework; and
 - b. that the FinTech Operator is aware of its obligations as a subject person under the PMLFTR; and
- vii. Further to point (vi) (b) above, a description of the systems which the FinTech Operator has in place to satisfy the applicable AML/CFT requirements.

Title 5 Guidance for Credit Institutions, Payment Institutions and Electronic Money Institutions opening accounts for FinTechs accepting DLT Assets as a means of payment

Section 1 Scope and Application

G2-5.1.1 This Title provides guidance for Institutions opening accounts for FinTechs accepting DLT Assets as a means of payment.

Section 2 Guidance for Credit Institutions, Payment Institutions and Electronic Money Institutions opening accounts for FinTechs accepting DLT Assets as a means of payment

G2-5.2.1 Pursuant to the VFA Act, and in line with the MFSA's policy that VFA business should be segregated from traditional financial services activity, accounts opened by Credit Institutions, Payment Institutions and Electronic Money Institutions for FinTechs accepting DLT Assets as a means of payment, shall not directly receive or at any time hold any VFAs.

G2-5.2.2 Further to G2-2.2.2, in assessing the risk arising from the customer accepting DLT assets as a form of payment, institutions should *inter alia* base their risk assessment on points (i) to (vi) of G2-5.2.3.

G2-5.2.3 Pursuant to G2-2.2.2, where FinTech Operators accept DLT Assets as a means of payment, Credit Institutions, Payment Institutions and Electronic Money Institutions should *inter alia* seek information from the FinTech Operator on:

- i. any DLT Exchange being used by the FinTech Operator;
- ii. any custodian or wallet provider being used by the FinTech Operator;
- iii. whether the entities listed in points [i] and [ii] are licensed or otherwise authorised in Malta or in another jurisdiction;
- iv. whether the entities listed in points [i] and [ii] are subject to AML/CFT obligations;

- v. a list of the DLT Assets which are accepted by the FinTech Operator;
and
- vi. the frequency of conversion into fiat currencies of DLT Assets
accepted as a means of payment.

CONCLUDING REMARKS

This Guidance Document provides subject persons with additional guidance on how they can better determine the risks presented in the FinTech sector; however, subject persons are reminded that any risk assessment is not static and that changes that influence the result of the same may occur. In this light, subject persons are required to ensure that any information they obtain is kept updated. In addition, it must also be kept in mind that there are on-going monitoring obligations which need to be calibrated inter alia on the basis of the risks presented by a given customer. These obligations are equally applicable in the particular scenarios considered in this document.

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

MALTA FINANCIAL SERVICES AUTHORITY

NOTABILE ROAD, ATTARD, BKR 3000, MALTA.

COMMUNICATIONS@MFSA.COM.MT

+356 2144 1155

WWW.MFSA.COM.MT