Retail Payment Services and Card Schemes Regulation

نظام خدمات الدفع للتجزئة ومنظومات البطاقات

المحتويـــات
CONTENTS

Circular No.	**:**	**15/2021**	**تعميم رقم**	**:**	**2021\15**
Date	**:**	**06/06/2021**	**التاريخ**	**:**	**2021\06\06**
To	**:**	**Providers of Retail Payment Services and Card Schemes in the United Arab Emirates**	**إلى**	**:**	**مقدمي خدمات الدفع للتجزئة ومنظومات البطاقات في الإمارات العربية المتحدة**
Subject	**:**	**Retail Payment Services and Card Schemes Regulation**	**الموضوع**	**:**	**نظام خدمات الدفع للتجزئة ومنظومات البطاقات**

Introduction

The Regulation ('RPSCS Regulation') lays down the rules and conditions established by the Central Bank for granting a License for the provision of Retail Payment Services. The Retail Payment Services are digital payment services in the State and comprise nine categories, namely Payment Account Issuance Services, Payment Instrument Issuance Services, Merchant Acquiring Services, Payment Aggregation Services, Domestic and Cross-border Fund Transfer Services, Payment Token Services, Payment Initiation Services and Payment Account Information Services. It also requires Card Schemes to obtain a License from the Central Bank and sets out the conditions for granting such License as well as the ongoing obligations of Card Schemes. The Central Bank has furthermore been given the right to receive information on the fees and charges of Card Schemes, and regulate such fees and charges if the Central Bank considers it appropriate. In addition, proper contractual arrangements are required between Banks or other Payment Service Providers providing Payment Account Issuance Services, on one hand, and Payment Service Providers providing Payment Initiation and Payment Account Information Services, on the other hand. Payment Service Providers wishing to participate in wages distribution and be given access to the Wages Protection System are subject to a set of on-going requirements.

The Central Bank Law requires providing money transfer services, electronic retail payments, and digital money services to be subject to a licensing regime administered by the Central Bank and

المقدمة

يتناول النظام ("نظام خدمات الدفع للتجزئة ومنظومات البطاقات") القواعد والشروط الصادرة عن المصرف المركزي لمنح ترخيص تقديم خدمات الدفع للتجزئة. خدمات الدفع للتجزئة هي خدمات دفع رقمية في الدولة وتتضمن تسع فئات، وهي خدمات إصدار حساب الدفع، خدمات إصدار أداة الدفع، خدمات تحصيل المعاملات، خدمات تجميع الدفع، خدمات تحويل الأموال محلياً وعبر الحدود، خدمات رمز الدفع، خدمات إنشاء الدفع وخدمات معلومات حساب الدفع. يفرض هذا النظام على منظومات البطاقات الحصول على ترخيص من المصرف المركزي ويحدد شروط الحصول على الترخيص والالتزامات المستمرة لمنظومات البطاقات. للمصرف المركزي أيضاً تلقي المعلومات حول رسوم ومصاريف منظومات البطاقات، وتنظيم ومراقبة هذه الرسوم والمصاريف عند الضرورة. إضافةً لما تقدم، يلزم وجود ترتيبات تعاقدية مناسبة بين البنوك أو مقدمي خدمات الدفع الآخرين الذين يقدمون خدمات إصدار حساب الدفع من جهة، ومقدمي خدمات الدفع الذين يقدمون خدمات إنشاء الدفع وخدمات معلومات حساب الدفع من جهة أخرى. يخضع مقدمو خدمات الدفع الراغبين في المشاركة في صرف الأجور وإمكانية الوصول إلى نظام حماية الأجور لمجموعة من المتطلبات المستمرة.

يتطلب قانون المصرف المركزي إخضاع خدمات تحويل الأموال، خدمات مدفوعات التجزئة الإلكترونية وخدمات الأموال الرقمية لنظام الترخيص المدار من قبل المصرف

provides the statutory basis for the powers of the Central Bank in relation to the licensing and ongoing supervision of Payment Service Providers and Card Schemes.

المركزي، ويحدد الأساس القانوني لصلاحيات المصرف المركزي فيما يتعلق بالترخيص والإشراف المستمر على مقدمي خدمات الدفع ومنظومات البطاقات.

Scope and Objectives

نطاق تطبيق النظام وأهدافه

This Regulation sets out the requirements concerning:

يحدد هذا النظام المتطلبات المتعلقة بما يلي:

- conditions for granting and maintaining a License for the provision of Retail Payment Services;
- شروط منح والحفاظ على ترخيص تقديم خدمات الدفع للتجزئة؛
- rights and obligations of Retail Payment Service Users and Payment Service Providers;
- حقوق والتزامات مستخدمي خدمات الدفع للتجزئة ومقدمي خدمات الدفع؛
- proper contractual arrangements allowing Payment Service Providers providing Payment Initiation and Payment Account Information Services to access Payment Accounts held with Banks and other Payment Service Providers providing Payment Account Issuance Services;
- الترتيبات التعاقدية المناسبة التي تسمح لمقدمي خدمات الدفع الذين يقدمون خدمات إنشاء الدفع وخدمات معلومات حساب الدفع الوصول الى حسابات الدفع لدى البنوك ومقدمي خدمات الدفع الآخرين الذين يقدمون خدمات إصدار حسابات الدفع؛
- conditions for granting a License to Card Schemes;
- شروط الحصول على ترخيص منظومات البطاقات؛
- conditions for participating and obtaining an access to the Wages Protection System;
- شروط المشاركة والحصول على حق الوصول الى نظام حماية الأجور؛
- powers of the Central Bank with regard to the supervision of Payment Service Providers and the on-going reporting requirements for Card Schemes.
- صلاحيات المصرف المركزي في الرقابة على مقدمي خدمات الدفع والمتطلبات المستمرة لرفع التقارير الخاصة بمنظومات البطاقات.

In exercising its powers and functions under this Regulation, the Central Bank has regard to the following objectives:

يراعي المصرف المركزي، في إطار ممارسة صلاحياته ومهامه المنصوص عليها ضمن هذا النظام، تحقيق الأغراض التالية:

- ensuring the safety, soundness and efficiency of Retail Payment Services;
- ضمان سلامة، وصحة وكفاءة خدمات الدفع للتجزئة؛

- adoption of effective and risk-based licensing requirements for Payment Service Providers;
- promoting the reliability and efficiency of Card Schemes as well as public confidence in Card-based Payment Transactions;
- promoting innovation and creating a level playing field for market participants; and
- reinforcing the UAE's status as a leading payment hub in the region.

- اعتماد متطلبات ترخيص فعالة وقائمة على المخاطر لمقدمي خدمات الدفع؛
- تعزيز موثوقية وكفاءة منظومات البطاقات وثقة الجمهور في معاملات الدفع بواسطة البطاقات؛
- تشجيع الابتكار وخلق فرص متكافئة للمشاركين في السوق؛ و
- تعزيز مكانة دولة الإمارات العربية المتحدة كمحور رائد في تقديم خدمات الدفع في المنطقة.

Exclusions

الاستثناءات

This Regulation shall not apply to the following:

لا يسري هذا النظام على ما يلي:

1. Payment Transactions involving Stored Value Facilities;
1. معاملات الدفع التي تتضمن تسهيلات القيم المخزنة؛
2. Transactions involving Commodity or Security Tokens;
2. المعاملات التي تتضمن رموز السلع والأوراق المالية؛
3. Transactions involving Virtual Asset Tokens;
3. المعاملات التي تتضمن رموز الأصول الافتراضية؛
4. Payment Transactions involving Remittances;
4. معاملات الدفع التي تتضمن التحويلات؛
5. Currency exchange operations where the funds are not held on a Payment Account;
5. عمليات صرف العملات التي لا يتم فيها الاحتفاظ بالأموال في حساب الدفع؛
6. Any service other than Payment Initiation and Payment Account Information Service, including (but not limited to) any of the following:
6. أي خدمات أخرى ما عدا خدمات إنشاء الدفع وخدمات معلومات حساب الدفع، بما في ذلك، على سبيل المثال لا الحصر، ما يلي:
   6.1. services, provided by any technical service provider that supports the provision of any payment service, but does not at any time enter into possession of any money under that payment service;
   6.1 الخدمات، التي يقدمها أي مقدم خدمة فنية لدعم توفير أي خدمة دفع، دون أن تدخل أي من الأموال موضوع خدمة الدفع هذه في أي وقت في حيازته؛
   6.2. the service of processing or storing data;
   6.2 خدمة معالجة أو تخزين البيانات؛

6.3. any information technology security, trust or privacy protection service;	6.3 أي خدمة خاصة بأمن التكنولوجيا، أو العهد المالية أو حماية الخصوصية؛
6.4. any data or entity authentication service;	6.4 أي خدمة مصادقة أو تحقق خاصة بالبيانات أو المنشآت؛
6.5. any information technology service;	6.5 أي خدمة خاصة بتكنولوجيا المعلومات؛
6.6. the service of providing a communication network; and	6.6 خدمة توفير شبكة إتصال؛ و
6.7. the service of providing and maintaining any terminal or device used for any payment service.	6.7 خدمة توفير وصيانة أي محطة أو جهاز يستخدم لأي خدمة دفع.
7. Payment Transactions carried out within a payment system or securities settlement system between Payment Service Providers and settlement agents, central counterparties, clearing houses, central banks or other participants in such system including central securities depositories;	7. معاملات الدفع التي تتم ضمن نظام دفع أو نظام تسوية أوراق مالية بين مقدمي خدمات الدفع ووكلاء التسوية، الوسطاء المركزيين للتسوية، غرف المقاصة، المصارف المركزية أو المشاركين الآخرين في هذا النظام بما في ذلك نظم الإيداع المركزية للأوراق المالية؛
8. Payment Transactions and related services between a parent undertaking and its subsidiary or between subsidiaries of the same parent undertaking, without any intermediary intervention by a Payment Service Provider other than an undertaking belonging to the same group; and	8. معاملات الدفع والخدمات ذات الصلة فيما بين الشركة الأم والشركات التابعة لها أو فيما الشركات التابعة للشركة الأم نفسها، دون أي تدخل وسيط من مقدم خدمات الدفع فيما عدا التعهد الخاص بالمجموعة نفسها؛ و
9. Any other relevant activity that may be designated by the Central Bank.	9. أي نشاط آخر ذات صلة قد يحدده المصرف المركزي.

Article (1): Definitions

المادة (1): تعريفات

1. **Agent:** means a juridical Person providing Retail Payment Services on behalf of a Payment Service Provider.

1. **الوكيل:** يعني الشخص الاعتباري الذي يتولى تقديم خدمات الدفع للتجزئة نيابةً عن مقدم خدمات الدفع.

2. **AML/CFT:** means Anti-Money Laundering and Combating the Financing of Terrorism.

2. **مواجهة غسل الأموال ومكافحة تمويل الإرهاب:** يعني مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب.

3. **AML Law:** means Decree Federal Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations and Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Federal Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations, as may be amended from time to time, and any instructions, guidelines and notices issued by the Central Bank relating to their implementation or issued in this regard.

3. **قانون مواجهة غسل الأموال:** يعني المرسوم بقانون اتحادي رقم (20) لسنة 2018 في شأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة وقرار مجلس الوزراء رقم (10) لسنة 2019 بشأن اللائحة التنفيذية للمرسوم بقانون إتحادي رقم (20) لسنة 2018 في شأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة، والتعديلات التي قد تطرأ عليها من وقتٍ لآخر، وأية تعليمات ومبادئ توجيهية وإشعارات صادرة عن المصرف المركزي حول تنفيذها أو صادرة في هذا الشأن.

4. **Annex I:** means the list of Retail Payment Services that a Payment Service Provider may provide subject to the requirements of this Regulation.

4. **الملحق 1:** يعني قائمة خدمات الدفع للتجزئة التي يجوز لمقدم خدمات الدفع تقديمها وفق متطلبات هذا النظام.

5. **Annex II:** means the Guidance on the best practices for technology risk and information security.

5. **الملحق 2:** يعني الإرشادات حول أفضل الممارسات الخاصة بمخاطر التكنولوجيا وأمن المعلومات.

6. **Annex III:** means the minimum level of information to be reported by Card Schemes to the Central Bank.

6. **المحلق 3:** يعني الحد الأدنى من المعلومات الواجب على منظومات البطاقات إبلاغها للمصرف المركزي.

7. **Applicant:** means a juridical Person duly incorporated in the State in accordance with Federal Law No. 2 of 2015 on Commercial Companies and as provided for under Article (74) of the Central Bank Law, which files an Application with the Central Bank for the granting of a License for the provision of one or more Retail Payment Services, operation of a Card Scheme or the modification of the scope of a granted License.

7. **مقدم الطلب:** يعني شخص اعتباري مؤسس في الدولة وفقاً للقانون الاتحادي رقم (2) لسنة 2015 بشأن الشركات التجارية، وطبقاً للمادة (74) من قانون المصرف المركزي، الذي يتقدم بطلب الى المصرف المركزي للحصول على ترخيص لتقديم خدمة أو أكثر من خدمات الدفع للتجزئة، تشغيل منظومة البطاقات أو تعديل نطاق الترخيص الممنوح له.

8. **Application:** means a written request for obtaining a License for the provision of one or more Retail Payment Services submitted by an Applicant which contains the information and documents specified in this Regulation or by the Central Bank, and is in the form specified by the Central Bank's Licensing Division, including a written request for obtaining a modification to the scope of a granted License.

8. **طلب الترخيص:** يعني الطلب الخطي للحصول على ترخيص لتقديم واحدة أو أكثر من خدمات الدفع للتجزئة المقدم من مقدم الطلب الذي يضم المعلومات والمستندات المنصوص عليها في هذا النظام أو المحددة من المصرف المركزي، حسب الاستمارة الصادرة عن قسم الترخيص في المصرف المركزي، بما في ذلك الطلب الخطي للحصول على تعديل لنطاق الترخيص الممنوح له.

9. **Auditor:** means an independent juridical Person that has been appointed to audit the accounts and financial statements of a Payment Service Provider in accordance with Article (10) (7).

9. **المدقق:** يعني الشخص الاعتباري المستقل المعين لتدقيق الحسابات والقوائم المالية لمقدم خدمات الدفع وفقاً للبند (7) من المادة (10) من هذا النظام.

10. **Bank:** any juridical person licensed in accordance with the provisions of the Central Bank Law, to primarily carry on the activity of taking deposits, and any other Licensed Financial Activities.

10. **البنك:** يعني أي شخص اعتباري مرخص له وفقًا لأحكام قانون المصرف المركزي بممارسة نشاط تلقي الودائع بشكل رئيسي وأي من الأنشطة المالية المرخصة الأخرى.

11. **Beneficial Owner:** means the natural person who owns or exercises effective ultimate control, directly or indirectly, over a Retail Payment Service User (client) or the natural person on whose behalf a transaction is being conducted or, the natural person who exercises effective ultimate control over a legal person or legal arrangement.

11. **المستفيد الحقيقي:** يعني الشخص الطبيعي الذي يمتلك أو يمارس سيطرة فعلية نهائية، مباشرة أو غير مباشرة، على مستخدم خدمات الدفع للتجزئة (العميل) أو الشخص الطبيعي الذي تجري المعاملة نيابةً عنه أو الذي يمارس سيطرة فعلية نهائية على شخص اعتباري أو ترتيب قانوني.

12. **Branded:** means having any digital name, term, sign, logo, symbol or combination thereof that is capable of differentiating the Card Scheme under which Payment Transactions are executed.

12. **حامل علامة تجارية:** يعني الحائز على أي اسم رقمي أو مصطلح أو علامة أو شعار أو رمز أو مجموعة منها التي من شأنها تمييز منظومة البطاقات التي يتم بموجبها تنفيذ معاملات الدفع.

13. **Board:** means the board of directors of an Applicant, Payment Service Provider or a Card Scheme in accordance with applicable corporate law.

13. **المجلس:** يعني مجلس إدارة مقدم الطلب أو مقدم خدمات الدفع أو منظومة البطاقات وفقاً لأحكام قانون الشركات المعمول به.

14. **Business Day:** means a day other than Friday, Saturday, public holiday or other non-working holiday or day in the State.

14. **يوم عمل:** يعني أي يوم ما عدا الجمعة أو السبت أو أيام العطل الرسمية أو أيام العطل الأخرى أو الأيام غير المخصصة للعمل في الدولة.

15. **Card-based Payment Transactions:** means a service based on a Card Scheme's infrastructure and business rules to make Payment Transactions by means of any card, telecommunication, digital or IT device or software if this results in a debit or a credit card transaction.

15. **معاملات الدفع بواسطة البطاقة:** تعني خدمة تستند إلى البنية التحتية لمنظومة البطاقات وقواعد العمل الخاصة بتنفيذ معاملات الدفع بواسطة أي بطاقة، جهاز اتصالات، جهاز رقمي، جهاز أو برنامج تكنولوجيا المعلومات إذا نتج عن ذلك معاملة على بطاقة خصم أو ائتمان.

16. **Card Issuer:** means a category of Payment Service Provider providing a Payer with a Payment Instrument to initiate and process the Payer's Card-based Payment Transactions.

16. **مُصدر البطاقة:** يعني فئة من مقدمي خدمات الدفع تزود الدافع بأداة دفع لمباشرة ومعالجة معاملات الدفع بواسطة البطاقة الخاصة بالدافع.

17. **Cardholder:** means a Person who holds a Payment Instrument, physical or otherwise, issued by a Card Issuer based on a contract for the provision of an electronic payment instrument.

17. **حامل البطاقة:** يعني الشخص الذي يحمل أداة دفع، مادية أو غير ذلك، صادرة عن مُصدر البطاقة بناءً على عقد تقديم أداة دفع إلكترونية.

18. **Card Scheme:** means a single set of rules, practices and standards that enable a holder of a Payment Instrument to effect the execution of Card-based Payment Transactions within the State which is separated from any infrastructure of payment system that supports its operation, and includes the Card Scheme Governing Body. For the avoidance of doubt, a Card Scheme may be operated by a private or Public Sector Entity.

18. **منظومة البطاقات:** تعني مجموعة من القواعد والممارسات والمعايير التي تمكن حامل أداة دفع من القيام بمعاملات الدفع بواسطة البطاقة داخل الدولة بشكل منفصل عن أي بنية تحتية لنظام الدفع الذي يدعم تشغيلها، وتتضمن الكيان المسؤول عن إدارة منظومة البطاقات. ولتجنب الشك، من الممكن تشغيل منظومة البطاقات من قبل كيان تابع للقطاع خاص أو هيئات القطاع العام على حدٍ سواء.

19. **Card Scheme License:** means a License for operating as a Card Scheme, as referred to in Article (18).

19. **ترخيص منظومة البطاقات:** يعني ترخيص تشغيل منظومة بطاقات وفقاً لما تم الإشارة إليه في المادة (18) من النظام.

20. **Card Scheme Governing Body:** means the juridical Person responsible and/or accountable for the functioning and operation of a Card Scheme.

20. **الكيان المسؤول عن إدارة منظومة البطاقات:** يعني الشخص الاعتباري الذي يتولى و/أو يكون مسؤولاً عن عمل وتشغيل منظومة بطاقات.

21. **Category I License:** means a License for the provision of the Retail Payment Services referred to in Article (3) (2).

21. **ترخيص الفئة الأولى:** يعني ترخيص تقديم خدمات الدفع للتجزئة المشار إليها في البند (2) من المادة (3).

22. **Category II License** means a License for the provision of the Retail Payment Services referred to in Article (3) (3).

22. **ترخيص الفئة الثانية:** يعني ترخيص تقديم خدمات الدفع للتجزئة المشار إليها في البند (3) من المادة (3).

23. **ترخيص الفئة الثالثة:** يعني ترخيص تقديم خدمات الدفع للتجزئة المشار إليها في البند (4) من المادة (3).

23. **Category III License** means a License for the provision of the Retail Payment Services referred to in Article (3) (4).

24. **ترخيص الفئة الرابعة:** يعني ترخيص تقديم خدمات الدفع للتجزئة المشار إليها في البند (5) من المادة (3).

24. **Category IV License** means a License for the provision of the Retail Payment Services referred to in Article (3) (5).

25. **المصرف المركزي:** يعني مصرف الإمارات العربية المتحدة المركزي.

25. **Central Bank:** means the Central Bank of the United Arab Emirates.

26. **قانون المصرف المركزي:** يعني المرسوم بقانون اتحادي رقم (14) لسنة 2018 في شأن المصرف المركزي وتنظيم المنشآت والأنشطة المالية، وأي تعديل أو استبدال قد يطرأ عليه من حين لآخر.

26. **Central Bank Law:** means the Decretal Federal Law No. (14) of 2018 Regarding the Central Bank and Organization of Financial Institutions and Services, as may be amended or substituted from time to time.

27. **علامة تجارية مشتركة:** تعني تضمين علامة تجارية للدفع واحدة على الأقل وعلامة تجارية غير متعلقة بالدفع في وسيلة الدفع نفسها.

27. **Co-Branded:** means having the inclusion of at least one payment brand and one non-payment brand on the same Payment Instrument.

28. **المسيطر:** يعني الشخص الطبيعي أو الاعتباري الذي يملك بمفرده أو مع شركائه نسبة 20٪ على الأقل من أسهم أحد مقدمي خدمات الدفع أو الذي هو في وضع يجيز له بالتحكم بنسبة 20٪ على الأقل من الأصوات الخاصة بأحد مقدمي خدمات الدفع.

28. **Controller:** means a natural or juridical Person that alone or together with the Person's associates has an interest in at least 20% of the shares in a Payment Service Providers or is in a position to control at least 20% of the votes in a Payment Service Provider.

29. **رمز السلع:** يعني نوعًا من الأصول المشفرة الذي يمنح حامله حق الوصول إلى منتج أو خدمة حالية أو مستقبلية، ولا يقبله إلا مُصدر ذلك الرمز. ويمكن أيضا الإشارة إليه كـ "رمز خدمة أو خدمات"

29. **Commodity Token**: means a type of Crypto-Asset that grants its holder an access to a current or prospective product or service, and is only accepted by the issuer of that token. Commodity token can also be referred to as utility token

30. **الشكوى:** تعني تعبير شفهي أو خطي عن عدم رضا العميل عن منتج، خدمة، إجراء، سياسة أو أفعال من قبل المنشأة المالية المرخصة والتي يتم تقديمها إما خطياً أو شفهياً إلى موظف في المنشأة المالية المرخصة.

30. **Complaint:** Means an expression of dissatisfaction by a consumer with a product, service, policy, procedure or actions by the licensed financial institution that is presented to an Employee of the licensed financial institution in writing or verbally.

31. **خدمة تحويل الأموال عبر الحدود:** تعني خدمة دفع للتجزئة لتحويل الأموال حيث يكون مقدمي خدمات الدفع الخاصين بالدافع والمدفوع له موجودين في مناطق اختصاص أو دول مختلفة.

31. **Cross-Border Fund Transfer Service:** means a Retail Payment Service for the transfer of funds in which the Payment Service Providers of the Payer and the Payee are located in different jurisdictions/countries.

32. **الأصول المشفرة:** تعني التمثيل الرقمي المشفر للقيمة أو الحقوق التعاقدية التي تستخدم تكنولوجيا الدفاتر الموزعة والتي يمكن تحويلها، تخزينها أو تداولها إلكترونياً.

32. **Crypto-Assets:** means cryptographically secured digital representations of value or contractual rights that use a form of Distributed Ledger Technology and can be transferred, stored or traded electronically.

33. **العناية الواجبة تجاه العملاء:** تعني عملية التعرف أو التحقق من معلومات مستخدم خدمات الدفع للتجزئة أو المستفيد الحقيقي، سواء كان شخصاً طبيعياً أو اعتبارياً أو ترتيباً قانونياً، وطبيعة عمله والغرض من علاقة العمل وهيكل الملكية والسيطرة عليه.

33. **Customer Due Diligence or CDD:** means the process of identifying or verifying the information of a Retail Payment Service User or Beneficial Owner, whether a natural or legal person or a legal arrangement, and the nature of its activity and the purpose of the business relationship and the ownership structure and control over it.

34. **خدمات أمين الحفظ:** تعني حفظ أو التحكم، نيابةً عن أطراف ثالثة، في رموز الدفع، ووسائل الوصول الى هذه الرموز، حيثما ينطبق ذلك في شكل مفاتيح تشفير خاصة.

34. **Custodian Services**: means the safekeeping or controlling, on behalf of third parties, of Payment Tokens, the means of access to such tokens, where applicable in the form of private cryptographic keys.

35. **خرق البيانات:** يعني اختراق نظام تكنولوجيا المعلومات حيث يشتبه في افصاح غير مصرح به، سرقة، تعديل أو إتلاف لبيانات حامل البطاقة أو مستخدم خدمات الدفع للتجزئة، ويكون من المحتمل أن يؤدي ذلك إلى خسارة لحامل البطاقة أو لمستخدم خدمات الدفع للتجزئة.

35. **Data Breach:** means an intrusion into an IT system where unauthorized disclosure or theft, modification or destruction of Cardholder or Retail Payment Service User data is suspected and such is likely to result in a loss for the Cardholder or Retail Payment Service User.

36. **الشخص موضوع البيانات:** يعني الشخص الطبيعي المحدد أو القابل للتحديد موضوع البيانات الشخصية.

36. **Data Subject:** means an identified or identifiable natural Person who is the subject of Personal Data.

37. **خدمات النقود الرقمية:** تعني، لأغراض هذا النظام، النشاط التجاري المتعلق بتقديم خدمات رموز الدفع.

37. **Digital Money Services:** means, for the purposes of this Regulation, the business activity related to the provision of Payment Token Services.

38. **تكنولوجيا الدفاتر الموزعة:** تعني فئة من التكنولوجيا التي تدعم التسجيل الموزع للبيانات المشفرة عبر الشبكة وهي نوع من قواعد البيانات اللامركزية التي يوجد منها نسخ متطابقة متعددة موزعة بين عدة مشاركين ويمكن الوصول إليها عبر مراكز ومواقع مختلفة، والتي يتم تحديثها بشكل متزامن بإجماع المشاركين، مما يلغي الحاجة إلى سلطة مركزية أو

38. **Distributed Ledger Technology:** means a class of technologies that supports the distributed recording of encrypted data across a network and which is a type of decentralized database of which there are multiple identical copies distributed among multiple participants and accessible across different sites and locations, and which are updated in a synchronized manner by consensus of the participants, eliminating the

need for a central authority or intermediary to process, validate or authenticate transactions or other types of data exchanges.

وسيط لمعالجة أو التحقق من صحة أو مصادقة المعاملات أو أنواع أخرى من تبادل البيانات.

39. **Domestic Fund Transfer Service:** means the Retail Payment Service of accepting money for the purpose of executing, or arranging for the execution of Payment Transactions between a Payer in the State and a Payee in the State.

39. **خدمة تحويل الأموال محلياً:** تعني خدمة دفع للتجزئة خاصة بقبول الأموال بغرض تنفيذ أو الترتيب لتنفيذ معاملات الدفع بين دافع في الدولة ومدفوع له في الدولة.

40. **Electronic Payment Service:** means any and each of the Retail Payment Services listed in points (1) to (4) and (8) to (9) of Annex I.

40. **خدمة الدفع الالكتروني:** تعني كامل وأي من خدمات الدفع للتجزئة المدرجة ضمن البنود (1) الى (4) و(8) الى (9) من المحلق 1.

41. **Employer:** means a Person using the Wages Protection System for the payment of wages.

41. **صاحب العمل:** يعني الشخص الذي يستخدم نظام حماية الأجور لدفع الأجور.

42. **Exchange House:** means an exchange business that has been licensed under the Regulations re Licensing and Monitoring of Exchange Business.

42. **الصرافة:** تعني أعمال الصرافة التي تم ترخيصها بموجب نظام ترخيص ومراقبة أعمال الصرافة.

43. **Exempted Person:** means any Person who is exempted from the requirement to hold a License as per Article (2) of this Regulation.

43. **الشخص المعفى:** يعني أي شخص معفى من شرط الحصول على ترخيص بموجب المادة (2) من هذا النظام.

44. **Facilitating the Exchange of Payment Tokens:** means a Retail Payment Service related to establishing or operating a Payment Token exchange, in a case where the person that establishes or operates that exchange, for the purposes of an offer or invitation made or to be made on that Payment Token exchange, to buy or sell any Payment Token in exchange for Fiat Currency or Payment Token, whether of the same or a different type, comes into possession of any Fiat Currency or Payment Token, whether at the time that offer or invitation is made or otherwise.

44. **تسهيل تداول رموز الدفع:** يعني خدمة الدفع للتجزئة المتعلقة بإنشاء أو تشغيل تداول رموز الدفع، في حال حيازة الشخص، الذي يُنشئ هذا التداول أو يُشغله، لأغراض عرض أو دعوة مقدمة أو ستقدم لتبادل رمز دفع معين لشراء أو بيع أي رمز دفع مقابل الأوراق النقدية أو رمز الدفع، سواء كان من نفس النوع أو من نوع مختلف، أي أوراق نقدية أو رمز دفع، سواء في وقت صدور ذلك العرض أو الدعوة أو غير ذلك.

45. **FATF:** an inter-government body which sets international standards that aim to prevent global money laundering and terrorist financing activities.

45. **مجموعة العمل المالي:** هيئة مستقلة متعددة الحكومات تضع معايير دولية تستهدف منع أنشطة غسل الأموال وتمويل الإرهاب في العالم.

46. **Fiat Currency:** means a currency that is controlled by the respective central bank, has the

46. **الأوراق النقدية:** تعني العملة الخاضعة لرقابة المصرف المركزي المعني، والتي لها قوة إبراء

status of legal tender and is required to be accepted within a given jurisdiction.

بموجب القانون والواجبة القبول في نطاق اختصاص معين.

47. **Financial Free Zones:** means free zones subject to the provisions of Federal Law No (8) of 2004, regarding Financial Free Zones, as may be amended or supplemented from time to time.

47. **المناطق الحرة المالية:** تعني المناطق الحرة الخاضعة لأحكام القانون الاتحادي رقم (8) لسنة 2004 في شأن المناطق الحرة المالية، والقوانين المعدلة أو المكملة له من وقت الى آخر.

48. **Four Party Card Scheme**: means a Card Scheme in which Card-based Payment Transactions are made from the payment account of a Payer to the payment account of a payee through the intermediation of the scheme, an issuer (on the payer's side) and an acquirer (on the Payee's side).

48. **منظومة بطاقات رباعية الأطراف:** تعني منظومة البطاقات الي تتم فيها معاملات الدفع بواسطة البطاقة من حساب الدفع الخاص بالدافع إلى حساب المدفوع له من خلال وساطة المنظومة، المصدر (من جانب الدافع) والمحصل (من جانب المدفوع له).

49. **Framework Agreement:** means a payment service agreement for the provision of Retail Payment Services which governs the future execution of individual and successive Payment Transactions and which may contain the terms and conditions for opening a Payment Account**.**

49. **الاتفاقية الإطارية:** تعني اتفاقية خدمة دفع لتوفير خدمات الدفع للتجزئة التي تحكم التنفيذ المستقبلي لمعاملات الدفع الفردية والمتتالية والتي قد تحتوي على شروط وأحكام فتح حساب دفع.

50. **Group:** means a corporate group which consists of a parent entity and its subsidiaries, and the entities in which the parent entity or its subsidiaries hold, directly or indirectly, 5% or more of the shares, or are otherwise linked by a joint venture relationship.

50. **المجموعة:** تعني مجموعة الشركات التي تتألف من الشركة الأم والشركات التابعة لها، والشركات التي تمتلك فيها الشركة الأم أو الشركات التابعة لها، بشكل مباشر أو غير مباشر، 5٪ أو أكثر من الأسهم، أو المرتبطة بطريقة أخرى من خلال علاقة تشاركية.

51. **Legal Form:** means the legal form of Applicants established in accordance with Article (74) of the Central Bank Law.

51. **الشكل القانوني:** يعني الشكل القانوني لمقدمي الطلب المعتمد وفقاً لأحكام المادة (74) من قانون المصرف المركزي.

52. **Level 2 Acts:** means any written act that may be adopted or issued by the Central Bank complementing the implementation of this Regulation, such as, without being limited to, rules, directives, decisions, instructions, notices, circulars, standards, and rulebooks.

52. **أحكام المستوى الثاني:** تعني الأحكام المكتوبة التي قد يعتمدها أو يصدرها المصرف المركزي لتكون مكملةً لتنفيذ هذا النظام، ومنها على سبيل المثال لا الحصر، القواعد، التوجيهات، القرارات، التعليمات، الإخطارات، التعاميم، المعايير وكتيبات القواعد.

53. **License:** means a License issued by the Central Bank to an Applicant to provide Retail Payment Services or operate a Card Scheme in the State.

53. **الترخيص:** يعني ترخيص صادر عن المصرف المركزي لمقدم الطلب لتقديم خدمات الدفع للتجزئة أو إدارة منظومة بطاقات في الدولة. ويبقى هذا

The License is valid unless it is withdrawn, suspended or revoked by the Central Bank.

الترخيص ساري المفعول، ما لم يقم المصرف المركزي بسحبه، تعليقه أو إلغائه.

54. **Licensed Financial Activities:** means the financial activities subject to Central Bank licensing and supervision, which are specified in Article (65) of the Central Bank Law.

54. **الأنشطة المالية المرخصة:** تعني الأنشطة المالية الخاضعة لترخيص ورقابة المصرف المركزي والمحددة في المادة (65) من قانون المصرف المركزي.

55. **Major Regulatory Requirement:** means any requirement of this Regulation or Level 2 Acts the violation of which is capable of compromising and/or negatively affecting the attainment of the Central Bank's objectives pursued under this Regulation, as determined at the discretion of the Central Bank.

55. **المتطلبات الرقابية الرئيسية:** تعني أي متطلبات محددة بموجب هذا النظام أو أحكام المستوى الثاني، يمكن أن تؤدي مخالفتها إلى التأثير سلبًا على تحقيق أهداف المصرف المركزي المنشودة بموجب هذا النظام، على النحو المحدد وفقًا لتقدير المصرف المركزي.

56. **Management:** means the Applicant, Payment Service Provider, Agent and Card Scheme's senior officers that are involved in the daily management, supervision and control of the business services of the entity, typically including the chief executive officer, his or her alternate(s) and each person directly reporting to that officer. The chief executive officer and his or her alternate(s) shall be a natural person who are ordinarily residing in the State whereas the remaining members of Management shall be based in the State unless the Central Bank allows otherwise.

56. **الإدارة:** تعني كبار موظفي مقدم الطلب، مقدم خدمات الدفع، الوكيل ومنظومة البطاقات الذين يشاركون في الإدارة اليومية، الإشراف والرقابة على خدمات الأعمال في المنشأة، وتضم عادةً الرئيس التنفيذي ونائبه (نوابه) وكل شخص يرفع تقاريره مباشرة إلى الرئيس التنفيذي. يجب أن يكون الرئيس التنفيذي ونائبه (نوابه) أشخاصاً طبيعيين مقيمين عادةً في الدولة، في حين أن أعضاء الإدارة الآخرين يجب أن يكون لهم مقر في الدولة ما لم يجيز المصرف المركزي بخلاف ذلك.

57. **Means of Distance Communication:** means a method which may be used for the conclusion of a payment services agreement without the simultaneous physical presence of the Payment Service Provider and the Retail Payment Service User.

57. **وسائل الاتصال عن بعد:** تعني طريقة يمكن استخدامها لإبرام اتفاقية خدمات الدفع دون التواجد الشخصي المتزامن لمقدم خدمات الدفع ومستخدم خدمات الدفع للتجزئة.

58. **Merchant:** means a Person who accepts Payment Instruments as a mode of payment for the purchase and sale of goods and services.

58. **التاجر:** يعني الشخص الذي يقبل أدوات الدفع كوسيلة للسداد لشراء وبيع السلع والخدمات.

59. **Merchant Acquirer:** means a category of Payment Service Provider providing Merchant Acquiring Services.

59. **المحصل:** يعني فئة من مقدمي خدمات الدفع الذين يقدمون خدمات تحصيل المعاملات.

60. **Merchant Acquiring Service:** means a Retail Payment Service provided by a Payment Service Provider contracting with a Payee to accept and process Payment Transactions, which results in a transfer of funds to the Payee.

60. **خدمة تحصيل المعاملات:** تعني خدمة دفع للتجزئة مقدمة من مقدم خدمات الدفع المتعاقد مع مدفوع له لقبول ومعالجة معاملات الدفع، التي ينتج عنها تحويل أموال الى المدفوع له.

61. **Money Transfer Services:** means the Domestic and Cross-border Fund Transfers Services, excluding Remittances.

61. **خدمة تحويل الأموال:** تعني خدمة تحويل الأموال محلياً أو عبر الحدود، باستثناء التحويلات.

62. **Money's Worth:** means value added onto an SVF by the customer; value received on the customer's SVF account; and value redeemed by the customer including not only "money" in the primary sense but also other forms of monetary consideration or assets such as values, reward points, Crypto-Assets, or Virtual Assets. For example, a value top-up of an SVF account may take the form of values, reward points, Crypto-Assets, or Virtual Assets earned by the SVF customer from making purchases of goods and services. Similarly, value received on the account of the SVF customer may take the form of an on-line transfer of value, reward points, Crypto-Assets, or Virtual Assets between fellow SVF customers.

62. **قيمة الأموال:** تعني القيمة المضافة الى تسهيلات القيمة المخزنة من قبل العميل، القيمة المستلمة في حساب تسهيلات القيمة المخزنة الخاص بالعميل، والقيمة المستردة من قبل العميل، دون أن يقتصر ذلك على "المال" بحد ذاته، إنما يشمل أشكال أخرى من المقابل النقدي أو الأصول مثل القيم، ونقاط المكافأة، والأصول المشفرة والافتراضية. على سبيل المثال، تعبئة رصيد حساب تسهيلات القيمة المخزنة قد يتخذ شكل القيم، نقاط المكافأة، الأصول المشفرة أو الأصول الافتراضية التي حصل عليها عميل تسهيلات القيمة المخزنة من خلال شرائه السلع والخدمات. وبالمثل، فإن القيمة المودعة في حساب عميل تسهيلات القيمة المخزنة قد تتخذ شكل تحويل عبر الانترنت للقيمة، نقاط المكافأة، الأصول المشفرة أو الأصول الافتراضية فيما بين عملاء تسهيلات القيمة المخزنة.

63. **Payment Account:** means an account with a Payment Service Provider held in the name of at least one Retail Payment Service User which is used for the execution of Payment Transactions.

63. **حساب الدفع:** يعني حسابًا مع مقدم خدمات الدفع المحتفظ به باسم مستخدم خدمات دفع للتجزئة واحد على الأقل والذي يتم استخدامه لتنفيذ معاملات الدفع.

64. **Payment Account Information Service:** means a Retail Payment Service to provide consolidated information on one or more Payment Accounts held by a Retail Payment Service User with either another Payment Service Provider or with more than one Payment Service Providers. For the avoidance of doubt, the Payment Account Information Service does not involve the holding of Retail Payment Service User's funds at any time.

64. **خدمة معلومات حساب الدفع:** تعني خدمة دفع للتجزئة لتوفير معلومات متكاملة عن واحد أو أكثر من حسابات الدفع التي يحتفظ بها مستخدم خدمات الدفع للتجزئة مع مقدم خدمات دفع آخر أو مع أكثر من مقدمي خدمات الدفع. ولتجنب الشك، لا تتضمن خدمة معلومات حساب الدفع الاحتفاظ بأموال مستخدم خدمات الدفع للتجزئة في أي وقت.

65. **Payment Account Issuance Service:** means a Retail Payment Service, other than Domestic and Cross-border Fund Transfer Services,

65. **خدمة إصدار حساب الدفع:** تعني خدمة دفع للتجزئة، ما عدا عن خدمات تحويل الأموال محلياً وعبر الحدود، التي تتيح (أ) فتح حساب الدفع، (ب) إيداع

النقد في حساب الدفع، (ج) سحب النقد من حساب الدفع، و(د) جميع العمليات اللازمة لتشغيل حساب الدفع. يتم استخدام حساب الدفع فقط للاحتفاظ بالأموال/النقد العابر ولا يسمح بتخزين الأموال/ النقد والحفاظ عليها من خلاله.

enabling (i) the opening of a Payment Account; (ii) cash to be placed on a Payment Account; (iii) cash to be withdrawn from a Payment Account; and (iv) all necessary operations for operating a Payment Account. The Payment Account is only used for holding fund/cash in transit and not allowed to store and maintain fund/cash.

66. **خدمة تجميع الدفع:** تعني خدمة دفع للتجزئة تسهل قبول مواقع التجارة الإلكترونية والتجار لأدوات الدفع المختلفة من مستخدمي خدمات الدفع للتجزئة لاستكمال التزامات الدفع الخاصة بهم دون الحاجة إلى قيام التجار بإنشاء نظام تجميع دفع منفصل خاص بهم. يسهل تجميع الدفع على التجار الاتصال بالمحصلين؛ الذين يتلقون، في إطار هذه العملية، دفوعات من مستخدمي خدمات الدفع للتجزئة، فيقومون بجمعها وتحويلها إلى التجار بعد فترة من الوقت.

66. **Payment Aggregation Service:** means a Retail Payment Service facilitating e-commerce websites and Merchants to accept various Payment Instruments from the Retail Payment Service Users for completion of their payment obligations without the need for Merchants to create a separate payment integration system of their own. Payment aggregation facilitates Merchants to connect with Merchant acquirers; in the process, they receive payments from Retail Payment Service Users, pool and transfer them on to the Merchants after a time period.

67. **بيانات الدفع:** تعني أية معلومات مرتبطة بمستخدم خدمات الدفع للتجزئة، بما في ذلك البيانات المالية ولا تشمل البيانات الشخصية.

67. **Payment Data:** means any information related to a Retail Payment Service User, including financial data and excluding Personal Data.

68. **خدمة إنشاء الدفع:** تعني خدمة دفع للتجزئة لإنشاء أمر دفع بناءً على طلب مستخدم خدمات الدفع للتجزئة فيما يتعلق بحساب الدفع لدى مقدم خدمات دفع آخر. لتجنب الشك، لا تتضمن خدمة إنشاء الدفع الاحتفاظ بأموال الدافع والحفاظ عليها في أي وقت.

68. **Payment Initiation Service:** means a Retail Payment Service to initiate a Payment Order at the request of the Retail Payment Service User with respect to a Payment Account held at another Payment Service Provider. For the avoidance of doubt, the Payment Initiation Service does not involve the holding and maintenance of Payer's funds at any time.

69. **أداة الدفع:** تعني جهاز أو أجهزة مخصصة، بطاقة دفع و/أو مجموعة إجراءات متفق عليها بين مستخدم خدمات الدفع للتجزئة ومقدم خدمات الدفع، يتم استخدامها من أجل إنشاء أمر الدفع.

69. **Payment Instrument:** means a personalized device(s), a payment card and/or set of procedures agreed between the Retail Payment Service User and the Payment Service Provider, and used in order to initiate a Payment Order.

70. **خدمة إصدار أداة الدفع:** تعني خدمة دفع للتجزئة ترتبط بتوفير أداة دفع لمستخدم خدمات الدفع للتجزئة التي تمكنه من إنشاء أوامر الدفع بالإضافة الى معالجة معاملات الدفع الخاصة بمستخدم خدمات الدفع للتجزئة.

70. **Payment Instrument Issuance Service:** means a Retail Payment Service related to the provision of a Payment Instrument to a Retail Payment Service User which enables it to initiate Payment Orders as well as the Processing of the Retail Payment Service User's Payment Transactions.

71. **Payment Service Provider:** means a legal Person that has been licensed in accordance with this Regulation to provide one or more Retail Payment Services and has been included in the Register as per Article (73) of the Central Bank Law.

71. **مقدم خدمات الدفع:** يعني شخص اعتباري حائز على ترخيص بموجب هذا النظام لتقديم خدمة أو أكثر من خدمات الدفع للتجزئة والمدرج في السجل وفقاً للمادة (73) من قانون المصرف المركزي.

72. **Payment Token Issuing**: means a Retail Payment Service related to the issuing of Payment Tokens by a Payment Service Provider. For the avoidance of doubt, Payment Tokens may not be offered to the public or segments thereof unless the Payment Service Provider issuing the Payment Tokens has obtained a Category I License, drafted a White Paper in respect of those Payment Tokens and received an approval by the Central Bank prior to offering such tokens to the public.

72. **إصدار رمز الدفع:** يعني خدمة الدفع للتجزئة المتعلقة بإصدار رموز الدفع من قبل مقدم خدمات الدفع. لتجنب الشك، لا يجوز تقديم رموز الدفع للجمهور أو لمجموعة منه إلا إذا حصل مقدم خدمات الدفع الذي أصدر رموز الدفع على ترخيص الفئة الأولى، وأعد ورقة بيضاء فيما يتعلق برموز الدفع وحصل على موافقة المصرف المركزي قبل عرض هذه الرموز للجمهور.

73. **Payment Token:** means a type of Crypto-Asset that is backed by one or more Fiat Currencies, can be digitally traded and functions as (i) a medium of exchange; and/or (ii) a unit of account; and/or (iii) a store of value, but does not have legal tender status in any jurisdiction. A Payment Token is neither issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the Payment Token. For the avoidance of doubt, a Payment Token does not represent any equity or debt claim.

73. **رمز الدفع:** يعني نوعًا من الأصول المشفرة مغطاة بواحدة أو أكثر من الأوراق النقدية، يمكن تداوله رقميًا ويعمل باعتباره (أ) وسيلةً للتبادل؛ (ب) وحدة الحساب؛ و/أو (ج) مخزن القيمة، ولكن ليس له قوة إبراء بموجب القانون في أي منطقة اختصاص. لا يتم إصدار رمز الدفع أو ضمانه من قبل أي منطقة اختصاص، ولا يؤدي الوظائف المذكورة أعلاه إلا بالاتفاق داخل جماعة مستخدمي رمز الدفع. لتجنب الشك، لا يمثل رمز الدفع أي مطالبة بحقوق الملكية أو الديون.

74. **Payment Token Buying**: means the buying of Payment Tokens in exchange for any Fiat Currency or Payment Token.

74. **شراء رمز الدفع:** يعني شراء رموز الدفع مقابل أي من الأوراق النقدية أو رموز الدفع.

75. **Payment Token Selling:** means the selling of Payment Tokens in exchange for any Fiat Currency or Payment Token.

75. **بيع رمز الدفع:** يعني بيع رموز الدفع مقابل أي من الأوراق النقدية أو رموز الدفع.

76. **Payment Token Services:** means the Retail Payment Services consisting of any of the following activities related to Payment Tokens: (i) Payment Token Issuing; (ii) Payment Token Buying; (iii) Payment Token Selling; (iv) Facilitating the Exchange of Payment Tokens;

76. **خدمات رمز الدفع:** تعني خدمات الدفع للتجزئة التي تشمل أي من الأنشطة التالية المرتبطة برموز الدفع: (أ) إصدار رمز الدفع، (ب) شراء رمز الدفع، (ج) بيع رمز الدفع، (د) تسهيل تداول رموز الدفع، (هـ) تمكين الدفعات للتجار و/أو تمكين الدفعات المباشرة

بين الأقران، و(و) خدمات أمين الحفظ. لتجنب الشك، يجوز لمقدم خدمات الدفع تقديم واحدة فقط من خدمات الدفع للتجزئة المشار إليها في الفقرتين (هـ) و(و)؛ وفي حال رغبته بتوفير كليهما والسماح لمستخدمي خدمات الدفع للتجزئة باسترداد رموز الدفع بأي أوراق نقدية بموجب ترتيب تعاقدي، فيجب أن يمتثل لمتطلبات تسهيلات القيم المخزنة ذات الصلة.

(v) enabling payments to Merchants and/or enabling peer-to-peer payments; and (vi) Custodian Services. For the avoidance of doubt, a Payment Service Provider may provide only one of the Retail Payment Services referred to in points (v) and (vi); if it wishes to provide both and allows Retail Payment Service Users to redeem the Payment Tokens with any Fiat Currency under a contractual arrangement, it must comply with the respective SVF requirements.

77. **معاملة الدفع:** تعني إجراء ينشئه الدافع أو نيابة عنه أو المدفوع له لوضع الأموال، تحويلها أو سحبها، بصرف النظر عن أي التزامات قائمة بين الدافع والمدفوع له.

77. **Payment Transaction:** means an act initiated by the Payer or on his behalf or by the Payee of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the Payer and the Payee.

78. **المدفوع له:** يعني الشخص المقصود المتلقي للأموال التي خضعت لمعاملة دفع.

78. **Payee:** means a Person who is the intended recipient of funds which have been the subject of a Payment Transaction.

79. **الدافع:** يعني الشخص صاحب حساب دفع الذي يجيز أمر دفع من هذا الحساب؛ أو في حال عدم وجود حساب دفع، الشخص الذي يعطي أمر دفع.

79. **Payer:** means a Person who holds a Payment Account and allows a Payment Order from that Payment Account, or, where there is no Payment Account, a Person who gives a Payment Order.

80. **الشخص:** يعني الشخص الطبيعي أو الاعتباري.

80. **Person** means any natural or legal Person.

81. **البيانات الشخصية:** تعني أية معلومات ترتبط بشخص طبيعي محدد أو قابل للتحديد.

81. **Personal Data:** means any information which are related to an identified or identifiable natural Person.

82. **المعالجة:** تعني معالجة معاملة الدفع اللازمة لتنفيذ أمر دفع، بما في ذلك المقاصة والتسوية، بين المحصل ومُصدر البطاقة.

82. **Processing:** means Payment Transaction processing necessary for the handling of an instruction, including clearing and settlement, between the Merchant Acquirer and the Card Issuer.

83. **الترويج:** يعني أي شكل من أشكال الاتصال، بأي وسيلة، يهدف إلى دعوة أو عرض تنظيم اتفاقية تتعلق بأي خدمة دفع للتجزئة. لتجنب الشك، لا يتحمل أي شخص تم تكليفه بتقديم أو المشاركة في أنشطة ترويجية من قبل شخص يقدم خدمات الدفع للتجزئة دون الحصول على ترخيص أي مسؤولية بموجب هذا النظام.

83. **Promotion:** means any form of communication, by any means, aimed at inviting or offering to enter into an agreement related to any Retail Payment Service. For the avoidance of doubt, any Person that has been mandated to provide or engage in Promotion activities by a Person providing Retail Payment Services without

holding a License shall not be held liable under this Regulation.

84. **Public Sector Entity:** means the Federal Government, Governments of the Union's member Emirates, public institutions and organizations.

84. **هيئات القطاع العام:** تعني الحكومة الاتحادية، حكومات الإمارات الأعضاء في الاتحاد، والهيئات والمؤسسات العامة.

85. **Register:** means the Register referred to in Article (73) of the Central Bank Law.

85. **السجل:** يعني السجل المشار إليه في المادة (73) من قانون المصرف المركزي.

86. **Regulation:** means the Retail Payment Services and Card Schemes Regulation.

86. **النظام:** يعني نظام خدمات الدفع للتجزئة ومنظومات البطاقات.

87. **Remittance:** means the receipt of funds from a Payer without any Payment Accounts being created in the name of the Payer or the Payee.

87. **التحويل:** يعني استلام الأموال من الدافع دون فتح أي حسابات دفع باسم الدافع أو المدفوع له.

88. **Reserve of Assets**: means the pool of Fiat Currencies that are legal tender backing the value of a Payment Token.

88. **احتياطي الأصول:** يعني مجموع الأوراق النقدية التي لها قوة إبراء بموجب القانون والتي تدعم قيمة رمز الدفع.

89. **Retail Payment Service:** means any business activity set out in Annex I.

89. **خدمات الدفع للتجزئة:** تعني أي نشاط تجاري محدد في الملحق 1.

90. **Retail Payment Service User:** means a Person who intends to make use of or makes use of a Retail Payment Service in the capacity of a Payer, Payee or both.

90. **مستخدم خدمات الدفع للتجزئة:** يعني الشخص الذي يعتزم الاستفادة أو يستفيد من خدمة دفع للتجزئة بصفته دافعًا أو مدفوع له أو كليهما.

91. **Sensitive Payment Data:** means data, including personalized security credentials which can be used to carry out unauthorized activities. For the purposes of Payment Initiation and Payment Account Information Services, the name of the Payment Account owner and Payment Account number shall not constitute Sensitive Payment Data.

91. **بيانات الدفع الحساسة:** تعني البيانات، بما في ذلك بيانات الأمان المخصصة التي يمكن استخدامها لتنفيذ أنشطة غير مصرح بها. يجب ألا يشكل اسم مالك حساب الدفع ورقم حساب الدفع بيانات دفع حساسة لأغراض خدمات إنشاء الدفع وخدمات معلومات حساب الدفع.

92. **Single Retail Payment Agreement:** means an agreement which governs the execution of an individual Payment Transaction.

92. **اتفاقية الدفع للتجزئة لمرة واحدة:** يعني الاتفاقية التي تحكم تنفيذ معاملة دفع فردية.

93. **State:** means the United Arab Emirates.

93. **الدولة:** تعني الإمارات العربية المتحدة.

94. **Security Token:** means a type of Crypto-Asset that provides its holder with rights and

94. **رمز الأوراق المالية:** يعني نوعًا من الأصول المشفرة يوفر لحامله حقوقًا والتزامات تمثل مطالبة

obligations that represent a debt or equity claim against the issuer of that token.

بالدين أو بحقوق الملكية في مواجهة مُصدر ذلك الرمز.

95. **Stored Value Facility or SVF**: means a facility (other than cash) for or in relation to which a Customer, or another person on the Customer's behalf, pays a sum of money (including Money's Worth such as values, reward points, Crypto-Assets or Virtual Assets) to the issuer, whether directly or indirectly, in exchange for: (a) the storage of the value of that money (including Money's Worth such as values, reward points, Crypto-Assets or Virtual Assets), whether in whole or in part, on the facility; and (b) the "Relevant Undertaking". SVF includes Device-based Stored Value Facility and Non-device based Stored Value Facility.

95. **تسهيلات القيمة المخزنة:** تعني تسهيلات (غير نقدية) يدفع عنها أو بما يتعلق بها العميل، أو شخص آخر نيابةً عن العميل، مبلغاً من المال (بما في ذلك قيمة الأموال ومنها القيم، نقاط المكافأة، والأصول المشفرة أو الافتراضية) للمصدر، سواء بشكل مباشر أو غير مباشر، مقابل: (أ) تخزين قيمة هذه الاموال (بما في ذلك قيمة الأموال ومنها القيم، نقاط المكافأة، والأصول المشفرة أو الافتراضية)، سواء كلياً أو جزئياً، ضمن التسهيلات؛ و(ب) "التعهد ذات الصلة". تشمل تسهيلات القيمة المخزنة تسهيلات القيمة المخزنة القائمة على الأجهزة وغير القائمة على الأجهزة على حدٍ سواء.

96. **Third country:** means a country other than the UAE.

96. **دولة ثالثة:** تعني أي دولة غير دولة الإمارات العربية المتحدة.

97. **Three Party Card Scheme**: means a Card Scheme in which the scheme itself provides Merchant Acquiring and Payment Instrument Issuing Services and Card-based Payment Transactions are made from the Payment Account of a Payer to the Payment Account of a Payee within the Card Scheme. When a Three Party Card Scheme licenses other Payment Service Providers for the issuance of Card-based Payment Instruments or the Merchant Acquiring of Card-based Payment Transactions, or both, or issues Card-based Payment Instruments with a co-branding partner or through an agent, it is considered to be a Four Party Card Scheme.

97. **منظومة بطاقات ثلاثية الأطراف:** يُقصد بها منظومة البطاقات التي تقدم بنفسها خدمات تحصيل المعاملات وخدمات إصدار أدوات الدفع ومعاملات الدفع بواسطة البطاقة التي تتم من حساب الدفع الخاص بالدافع إلى حساب الدفع الخاص بالمدفوع له ضمن منظومة البطاقات. عندما تقوم منظومة بطاقات ثلاثية الأطراف بترخيص مقدمي خدمات الدفع آخرين لإصدار أدوات الدفع بواسطة البطاقة أو لتحصيل معاملات الدفع بواسطة البطاقة، أو كليهما، أو إصدار أدوات الدفع بواسطة البطاقة مع شريك في العلامة التجارية أو من خلال وكيل، تعتبر منظومة بطاقات رباعية الأطراف.

98. **UAE:** means the United Arab Emirates.

98. **الإمارات العربية المتحدة:** تعني دولة الإمارات العربية المتحدة.

99. **Unauthorized Payment Transaction:** means a Payment Transaction for the execution of which the Payer has not given consent. Consent to execute a Payment Transaction or a series of Payment Transactions shall be given in the form agreed between the Payer and the Payment Service Provider. Consent to execute a Payment

99. **معاملة دفع غير مصرح بها:** تعني معاملة دفع لم يوافق الدافع على تنفيذها. يجب إعطاء الموافقة على تنفيذ معاملة الدفع أو سلسلة من معاملات الدفع بالشكل المتفق عليه بين الدافع ومقدم خدمات الدفع. يمكن أيضًا إعطاء الموافقة على تنفيذ معاملة الدفع عبر المدفوع له أو مقدم خدمة إنشاء الدفع.

Transaction may also be given via the Payee or the Payment Initiation Service Provider.

100. **Virtual Assets:** A Virtual Asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual Assets do not include digital representations of Fiat Currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.

100. **الأصول الافتراضية:** هي تمثيل رقمي للقيمة التي يمكن تداولها رقميًا أو تحويلها، ويمكن استخدامها لأغراض الدفع أو الاستثمار. لا تشمل الأصول الافتراضية التمثيل الرقمي للأوراق النقدية والمالية والأصول المالية الأخرى التي سبقت تغطيتها في التوصيات الأخرى لمجموعة العمل المالي.

101. **Virtual Assets Service Providers:** Virtual Asset Service Provider means any natural or legal person who is not covered elsewhere under the FATF Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: (i) exchange between Virtual Assets and Fiat Currencies; (ii) exchange between one or more forms of Virtual Assets; (iii) transfer of Virtual Assets; (iv.) safekeeping and/or administration of Virtual Assets or instruments enabling control over Virtual Assets; and (v) participation in and provision of financial services related to an issuer's offer and/or sale of a Virtual Asset.

101. **مقدمو خدمات الأصول الافتراضية:** يُقصد بمقدم خدمة الأصول الافتراضية أي شخص طبيعي أو اعتباري لم يتم تغطيته في أي توصية أخرى لمجموعة العمل المالي، والذي يقوم بإجراء واحد أو أكثر من الأنشطة أو العمليات التالية لصالح أو نيابة عن شخص طبيعي أو اعتباري آخر: (1) التبادل بين الأصول الافتراضية والأوراق النقدية؛ (2) التبادل بين شكل أو أكثر من الأصول الافتراضية؛ (3) نقل الأصول الافتراضية؛ (4) حفظ و / أو إدارة الأصول الافتراضية أو الأدوات التي تمكن من التحكم في الأصول الافتراضية؛ و (5) المشاركة في وتقديم الخدمات المالية المتعلقة بعرض المصدر و / أو بيع أصل افتراضي.

102. **Virtual Asset Token**: means a type of Crypto-Asset that can be digitally traded and functions as (i) a unit of account; and/or (ii) a store of value. Although some Virtual Asset Tokens may be accepted as a means of payment, they are generally not accepted as a medium of exchange, may not have an issuer and do not have legal tender status in any jurisdiction. A Virtual Asset Token is neither issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the Virtual Asset Token. For the avoidance of doubt, a Virtual Asset Token does not represent any equity or debt claim, and it is not backed by any Fiat Currency.

102. **رموز الأصول الافتراضية:** تعني نوعًا من الأصول المشفرة التي يمكن تداولها رقميًا وتعمل (أ) كوحدة حساب؛ و/أو (2) مخزن للقيمة. على الرغم من أنه قد يتم قبول بعض رموز الأصول الافتراضية كوسيلة للدفع، إلا أنها لا تُقبل عمومًا كوسيلة للتبادل، وقد لا يكون لها مُصدر وليس لها قوة إبراء بموجب القانون في أي منطقة اختصاص. لا يتم إصدار رمز الأصول الافتراضية أو ضمانه من قبل أي منطقة اختصاص، ولا يؤدي الوظائف المذكورة أعلاه إلا بالاتفاق داخل جماعة مستخدمي رمز الأصول الافتراضية. لتجنب الشك، لا يمثل رمز الأصول الافتراضية أي مطالبة بحقوق الملكية أو الديون، وهو غير مغطى بأي أوراق نقدية.

103. **Virtual Asset Token Services**: means any of the following services: (i) enabling peer-to-peer Virtual Asset Token transfers, and (ii) custodian services of Virtual Asset Tokens.

103. **خدمات رموز الأصول الافتراضية:** تعني أيًا من الخدمات التالية: (أ) تمكين عمليات تحويل رمز الأصول الافتراضية من خلال المشاركة المباشرة بين الأقران، و(2) خدمات أمين الحفظ لرموز الأصول الافتراضية.

104. **Wages Protection System or WPS:** means a reconciliation system implemented at the Central Bank aimed at providing a safe, secure, efficient and robust mechanism for streamlining the timely and efficient payment of wages.

104. **نظام حماية الأجور:** يعني أي نظام توافق مطبق في المصرف المركزي يهدف إلى توفير آلية آمنة ومؤمنة وفعالة وقوية لتسهيل دفع الأجور في الوقت المناسب وبكفاءة.

105. **Wire Transfer:** means any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person

105. **التحويلات الإلكترونية:** تعني أي معاملة تتم نيابة عن صاحب المعاملة من خلال مؤسسة مالية بوسائل إلكترونية بهدف جعل مبلغ من الأموال متوفر لشخص مستفيد في مؤسسة مالية مستفيدة، بغض النظر عما إذا كان صاحب المعاملة والمستفيد هما نفس الشخص.

106. **WPS Payment Account:** means a WPS account opened in the infrastructure of the Central Bank and held for the purposes of holding and payment of wages.

106. **حساب دفع في نظام حماية الأجور:** يعني حساب مرتبط بنظام حماية الأجور في البنية التحتية للمصرف المركزي ويتم الاحتفاظ به لأغراض حفظ الأجور ودفعها.

107. **WPS Payment Account Holder:** means a holder of a Payment Account held with a Payment Service Provider who has been given access to the Wages Protection System for the purpose of executing transfers of wages.

107. **صاحب حساب دفع في نظام حماية الأجور:** يعني صاحب حساب دفع لدى مقدم خدمات الدفع الذي مُنح حق الوصول إلى نظام حماية الأجور بغرض تنفيذ تحويلات الأجور.

108. **White Paper:** means a detailed description in Arabic and English of: (i) the Payment Service Provider issuing a Payment Token and a presentation of the main participants involved in the project's design and development; (ii) a detailed description of the project and the type of Payment Token that will be offered to the public; (iii) the number of Payment Tokens that will be issued and the issue price; (iv) a detailed description of the rights and obligations attached to the Payment Token and the procedures and conditions for exercising those rights; (v) information on the underlying technology and standards applied by the Payment Service

108. **الورقة البيضاء**: تعني الوصف المفصل باللغتين العربية والإنجليزية لما يلي: (أ) إصدار مقدم خدمات الدفع رمزًا للدفع وعرضًا للمشاركين الرئيسيين المعنيين في تصميم المشروع وتطويره، (ب) وصفًا تفصيليًا للمشروع ونوع رمز الدفع الذي سيتم تقديمه للجمهور، (ج) عدد رموز الدفع التي سيتم إصدارها وسعر الإصدار، (د) وصف تفصيلي للحقوق والالتزامات المرتبطة برمز الدفع وإجراءات وشروط ممارسة تلك الحقوق، (هـ) معلومات عن التكنولوجيا والمعايير الأساسية المطبقة من قبل مقدم خدمات الدفع الذي يصدر رمز الدفع بما يجيز بالاحتفاظ برموز الدفع هذه،

تخزينها وتحويلها، (و) وصفًا تفصيليًا للمخاطر المتعلقة بإصدار مقدم خدمات الدفع رموز الدفع، ورموز الدفع، والعرض للجمهور وتنفيذ المشروع، والإفصاحات الأخرى التي قد يحددها المصرف المركزي، (ز) وصفًا تفصيليًا لترتيبات الحوكمة الخاصة بمقدم خدمات الدفع، بما في ذلك وصف دور ومهام ومستوى مسؤولية الأطراف الثالثة المسؤولة عن تشغيل واستثمار وحفظ احتياطي الأصول، وحيثما ينطبق، توزيع رموز الدفع، (ح) وصفًا تفصيليًا لاحتياطي الأصول، (ي) وصفًا تفصيليًا لترتيبات الحفظ الخاصة باحتياطي الأصول، بما في ذلك فصل الأصول؛ (ح) في حالة استثمار احتياطي الأصول، وصف تفصيلي لسياسة الاستثمار؛ و(ط) معلومات عن طبيعة الحقوق وإمكانية نفاذها، بما في ذلك أي حق استرداد مباشر أو أي مطالبات قد تكون لأصحاب رموز الدفع بشأن احتياطي الأصول أو تجاه مقدم خدمات الدفع الذي أصدر رموز الدفع، بما في ذلك كيفية التعامل مع هذه الحقوق في حال إجراءات الإفلاس. لتجنب الشك، يجب صياغة الورقة البيضاء بلغة بسيطة وسهلة الفهم وغير مضللة، ويجب أن تكون مؤرخةً. يجب اعتماد الورقة البيضاء من قبل إدارة مقدم خدمات الدفع ونشرها على الموقع الالكتروني لمقدم خدمات الدفع بعد الحصول على موافقة المصرف المركزي.

Provider issuing the Payment Token allowing for the holding, storing and transfer of those Payment Tokens; (vi) a detailed description of the risks relating to the Payment Service Provider issuing Payment Tokens, the Payment Tokens, the offer to the public and the implementation of the project, and other disclosures that the Central Bank may specify; (vii) detailed description of the Payment Service Provider's governance arrangements, including a description of the role, responsibilities and accountability of the third-parties responsible for operating, investment and custody of the Reserve of Assets, and, where applicable, the distribution of the Payment Tokens; (viii) a detailed description of the Reserve of Assets; (ix) a detailed description of the custody arrangements for the Reserve of Assets, including the segregation of the assets; (x) in case of an investment of the Reserve of Assets, a detailed description of the investment policy; and (xi) information on the nature and enforceability of rights, including any direct redemption right or any claims that holders of Payment Tokens may have on the Reserve of Assets or against the Payment Service Provider issuing the Payment Tokens, including how such rights may be treated in insolvency procedures.

For the avoidance of doubt, the White Paper shall be written in a simple, easy to understand and non-misleading language, and shall be dated. The White Paper shall be endorsed by the Payment Service Provider's Management and published on the Payment Service Provider's website after receipt of an approval by the Central Bank.

Article (2): Licensing

المادة (2): الترخيص

1. No Person shall provide or engage in the Promotion within the State of any of the Retail Payment Services set out in Annex I without obtaining a prior License from the Central Bank unless this Person is an exempted Person.

1. لا يجوز لأي شخص تقديم أو المشاركة في الترويج داخل الدولة لأي من خدمات الدفع للتجزئة المنصوص عليها في الملحق 1 دون الحصول على ترخيص مسبق من المصرف المركزي، ما لم يكن هذا الشخص شخصًا معفى.

Exempted Persons

الأشخاص المعفيين

2. Banks licensed in accordance with the Central Bank Law shall be deemed licensed to provide Retail Payment Services and shall therefore be exempt from the prohibition laid down in paragraph (1). Nevertheless, Banks shall be required to notify the Central Bank in writing if they intend to provide the Retail Payment Services referred to in points (3) to (4) and (7) to (9) of Annex I and obtain a No Objection Letter prior to commencing the provision of such services. Banks are exempted from the No Objection Letter requirement and any licensing requirements for providing the Retail Payment Services referred to in points (1), (2), (5) and (6) of Annex I.

2. تعتبر البنوك المرخصة من قبل المصرف المركزي تلقائيا مرخصة لتقديم خدمات الدفع للتجزئة وتكون بناءً لذلك معفاة من المنع المشار إليه في البند (1). ومع ذلك، يتعين على البنوك إخطار المصرف المركزي خطيًا في حال رغبتها تقديم خدمات الدفع للتجزئة المشار إليها في البنود (3) إلى (4) و(7) إلى (9) من الملحق 1 والحصول على خطاب عدم ممانعة قبل البدء في تقديم هذه الخدمات. تُعفى البنوك من متطلب خطاب عدم الممانعة وأي متطلبات ترخيص لتقديم خدمات الدفع للتجزئة المشار إليها في البنود (1)، (2)، (5) و(6) من الملحق 1.

3. For the avoidance of doubt, Banks providing Retail Payment Services other than the Retail Payment Services referred to in points (1), (2), (5) and (6) of Annex I, shall be required to comply only with the requirements set out in Article (11) on Payment Token Services, Article (12) on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations, Article (13) on Technology Risk and Information Security, and Article (14) on Obligations Towards Retail Payment Service Users.

3. لتجنب الشك، يتعين على البنوك التي تقدم خدمات الدفع للتجزئة، بخلاف خدمات الدفع للتجزئة المشار إليها في البنود (1)، (2)، (5) و(6) من المرفق 1، الامتثال فقط للمتطلبات المنصوص عليها في المادة (11) بشأن خدمات رمز الدفع، المادة (12) بشأن مواجهة غسل الأموال ومكافحة تمويل الإرهاب والتنظيمات غير المشروعة، المادة (13) بشأن مخاطر التكنولوجيا وأمن المعلومات، والمادة (14) بشأن الالتزامات تجاه مستخدمي خدمات الدفع للتجزئة.

4. Finance companies licensed in accordance with the finance companies Regulation shall be exempt from the prohibition laid down in paragraph (1) for the service of issuance of credit cards. For the avoidance of doubt, except issuance of credit cards, finance companies that intend to provide Retail Payment Services shall

4. تستثنى شركات التمويل المرخص لها بموجب نظام شركات التمويل من الحظر المنصوص عليه في البند (1) فيما يخص خدمة إصدار بطاقات الائتمان. لتجنب الشك، باستثناء إصدار بطاقات الائتمان، يتعين على شركات التمويل التي تعتزم تقديم خدمات الدفع للتجزئة الحصول على ترخيص مسبق من المصرف المركزي.

be required to obtain a prior License from the Central Bank.

5. The Central Bank may request from a Person or Exempted Person the provision of any information or documentation that it considers necessary to determine the eligibility for exemption or continued exemption, respectively.

5. يجوز للمصرف المركزي أن يطلب من شخص أو شخص معفى تزويده بأي معلومات أو مستندات يراها ضرورية لتحديد الأهلية للإعفاء أو استمرار الإعفاء تباعاً.

6. The Central Bank reserves the right to withdraw an exemption granted under this Article 2.

6. يحتفظ المصرف المركزي بحق إلغاء الإعفاء الممنوح بناء على المادة 2.

Article (3): License Categories

المادة (3): فئات الترخيص

1. A Person that intends to provide Retail Payment Services shall apply for one of the following categories of License:

1. يجب على الشخص الذي يعتزم تقديم خدمات الدفع للتجزئة التقدم بطلب الحصول على إحدى فئات الترخيص التالية:

1.1. Category I License;

1.1 ترخيص الفئة الأولى؛

1.2. Category II License;

1.2 ترخيص الفئة الثانية؛

1.3. Category III License; and

1.3 ترخيص الفئة الثالثة؛ و

1.4. Category IV License

1.4 ترخيص الفئة الرابعة.

2. An Applicant shall apply for a Category I License where it intends to provide one or more of the following Retail Payment Services:

2. يجب على مقدم الطلب التقدم للحصول على ترخيص الفئة الأولى إذا كان يعتزم تقديم واحدة أو أكثر من خدمات الدفع للتجزئة التالية:

2.1. Payment Account Issuance Services;

2.1 خدمات إصدار حساب الدفع؛

2.2. Payment Instrument Issuance Services;

2.2 خدمات إصدار أداة الدفع؛

2.3. Merchant Acquiring Services;

2.3 خدمات تحصيل المعاملات؛

2.4. Payment Aggregation Services;

2.4 خدمات تجميع الدفع؛

2.5. Domestic Fund Transfer Services;

2.5 خدمات تحويل الأموال محلياً؛

2.6. Cross-border Fund Transfer Services; and

2.6 خدمات تحويل الأموال عبر الحدود؛ و

2.7. Payment Token Services.

2.7 خدمات رمز الدفع.

3. An Applicant shall apply for a Category II License where it intends to provide one or more of the following Retail Payment Services:

3. يجب على مقدم الطلب التقدم للحصول على ترخيص الفئة الثانية إذا كان يعتزم تقديم واحدة أو أكثر من خدمات الدفع للتجزئة التالية:

3.1. Payment Account Issuance Services;

3.1 خدمات إصدار حساب الدفع؛

3.2. Payment Instrument Issuance Services;

3.2 خدمات إصدار أداة الدفع؛

3.3. Merchant Acquiring Services;

3.3 خدمات تحصيل المعاملات؛

3.4. Payment Aggregation Services;

3.4 خدمات تجميع الدفع؛

3.5. Domestic Fund Transfer Services; and

3.5 خدمات تحويل الأموال محلياً؛ و

3.6. Cross-border Fund Transfer Services.

3.6 خدمات تحويل الأموال عبر الحدود.

4. An Applicant shall apply for a Category III License where it intends to provide one or more of the following Retail Payment Services:

4. يجب على مقدم الطلب التقدم للحصول على ترخيص الفئة الثالثة إذا كان يعتزم تقديم واحدة أو أكثر من خدمات الدفع للتجزئة التالية:

4.1. Payment Account Issuance Services;

4.1 خدمات إصدار حساب الدفع؛

4.2. Payment Instrument Issuance Services;

4.2 خدمات إصدار أداة الدفع؛

4.3. Merchant Acquiring Services;

4.3 خدمات تحصيل المعاملات؛

4.4. Payment Aggregation Services; and

4.4 خدمات تجميع الدفع؛ و

4.5. Domestic Fund Transfer Services.

4.5 خدمات تحويل الأموال محلياً.

5. An Applicant shall apply for a Category IV License where it intends to provide one or all of the following Retail Payment Services:

5. يجب على مقدم الطلب التقدم للحصول على ترخيص الفئة الرابعة إذا كان يعتزم تقديم واحدة أو أكثر من خدمات الدفع للتجزئة التالية:

5.1. Payment Initiation Services; and

5.1 خدمات إنشاء الدفع؛ و

5.2. Payment Account Information Services.

5.2 خدمات معلومات حساب الدفع.

Article (4): License Conditions

المادة (4): شروط الترخيص

1. To be granted a License, an Applicant shall, at the time of submitting an Application:
   1.1. fulfil the Legal Form;
   1.2. meet the respective initial capital requirements per License Category specified in Article (6); and
   1.3. provide the necessary documents and information specified in the Central Bank application form as provided by the Licensing Division.
2. In addition to the requirements set out in paragraph (1) to be granted a Category I License, an Applicant shall, at the time of submitting an Application, provide a list of all Payment Tokens that it intends to issue and obtain a legal opinion on the assessment for all Payment Tokens.
3. In addition to the requirements set out in paragraph (1), to be granted a Category IV License, an Applicant shall, at the time of submitting an Application, hold a professional indemnity insurance as per Article (10) paragraphs (14) to (16).

1. للحصول على ترخيص، يجب على مقدم الطلب، عند تقديم الطلب:
   1.1 استيفاء الشكل القانوني؛
   1.2 استيفاء متطلبات رأس المال الأولي وفقاً لفئة الترخيص المحددة في المادة (6)؛ و
   1.3 تقديم المستندات والمعلومات اللازمة والمحددة في نموذج الطلب الخاص بالمصرف المركزي كما هو منصوص عليه من قبل قسم الترخيص.
2. بالإضافة إلى المتطلبات المنصوص عليها في البند (1)، للحصول على ترخيص الفئة الأولى، يجب على مقدم الطلب، عند تقديم الطلب، تقديم قائمة بجميع رموز الدفع التي يعتزم اصدارها والحصول على رأي قانوني بشأن تقييم جميع رموز الدفع.
3. بالإضافة إلى المتطلبات المنصوص عليها في البند (1)، للحصول على ترخيص الفئة الرابعة، يجب على مقدم الطلب، عند تقديم الطلب، حيازة تأمين التعويض المهني وفقاً للبنود (14) الى (16) من المادة (10).

Article (5): Licensing Procedure

المادة (5): إجراءات الترخيص

1. The licensing of Applicants shall be subject to the procedure envisaged in the Central Bank's Licensing Guidelines.
2. The Management of an Applicant is encouraged to meet with the Central Bank's Licensing Division before submitting a formal Application.

1. يخضع ترخيص مقدمي الطلبات للإجراءات المنصوص عليها في إرشادات الترخيص الصادرة عن المصرف المركزي.
2. يتم تشجيع إدارة مقدم الطلب على مقابلة قسم الترخيص بالمصرف المركزي قبل تقديم طلب رسمي.

Article (6): Initial Capital

المادة (6): رأس المال الأولي

1. An Applicant shall hold, upon being granted a License by the Central Bank, initial capital as per the below:

1. يجب على مقدم الطلب، عند منحه ترخيصًا من المصرف المركزي، أن يحتفظ برأس مال أولي وفقًا لما يلي:

1.1. for obtaining a Category I License:

1.1 للحصول على ترخيص الفئة الأولى:

1.1.1. initial capital of at least three (3) million Dirhams where the monthly average value of Payment Transactions amounts to ten (10) million Dirhams or above; or

1.1.1 رأس مال أولي لا يقل عن ثلاثة (3) ملايين درهم في حال كان متوسط القيمة الشهرية لمعاملات الدفع عشرة (10) ملايين درهم أو ما فوق؛ أو

1.1.2. initial capital of at least one and a half (1.5) million Dirhams where the monthly average value of Payment Transactions amounts to less than ten (10) million Dirhams.

1.1.2 رأس مال أولي لا يقل عن (1.5) مليون ونصف درهم في حال كان متوسط القيمة الشهرية لمعاملات الدفع أقل من عشرة (10) ملايين درهم؛

1.2. for obtaining a Category II License:

1.2 للحصول على ترخيص الفئة الثانية:

1.2.1. initial capital of at least two (2) million Dirhams where the monthly average value of Payment Transactions amounts to ten (10) million Dirhams or above; or

1.2.1 رأس مال أولي لا يقل عن (2) مليوني درهم في حال كان متوسط القيمة الشهرية لمعاملات الدفع عشرة (10) ملايين درهم أو ما فوق؛ أو

1.2.2. initial capital of at least one (1) million Dirhams where the monthly average value of Payment Transactions amounts to less than ten (10) million Dirhams.

1.2.2 رأس مال أولي لا يقل عن (1) مليون درهم في حال كان متوسط القيمة الشهرية لمعاملات الدفع أقل من عشرة (10) ملايين درهم.

1.3. for obtaining a Category III License:

1.3 للحصول على ترخيص الفئة الثالثة:

1.3.1. initial capital of at least one (1) million Dirhams where the monthly average value of Payment Transactions

1.3.1 رأس مال أولي لا يقل عن (1) مليون درهم في حال كان متوسط القيمة الشهرية

لمعاملات الدفع عشرة (10) ملايين درهم أو ما فوق؛ أو

amounts to ten (10) million Dirhams or above; or

1.3.2 رأس مال أولي لا يقل عن خمسمائة ألف (500،000) درهم في حال كان متوسط القيمة الشهرية لمعاملات الدفع أقل من عشرة (10) ملايين درهم.

1.3.2. initial capital of at least five hundred thousand (500,000) Dirhams where the monthly average value of Payment Transactions amounts to less than ten (10) million Dirhams.

1.4 للحصول على ترخيص الفئة الرابعة: رأس مال أولي لا يقل عن مئة ألف (100،000) درهم بغض النظر عن متوسط القيمة الشهرية لمعاملات الدفع.

1.4. for obtaining a Category IV License: initial capital of at least one hundred thousand (100,000) Dirhams regardless of the monthly average value of Payment Transactions.

2. يجب على مقدم الطلب تقديم معلومات إلى المصرف المركزي عن مصدر (مصادر) الأموال التي تشكل رأس المال الأولي وفقًا للبند (1).

2. An Applicant shall provide information to the Central Bank on the source(s) of funds that constitute the initial capital as per paragraph (1).

آلية إجراء الحساب

3. يتم حساب متوسط القيمة الشهرية لمعاملات الدفع المشار إليه في البند (1) على أساس المتوسط المتبدل للأشهر (3) السابقة أو، في حالة عدم وجود هذه البيانات عند منح الترخيص من قبل المصرف المركزي، على أساس خطة العمل والتوقعات المالية المقدمة.

Calculation Method

3. The monthly average value of Payment Transactions referred to in paragraph (1) shall be calculated on the basis of the moving average of the preceding (3) months or, where such data does not exist at the time of being granted a License by the Central Bank, on the basis of the business plan and financial projections provided.

المادة (7): إجمالي رأس المال

1. يجب على مقدم خدمات الدفع ضمان والاحتفاظ في جميع الأوقات بإجمالي رأس مال لا يقل عن متطلبات رأس المال الأولي المنصوص عليها في المادة (6)، مع الأخذ في الاعتبار فئة الترخيص المعنية.

2. يجوز للمصرف المركزي أن يفرض متطلبات إجمالي رأس مال أعلى من تلك المشار إليها في البند (1) إذا اعتبر، بالنظر إلى حجم وتعقيد أعمال مقدم خدمات الدفع، أن هذه المتطلبات الأعلى ضرورية للتحقق من كون مقدم خدمات الدفع يمتلك القدرة على الوفاء بالتزاماته بموجب هذا النظام.

Article (7): Aggregate Capital Funds

1. A Payment Service Provider shall hold and maintain at all times aggregate capital funds that do not fall below the initial capital requirements laid down in Article (6), taking into consideration the applicable License category.

2. The Central Bank may impose aggregate capital funds requirements higher than the ones referred to in paragraph (1) if, taking into consideration the scale and complexity of the Payment Service Provider's business, it considers such higher requirements essential to ensuring that the

Payment Service Provider has the ability to fulfil its obligations under this Regulation.

3. Where the monthly average value of Payment Transactions calculated in accordance with Article (6) (3) exceeds the Payment Transaction threshold of ten (10) million Dirhams in (3) consecutive months, Payment Service Providers shall report this fact to the Central Bank and become automatically subject to the higher aggregate capital funds requirements determined by the Central Bank under paragraph (2).

3. في حال تجاوز متوسط القيمة الشهرية لمعاملات الدفع المحسوبة وفقًا للبند (3) من المادة (6) الحد الأقصى لمعاملات الدفع البالغ عشرة (10) ملايين درهم خلال ثلاثة (3) أشهر متتالية، يتعين على مقدمي خدمات الدفع إبلاغ المصرف المركزي بهذا الشأن ليصبحوا تلقائيًا خاضعين لمتطلبات إجمالي رأس المال الأعلى التي يحددها المصرف المركزي بموجب البند (2).

4. The aggregate capital funds referred to in paragraph (1) shall be comprised of one or more of the capital items provided for in paragraphs (5) and (6).

4. يتألف إجمالي رأس المال المشار إليه في البند (1) من واحد أو أكثر من عناصر رأس المال المشار إليها في البندين (5) و(6).

Capital Items

عناصر رأس المال

5. A Payment Service Provider's aggregate capital funds shall consist of:

5. يتألف إجمالي رأس المال لمقدم خدمات الدفع من التالي:

5.1. Paid-up capital;

5.1 رأس المال المدفوع؛

5.2. Reserves, excluding revaluation reserves; and

5.2 الاحتياطيات، باستثناء احتياطيات إعادة التقييم؛ و

5.3. Retained earnings.

5.3 الأرباح المحتفظ بها.

6. The following items shall be deducted from the aggregate capital funds:

6. يجب عدم احتساب العناصر التالية ضمن إجمالي رأس المال:

6.1. Accumulated losses; and

6.1 الخسائر المتراكمة؛ و

6.2. Goodwill.

6.2 السمعة التجارية.

Article (8): Control of Controllers

المادة (8): الرقابة على المسيطرين

1. A Person shall not become a Controller in a Payment Service Provider without obtaining a prior approval from the Central Bank.

1. لا يجب لأي شخص أن يصبح مسيطراً في مقدم خدمات دفع دون الحصول على موافقة مسبقة من المصرف المركزي.

2. The Central Bank shall grant an approval under paragraph (1) if it considers that:

2. يمنح المصرف المركزي الموافقة المشار اليها في البند (1) إذا وجد أنه:

2.1. having regard to the likely influence of the Controller, the Payment Service Provider will remain compliant with the requirements of this Regulation and Level 2 Acts; and

2.1 بالنظر إلى التأثير المحتمل للمسيطر، سيظل مقدم خدمات الدفع ممتثلًا لمتطلبات هذا النظام وأحكام المستوى الثاني؛ و

2.2. the Controller meets the fit and proper requirements specified by the Central Bank.

2.2 استيفاء المسيطر للمتطلبات الملائمة المحددة من قبل المصرف المركزي.

3. The approval under paragraph (2) may be granted subject to any conditions that the Central Bank may impose on the Person, including but not limited to:

3. يجوز منح الموافقة بموجب البند (2) وفقًا لأية شروط قد يفرضها المصرف المركزي على الشخص، بما في ذلك على سبيل المثال لا الحصر:

3.1. conditions restricting the Person's disposal or further acquisition of shares or voting powers in the Payment Service Provider; and

3.1 الشروط التي تقيد قدرة الشخص على التصرف أو التملك اللاحق للأسهم أو حقوق التصويت في مقدم خدمات الدفع؛ و

3.2. conditions restricting the Person's exercise of voting power in the Payment Service Provider.

3.2 الشروط التي تقيد ممارسة الشخص لحق التصويت في مقدم خدمات الدفع.

Article (9): Principal Business

المادة (9): العمل الرئيسي

1. The principal business of a Payment Service Provider shall be the provision of the Retail Payment Service(s) for which it has been granted a License.

1. يجب أن يكون العمل الرئيسي لمقدم خدمات الدفع توفير خدمة (خدمات) الدفع للتجزئة التي تم منحه ترخيصًا لها.

2. Where a Payment Service Provider intends to provide ancillary service(s) falling outside the scope of its License, it shall obtain the approval of the Central Bank prior to commencing the provision of such service(s).

2. في حال اعتزم مقدم خدمات الدفع تقديم خدمة (خدمات) إضافية تقع خارج نطاق ترخيصه، فيجب عليه الحصول على موافقة المصرف المركزي قبل البدء في تقديم هذه الخدمة (الخدمات).

3. The Central Bank requires prior approval for the provision of any ancillary service(s) by a Payment Service Provider, and may require a Payment Service Provider that intends to provide ancillary service(s), to create a separate entity for the provision of such services, if it believes that the conduct of the ancillary activities may have a negative impact on the Payment Service Provider's ability to comply with the requirements of this Regulation and Level 2 Acts.

3. يوجب المصرف المركزي الحصول على موافقة مسبقة لتقديم أي خدمة (خدمات) إضافية من قبل مقدم خدمات الدفع، وقد يطلب من مقدم خدمات الدفع الذي يعتزم تقديم خدمة (خدمات) إضافية، إنشاء كيان منفصل لتقديم هذه الخدمات، إذا وجد أن تنفيذ الأنشطة الإضافية قد يكون له تأثير سلبي على قدرة مقدم خدمات الدفع على الامتثال لمتطلبات هذا النظام وأحكام المستوى الثاني.

Article (10): On-Going Requirements

المادة (10): المتطلبات المستمرة

Corporate Governance

الحوكمة المؤسسية

1. Payment Service Providers must comply with the below requirements on corporate governance.

1. يجب على مقدمي خدمات الدفع الامتثال للمتطلبات التالية بشأن الحوكمة المؤسسية.

2. Payment Service Providers must have and maintain effective, robust and well-documented corporate governance arrangements, including a clear organizational structure with well-defined, transparent and consistent lines of responsibility.

2. يجب أن يكون لدى مقدمي خدمات الدفع ترتيبات حوكمة فعالة، قوية وموثقة جيدًا والحفاظ عليها، بما في ذلك هيكل تنظيمي واضح، وتوزيع محدد وشفاف وملائم للمهام والمسؤوليات.

3. The corporate governance arrangements referred to in paragraph (2) must be comprehensive and proportionate to the nature, scale and complexity of the Retail Payment Services provided, and shall contain, at a minimum:

3. يجب أن تكون ترتيبات الحوكمة المؤسسية المشار إليها في البند (2) متكاملة ومتناسبة مع طبيعة، حجم وتعقيد خدمات الدفع للتجزئة المقدمة، ويجب أن تحتوي، كحد أدنى، على ما يلي:

3.1. an organization chart showing each division, department or unit, indicating the name of each responsible individual accompanied by a description of the respective function and responsibilities;

3.1 هيكل تنظيمي يوضح كل قسم، إدارة أو وحدة، مع الإشارة إلى اسم كل فرد مسؤول مصحوبًا بوصف الوظيفة والمهام والمسؤوليات الموكلة إليه؛

3.2. controls on conflicts of interest;

3.2 ضوابط لحالات تضارب المصالح؛

3.3. controls on integrity and transparency of the Payment Service Provider's operations;

3.3 ضوابط النزاهة والشفافية في عمليات مقدم خدمات الدفع؛

3.4. controls to ensure compliance with applicable laws and regulations;

3.4 ضوابط لضمان الامتثال للقوانين واللوائح المعمول بها؛

3.5. methods for maintaining confidentiality of information; and

3.5 طرق الحفاظ على سرية المعلومات؛ و

3.6. procedures for regular monitoring and auditing of all corporate governance arrangements.

3.6 إجراءات المراقبة والتدقيق المنتظمين لجميع ترتيبات الحوكمة المؤسسية.

Risk Management

إدارة المخاطر

4. Payment Service Providers must have and maintain robust and comprehensive policies and procedures to identify, manage, monitor and

4. يجب أن يكون لدى مقدمي خدمات الدفع سياسات وإجراءات قوية وشاملة وأن يحافظوا عليها لتحديد، إدارة، مراقبة والإبلاغ عن المخاطر الناشئة عن توفير

خدمات الدفع للتجزئة التي يتعرضون أو قد يتعرضون لها، وإجراءات الرقابة الداخلية المناسبة، بما في ذلك الإجراءات الإدارية والمحاسبية.

report the risks arising from the provision of Retail Payment Services to which they are or might become exposed, and adequate internal control mechanisms, including sound administrative and accounting procedures.

5. يجب أن تكون سياسات وإجراءات إدارة المخاطر الخاصة بمقدمي خدمات الدفع:

5. Payment Service Providers' risk management policies and procedures shall be:

5.1 محدثة؛

5.1. kept up-to-date;

5.2 خاضعة للمراجعة سنوياً؛ و

5.2. reviewed annually; and

5.3 متناسبة مع طبيعة، حجم وتعقيد خدمات الدفع للتجزئة المقدمة.

5.3. proportionate to the nature, scale and complexity of the Retail Payment Services provided.

6. يجب على مقدمي خدمات الدفع إحداث وظيفة لإدارة المخاطر، وظيفة تدقيق داخلي ووظيفة امتثال.

6. Payment Service Providers must establish a risk management function, an internal audit function and a compliance function.

المحاسبة والتدقيق

Accounting and Audit

7. يجب على مقدمي خدمات الدفع تعيين مدقق ليقوم على أساس سنوي بتدقيق التالي:

7. Payment Service Providers must appoint an Auditor to audit on an annual basis:

7.1 القوائم المالية أو القوائم المالية الموحدة لمقدم خدمات الدفع المعدة وفقًا للمعايير والممارسات المحاسبية المقبولة؛ و

7.1. the financial statements or consolidated financial statements of the Payment Service Provider prepared in accordance with the accepted accounting standards and practices; and

7.2 أنظمة وضوابط خدمات الدفع للتجزئة التي يقدمها مقدم خدمات الدفع، بشكل منفصل عن أي تدقيق يتناول خدمات الدفع الأخرى التي لا تشكل خدمات دفع للتجزئة.

7.2. the systems and controls of the Retail Payment Services provided by the Payment Service Provider, separately from any audit on non-Retail Payment Services.

8. بناءً على طلب المصرف المركزي، يجب على المدقق المعين أن يقدم، مباشرة أو من خلال مقدم خدمات الدفع، تقرير التدقيق في شكل وفي إطار زمني مقبولين من المصرف المركزي.

8. Upon request by the Central Bank, the appointed Auditor shall submit, directly or through the Payment Service Provider, a report of the audit in a form and within a timeframe acceptable to the Central Bank.

9. بالإضافة إلى تقرير التدقيق، يجوز للمصرف المركزي أن يطلب من المدقق ما يلي:

9. In addition to the report of audit, the Central Bank may request from the Auditor to:

9.1. submit any additional information in relation to the audit, if the Central Bank considers it necessary;

9.1 تقديم أي معلومات إضافية تتعلق بالتدقيق، إذا اعتبر المصرف المركزي ذلك ضروريًا؛

9.2. enlarge or extend the scope of the audit;

9.2 توسيع أو تمديد نطاق التدقيق؛

9.3. carry out any other examination.

9.3 إجراء أي مراجعة أخرى.

Record Keeping

الاحتفاظ بالسجلات

10. Payment Service Providers shall keep all necessary records on Personal and Payment Data for a period of (5) years from the date of receipt of such data, unless otherwise required by other applicable laws or the Central Bank.

10. يجب على مقدمي خدمات الدفع الاحتفاظ بجميع السجلات الضرورية الخاصة بالبيانات الشخصية وبيانات الدفع لمدة (5) سنوات من تاريخ استلام هذه البيانات، ما لم تفرض القوانين الأخرى المعمول بها أو المصرف المركزي خلاف ذلك.

Notification Requirements

متطلبات الإخطار

11. Where any material change affects the accuracy and completeness of information provided in an Application, the Applicant or Payment Service Provider, as the case may be, shall immediately notify the Central Bank of such change and provide all necessary information and documents.

11. يجب على مقدم الطلب أو مقدم خدمات الدفع، بحسب الحالة، عند حصول أي تغيير جوهري من شأنه التأثير على صحة واكتمال المعلومات المقدمة في الطلب، إخطار المصرف المركزي فوراً بهذا التغيير وتقديم جميع المعلومات والمستندات اللازمة.

12. A Payment Service Provider shall immediately notify the Central Bank of any violation or potential violation of a Major Regulatory Requirement of this Regulation or Level 2 Acts.

12. يجب على مقدم خدمات الدفع إخطار المصرف المركزي فوراً بأي مخالفة مؤكدة أو محتملة لأحد المتطلبات الرقابية الرئيسية المنصوص عليها في هذا النظام أو في أحكام المستوى الثاني.

13. A Payment Service Provider shall immediately notify the Central Bank if it becomes aware that any of the following events have occurred or are likely to occur:

13. يجب على مقدم خدمات الدفع إخطار المصرف المركزي فوراً إذا علم بوقوع أو احتمال حدوث أي من الأحداث التالية:

13.1. any event that prevents access to or disrupts the operations of the Payment Service Provider;

13.1 أي حدث يمنع الوصول إلى عمليات مقدم خدمات الدفع أو يعطلها؛

13.2. any legal action taken against the Payment Service Provider either in the State or in a Third Country;

13.2 أي إجراء قانوني تم اتخاذه تجاه مقدم خدمات الدفع سواء في الدولة أو في دولة ثالثة؛

13.3. the commencement of any insolvency, winding up, liquidation or equivalent proceedings, or the appointment of

13.3 بدء أي إجراءات إفلاس أو حل أو تصفية أو إجراءات مماثلة، أو تعيين أي حارس

any receiver, administrator or provisional liquidator under the laws of any country;

قضائي أو إداري أو مصفٍ مؤقت بموجب قوانين أي دولة؛

13.4. any disciplinary measure or sanction taken against the Payment Service Provider or imposed on it by a regulatory body other than the Central Bank, whether in the State or in a Third Country;

13.4 أي إجراء تأديبي أو عقوبة تم اتخاذه تجاه مقدم خدمات الدفع أو فرض عليه من قبل هيئة رقابية فيما عدا المصرف المركزي، سواء في الدولة أو في دولة ثالثة؛

13.5. any change in regulatory requirements to which it is subject beyond those of the Central Bank, whether in the State or in a Third Country; and

13.5 أي تغيير في المتطلبات الرقابية التي يخضع لها فيما عدا متطلبات المصرف المركزي، سواء في الدولة أو في دولة ثالثة؛ و

13.6. any other event specified by the Central Bank.

13.6 أي حدث آخر يحدده المصرف المركزي.

Professional Indemnity Insurance

تأمين التعويض المهني

14. Payment Service Providers providing Payment Initiation and Payment Account Information Services shall hold a professional indemnity insurance whose amount shall be decided upon by the Central Bank.

14. يلتزم مقدمو خدمات الدفع الذين يقدمون خدمات إنشاء الدفع وخدمات معلومات حساب الدفع الحصول على تأمين التعويض المهني بالقيمة التي يحددها المصرف المركزي.

15. The professional indemnity insurance of Payment Service Providers providing Payment Initiation Services referred to in paragraph (14) shall cover these Payment Service Providers' liabilities for Unauthorized Payment Transactions and non-execution, defective or late execution of Payment Transactions.

15. يجب أن يغطي تأمين التعويض المهني لمقدمي خدمات الدفع الذين يقدمون خدمات إنشاء الدفع المشار إليها في البند (14) مسؤوليات مقدمي خدمات الدفع عن معاملات الدفع غير المصرح بها، وعن عدم التنفيذ، التنفيذ المعيب أو المتأخر لمعاملات الدفع.

16. The professional indemnity insurance of Payment Service Providers providing Payment Account Information Services referred to in paragraph (14) shall cover these Payment Service Providers' liability vis-à-vis the Payment Service Provider providing Account Issuance Services or the Retail Payment Service User resulting from non-authorized or fraudulent access to or non-authorized or fraudulent use of Payment Account information.

16. يجب أن يغطي تأمين التعويض المهني لمقدمي خدمات الدفع الذين يقدمون خدمات معلومات حساب الدفع المشار إليها في البند (14) مسؤولية مقدمي خدمات الدفع تجاه مقدم خدمات الدفع الذي يقدم خدمات إصدار الحساب أو مستخدم خدمات الدفع للتجزئة الناتجة عن الوصول أو الاستخدام غير المصرح بهما أو المشبوهين لمعلومات حساب الدفع.

Article (11) Payment Token Services

المادة (11): خدمات رمز الدفع

1. This Article (11) is without prejudice to other provisions of this Regulation that are relevant to Payment Service Providers providing Payment Token Services.

1. لا تخل هذه المادة (11) بالأحكام الأخرى من هذا النظام ذات الصلة بمقدمي خدمات الدفع الذين يقدمون خدمات رمز الدفع.

2. For the avoidance of doubt, Payment Token Services do not include Security Token, Commodity Token and Virtual Asset Token and the provision of services associated with the same.

2. لتجنب الشك، لا تشمل خدمات رمز الدفع رمز الأوراق المالية، رمز السلع ورمز الأصول الافتراضية وتقديم الخدمات المرتبطة بها.

3. Security Token and Commodity Token fall within the jurisdiction of the Securities and Commodities Authority and as such are regulated by the Securities and Commodities Authority.

3. يكون رمز الأوراق المالية ورمز السلع من اختصاص هيئة الأوراق المالية والسلع، وبالتالي يتم تنظيمهما والرقابة عليهما من هيئة الأوراق المالية والسلع.

4. Virtual Asset Tokens, although may be accepted as a means of payment, are not generally accepted as a medium of exchange due to the lack of stability and high volatility in their market value. As a result, any services associated with Virtual Asset Tokens, including Virtual Asset Token Services, fall outside the scope of this Regulation.

4. على الرغم من إمكانية قبول رموز الأصول الافتراضية كوسيلة للدفع، إلا أنها غير مقبولة بشكل عام كوسيلة للتبادل بسبب عدم الاستقرار والتقلبات العالية في قيمتها السوقية. ونتيجةً لذلك، فإن أي خدمات مرتبطة برموز الأصول الافتراضية، بما في ذلك خدمات رموز الأصول الافتراضية تكون خارج نطاق هذا النظام.

Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations

مواجهة غسل الأموال ومكافحة تمويل الإرهاب والتنظيمات غير المشروعة

5. Payment Token Services shall be considered to carry high money laundering and terrorist financing risk due to their speed, anonymity and cross-border nature. In line with the FATF standards, Payment Services Providers providing Payment Token Services shall undertake risk assessment and take appropriate measures to manage and mitigate the identified risks in accordance with applicable legal and regulatory requirements. Payment Service Providers providing Payment Token Services shall comply with the FATF Guidance for a Risk-based Approach to Virtual Assets and Virtual Assets Service Providers, as may be supplemented from time to time, or any related

5. تنطوي خدمات رمز الدفع على مخاطر عالية فيما يتعلق بغسل الأموال وتمويل الإرهاب بسبب سرعة تداولها، إخفاء الهوية وطبيعتها العابرة للحدود. تماشياً مع معايير مجموعة العمل المالي، يجب على مقدمي خدمات الدفع الذين يقدمون خدمات رمز الدفع إجراء تقييم للمخاطر واتخاذ التدابير المناسبة لإدارة المخاطر المحددة والتخفيف منها وفقًا للمتطلبات القانونية والرقابية المعمول بها. يجب على مقدمي خدمات الدفع الذين يقدمون خدمات رمز الدفع الامتثال لإرشادات مجموعة العمل المالي الخاصة بالنهج القائم على المخاطر للأصول الافتراضية ومقدمي خدمات الأصول الافتراضية، كما يمكن استكماله من وقت

standards or guidance in assessing and managing risks in Payment Token Services.

لآخر، أو أي معايير أو إرشادات ذات صلة في تقييم وإدارة المخاطر الخاصة بخدمات رمز الدفع.

Technology Risk and Information Security

مخاطر التكنولوجيا وأمن المعلومات

Security Requirements

المتطلبات الأمنية

6. A Payment Service Provider providing Payment Token Services shall have a good understanding of the security risks and vulnerabilities of each Payment Token provided. It shall carry out a security risk assessment for each Payment Token.

6. يجب أن يكون لدى مقدم خدمات الدفع الذي يقدم خدمات رمز الدفع فهم جيد للمخاطر الأمنية والثغرات الخاصة بكل رمز دفع مقدم من قبله. كما يجب عليه إجراء تقييم للمخاطر الأمنية لكل رمز دفع.

Cyber Security Risk

مخاطر الأمن السيبراني

7. Payment Service Providers providing Payment Token Services whose monthly average value of Payment Transactions amounts to ten (10) million Dirhams or above shall regularly assess the necessity to perform penetration and cyber-attack simulation testing. Coverage and scope of testing shall be based on the cyber security risk profile, cyber intelligence information available, covering not only networks (both external and internal) and application systems but also social engineering and emerging cyber threats. A Payment Service Provider shall also take appropriate actions to mitigate the issues, threats and vulnerabilities identified in penetration and cyber-attack simulation testing in a timely manner, based on the impact and risk exposure analysis.

7. يجب على مقدمي خدمات الدفع الذين يقدمون خدمات رمز الدفع والذين يبلغ متوسط القيمة الشهرية لمعاملات الدفع الخاصة بهم عشرة (10) ملايين درهم أو ما فوق القيام بتقييم دوري لضرورة إجراء اختبار محاكاة الاختراق والهجوم السيبراني. يجب أن تستند التغطية ونطاق الاختبار إلى ملف تحديد مخاطر الأمن السيبراني، والمعلومات الاستخباراتية السيبرانية المتاحة، والتي لا تغطي الشبكات (الخارجية والداخلية) وأنظمة التطبيقات فحسب، بل تشمل أيضاً الهندسة الاجتماعية والتهديدات السيبرانية الناشئة. كما يجب على مقدم خدمات الدفع اتخاذ الإجراءات المناسبة للتخفيف من المشاكل، التهديدات والثغرات التي تم تحديدها في اختبار محاكاة الاختراق والهجمات السيبرانية في الوقت المناسب، بناءً على تحليل التأثير والتعرض للمخاطر.

Specific Obligations for Providing Retail Payment Service on Payment Tokens

التزامات خاصة لتقديم خدمات الدفع للتجزئة على رموز الدفع

Reserve of Assets

احتياطي الأصول

8. Payment Service Providers issuing Payment Tokens shall keep and maintain at all times a Reserve of Assets per category of Payment Token issued.

8. يجب على مقدمي خدمات الدفع الذين يصدرون رموز الدفع الابقاء على والاحتفاظ في جميع الأوقات باحتياطي الأصول لكل فئة من رموز الدفع المصدرة.

9. Payment Service Providers issuing Payment Tokens shall ensure effective and prudent

9. يجب على مقدمي خدمات الدفع الذين يصدرون رموز الدفع ضمان إدارة فعالة وحكيمة لاحتياطي الأصول.

management of the Reserve of Assets. They shall ensure that the creation and destruction of Payment Tokens is matched by a corresponding increase or decrease in the Reserve of Assets and that such increase or decrease is adequately managed to avoid any adverse impacts on the market of the Reserve Assets.

يجب عليهم التأكد من أن إنشاء وتدمير رموز الدفع يقابله زيادة أو نقصان في احتياطي الأصول، كما يجب أن تتم إدارة هذه الزيادة أو النقصان بشكل مناسب لتجنب أي آثار سلبية على سوق الأصول الاحتياطية.

Stabilisation Mechanism

آلية المحافظة على الاستقرار

10. Payment Service Providers issuing Payment Tokens shall have and maintain a clear and detailed policy on the selected stabilisation mechanism. That policy and procedure shall in particular:

10. يجب أن يعتمد ويحافظ مقدمو خدمات الدفع الذين يصدرون رموز الدفع على سياسة واضحة ومفصلة حول الآلية المختارة للمحافظة على الاستقرار، على ان تتضمن هذه السياسة والإجراءات على وجه الخصوص:

10.1 describe the type, allocation and composition of the reference assets the value of which aims at stabilising the value of the Payment Tokens;

10.1 وصف نوع، تخصيص وتكوين الأصول المرجعية التي تهدف قيمتها إلى تثبيت قيمة رموز الدفع؛

10.2 contain a detailed assessment of the risks, including credit risk, counterparty risk, market risk and liquidity risk, resulting from the Reserve of Assets;

10.2 تناول تقييم مفصل للمخاطر، بما في ذلك مخاطر الائتمان، المخاطر المرتبطة بالطرف المقابل، مخاطر السوق ومخاطر السيولة الناتجة عن احتياطي الأصول؛

10.3 describe the procedure for the creation and destruction of Payment Tokens and the consequence of such creation or destruction on the increase and decrease of the Reserve of Assets;

10.3 وصف آلية إنشاء وتدمير رموز الدفع ونتائج هذا الإنشاء أو التدمير على زيادة أو نقصان احتياطي الأصول؛

10.4 provide information on whether the Reserve of Assets is invested, and where part of the Reserve of Assets is invested, describe in detail the investment policy and contain an assessment of how that investment policy can affect the value of the Reserve of Assets; and

10.4 تقديم معلومات حول ما إذا كان احتياطي الأصول مستثمرًا، وفي حال استثمار جزء من احتياطي الأصول، وصف تفصيلي لسياسة الاستثمار وتناول تقييم لكيفية تأثير سياسة الاستثمار هذه على قيمة احتياطي الأصول؛ و

10.5 describe the procedure to purchase and redeem Payment Tokens against the Reserve of Assets, and list the persons who are entitled to such redemption.

10.5 وصف إجراءات شراء واسترداد رموز الدفع مقابل احتياطي الأصول، ووضع قائمة بالأشخاص الذين يحق لهم الاسترداد.

11. Payment Service Providers issuing Payment Tokens shall ensure an independent audit of the Reserve of Assets on a bi-annual basis as from the receipt of the Central Bank's approval of the White Paper with respect of the Payment Tokens.

11. يجب على مقدمي خدمات الدفع الذين يصدرون رموز الدفع التأكد من إجراء تدقيق مستقل لاحتياطي الأصول على أساس نصف سنوي اعتبارًا من استلام موافقة المصرف المركزي على الورقة البيضاء فيما يتعلق برموز الدفع.

Custody / *الحفظ*

12. Payment Service Providers issuing Payment Tokens shall establish, maintain and implement custody policies, procedures and contractual arrangements for each category of issued Payment Tokens that ensure at all times that:

12. يتعين على مقدمي خدمات الدفع الذين يصدرون رموز الدفع وضع والاحتفاظ وتنفيذ سياسات وإجراءات وترتيبات تعاقدية لحفظ كل فئة من فئات رموز الدفع الصادرة والتي تضمن في جميع الأوقات ما يلي:

12.1 the Reserve of Assets is segregated from the Payment Service Provider's own assets;

12.1 فصل احتياطي الأصول عن الأصول الخاصة بمقدم خدمات الدفع؛

12.2 the Reserve of Assets is not encumbered or pledged;

12.2 كون احتياطي الأصول غير مرهون؛

12.3 the Reserve of Assets is held in custody in accordance with paragraph (14); and

12.3 .حفظ احتياطي الأصول بموجب البند (14)؛ و

12.4 the Payment Service Providers have prompt access to the Reserve of Assets to meet any redemption requests from the holders of Payment Token.

12.4. تمتع مقدمي خدمات الدفع بإمكانية الوصول الفوري إلى احتياطي الأصول لتلبية أي طلبات استرداد من حاملي رمز الدفع.

13 The assets received in exchange for the Payment Tokens shall be held in custody by no later than (5) Business Days after the issuance of the Payment Tokens by:

13. سيتم حفظ الأصول المستلمة مقابل رموز الدفع لفترة لا تزيد عن (5) أيام عمل بعد إصدار رموز الدفع من خلال:

13.1 Bank; or

13.1 البنك؛ أو

13.2 Payment Service Provider providing Payment Token Custody.

13.2 مقدم خدمات الدفع الذي يقوم بحفظ رمز الدفع.

Investment of the Reserve of Assets / *استثمار احتياطي الأصول*

14 Payment Service Providers issuing Payment Tokens that invest a portion of the Reserve of

14. يتعين على مقدمي خدمات الدفع من مصدري رموز الدفع الذين يستثمرون جزءًا من احتياطي الأصول

Assets shall invest those assets only in highly liquid financial instruments with minimal market and credit risk. The investments shall be capable of being liquidated rapidly with minimal adverse price effect.

استثمار تلك الأصول فقط في أدوات مالية عالية السيولة مع حد أدنى من مخاطر السوق والائتمان. يجب أن تكون الاستثمارات قابلة للتصفية بسرعة وبأدنى تأثير سلبي على السعر.

15 All profits or losses, including fluctuations in the value of the financial instruments referred to in paragraph (14), and any counterparty or operational risks that result from the investment of the assets shall be borne by Payment Service Providers issuing the Payment Tokens.

15. يتحمل مقدمو خدمات الدفع الذين يصدرون رموز الدفع جميع الأرباح أو الخسائر، بما في ذلك التقلبات في قيمة الأدوات المالية المشار إليها في البند (14)، وأي مخاطر مرتبطة بالطرف المقابل أو مخاطر تشغيلية ناتجة عن استثمار الأصول.

Pre-Trade Transparency — *الشفافية السابقة للتداول*

16 Payment Service Providers that engage in Facilitating the Exchange of Payment Tokens shall disclose to its Retail Payment Service Users and the public as appropriate, on a continuous basis during normal trading, the following information relating to trading of each accepted Payment Tokens on their platform:

16. يجب على مقدمي خدمات الدفع الذين يقومون بتسهيل تداول رموز الدفع الإفصاح لمستخدمي خدمات الدفع للتجزئة وللجمهور حسب الحاجة، على أساس مستمر أثناء التداول العادي، عن المعلومات التالية المتعلقة بتداول كل رمز من رموز الدفع المقبولة على منصتهم:

16.1 the current bid, offer prices and volume;

16.1 العطاء الحالي وأسعار وحجم العرض؛

16.2 the depth of trading interest shown at the prices and volumes advertised through their systems for the accepted Payment Tokens; and

16.2 مدى الإقبال على التداول الظاهر من خلال الأسعار والأحجام المُعلن عنها من خلال أنظمتهم لرموز الدفع المقبولة؛ و

16.3 any other information relating to accepted Payment Tokens which would promote transparency relating to trading.

16.3 أي معلومات أخرى تتعلق برموز الدفع المقبولة والتي من شأنها تعزيز الشفافية المتعلقة بالتداول.

17 Payment Service Providers that engage in Facilitating the Exchange of Payment Tokens shall use appropriate mechanisms to enable pre-trade information to be made available to the public in an easy to access and uninterrupted manner.

17. يجب على مقدمي خدمات الدفع الذين يقومون بتسهيل تداول رموز الدفع استخدام الآليات المناسبة لتمكين إتاحة معلومات ما قبل التداول للجمهور بطريقة سهلة الوصول إليها ودون انقطاع.

Post-Trade Transparency — *الشفافية بعد التداول*

18 Payment Service Providers that engage in Facilitating the Exchange of Payment Tokens

18. يجب على مقدمي خدمات الدفع الذين يقوم بتسهيل تداول رموز الدفع الإفصاح للجمهور عن سعر، حجم

shall disclose the price, volume and time of the Payment Transactions executed in respect of accepted Payment Tokens to the public as close to real-time as is technically possible on a nondiscretionary basis. They shall use adequate mechanisms to enable post-trade information to be made available to the public in an easy to access and uninterrupted manner, at least during business hours.

ووقت معاملات الدفع المنفذة فيما يخص رموز الدفع المقبولة في أقرب وقت ممكن من الناحية الفنية على أساس غير تقديري. يجب عليهم استخدام آليات مناسبة لتمكين إتاحة معلومات ما بعد التداول للجمهور بطريقة سهلة الوصول ودون انقطاع، أقله خلال ساعات العمل.

Article (12) Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations

المادة (12): مواجهة غسل الأموال ومكافحة تمويل الإرهاب والتنظيمات غير المشروعة

1. Payment Service Providers must comply with the relevant UAE AML Laws and Regulations and address money laundering and terrorist financing risks through appropriate preventive measures to deter abuse of the sector as a conduit for illicit funds, and detect money laundering and terrorist financing activities and report any suspicious transactions to the Financial Intelligence Department at the Central Bank.

1. يجب على مقدمي خدمات الدفع الامتثال للقوانين والمتطلبات الرقابية ذات الصلة لمواجهة غسل الأموال والتصدي لمخاطر غسل الأموال وتمويل الإرهاب من خلال تدابير وقائية مناسبة لردع إساءة استخدام القطاع كقناة للأموال غير المشروعة، والكشف عن أنشطة غسل الأموال وتمويل الإرهاب والإبلاغ عن أي معاملات مشبوهة إلى دائرة المعلومات المالية في المصرف المركزي.

2. Payment Service Providers must have comprehensive and effective internal AML/CFT policies, procedures and controls in place. Payment Service Providers shall be prohibited from invoking banking, professional or contractual secrecy as a pretext for refusing to perform their statutory reporting obligation in regard to suspicious activity.

2. يجب على مقدمي خدمات الدفع أن يكون لديهم سياسات وإجراءات وضوابط داخلية متكاملة وفعالة لمواجهة غسل الأموال ومكافحة تمويل الإرهاب. يحظر على مقدمي خدمات الدفع اتخاذ السرية المصرفية، المهنية أو التعاقدية كذريعة لرفض أداء التزامهم القانوني بالإبلاغ عن النشاط المشبوه.

3. Payment Service Providers must identify, assess, and understand the ML/FT risks to which they are exposed and conduct enterprise-level and business relationship-specific risk assessments. Accordingly, all AML/CFT CDD, monitoring and controls must be risk-based and aligned to the risk assessments.

3. يجب على مقدمي خدمات الدفع تحديد، تقييم وفهم مخاطر غسل الأموال / تمويل الإرهاب التي يتعرضون لها وإجراء تقييمات للمخاطر على المستوى المؤسسي وعلاقات العمل. وبناءً على ذلك، يجب أن تكون كافة عمليات العناية الواجبة تجاه العملاء بشأن مواجهة غسل الأموال / ومكافحة تمويل الإرهاب، والمراقبة والضوابط قائمة على ومتماشية مع تقييمات المخاطر.

4. Payment Service Providers shall undertake periodic risk profiling of Retail Payment Service Users and assessment based on the AML/CFT requirements.

4. يجب على مقدمي خدمات الدفع إجراء معالجة دورية للمخاطر لمستخدمي خدمات الدفع للتجزئة وتقييمها بناءً على متطلبات مواجهة غسل الأموال ومكافحة تمويل الإرهاب.

5. Payment Service Providers shall assess whether a business relationship presents a higher money laundering and terrorist financing risk and assign a related risk rating. Payment Service Providers shall be prohibited from dealing in any way with shell banks or other shell financial institutions and from establishing or maintaining any business relationship or conducting any Payment Transaction under an anonymous or fictitious name or by pseudonym or number.

5. يجب على مقدمي خدمات الدفع تقييم ما إذا كانت علاقة العمل تنطوي على مخاطر غسل الأموال وتمويل الإرهاب أعلى وتحديد التصنيف المناسب لتلك المخاطر. يُحظر على مقدمي خدمات الدفع التعامل بأي شكل من الأشكال مع البنوك أو المؤسسات المالية الأخرى الوهمية وإنشاء أي علاقة عمل أو الحفاظ عليها أو إجراء أي معاملة دفع تحت اسم مجهول أو وهمي أو اسم أو رقم مستعار.

6. Payment Service Providers shall ensure that their CDD models are designed to address the specific risks posed by a Retail Payment Service User profile and Payment Instrument features. Payment Service Providers shall be prohibited from establishing or maintaining any business relationship or executing any Payment Transaction in the event that they are unable to complete adequate risk-based CDD measures for any reason.

6. يجب على مقدمي خدمات الدفع التأكد من أن نماذج العناية الواجبة تجاه العملاء الخاصة بهم مصممة لمعالجة المخاطر التي يثيرها الملف التعريفي لمستخدم خدمات الدفع للتجزئة وخصائص أدوات الدفع. يُحظر على مقدمي خدمات الدفع إنشاء أي علاقة أعمال أو الحفاظ عليها أو تنفيذ أي معاملة دفع في حالة عدم تمكنهم لأي سبب من الأسباب من إكمال الإجراءات المناسبة للعناية الواجبة للعملاء والقائمة على المخاطر.

7. Payment Service Providers providing Retail Payment Services must undertake certain CDD measures concerning Wire Transfers as stipulated in the relevant provisions of the AML Law if Wire Transfer services are provided by Payment Service Providers. Payment Service Providers should introduce appropriate systems for screening, as part of the CDD process, on all parties involved in a transaction against all applicable sanction lists (i.e. the UN sanction lists and the names contained in the 'search notices'/'search and freeze notices' issued by the Central Bank).

7. يجب على مقدمي خدمات الدفع الذين يقدمون خدمات الدفع للتجزئة اتخاذ بعض إجراءات العناية الواجبة تجاه العملاء فيما يتعلق بالتحويلات الإلكترونية على النحو المنصوص عليه في الأحكام ذات الصلة من قانون مواجهة غسل الأموال إذا كان مقدمو خدمات الدفع يقدمون خدمات التحويل الإلكتروني. يجب على مقدمي خدمات الدفع، كجزء من إجراءات العناية الواجبة تجاه العملاء، وضع أنظمة مناسبة لفحص جميع الأطراف المشاركة في معاملة بالاستناد إلى جميع قوائم الجزاءات المعمول بها (أي قوائم الجزاءات الموحدة للأمم المتحدة والأسماء الواردة في "بلاغات البحث" / "بلاغات البحث والتجميد" الصادرة عن المصرف المركزي).

8. If Payment Service Providers provide the service of Wire Transfers, they should take freezing action and prohibit conducting transactions with designated persons and entities, as per the obligations set out in the Central Bank's Notice 103/2020 on the Implementation of United Nations Security Council (UNSC) and the UAE

8. إذا كان مقدمو خدمات الدفع يقدمون خدمة التحويلات الإلكترونية، فيجب عليهم اتخاذ إجراءات التجميد وحظر إجراء المعاملات مع الأشخاص والكيانات المحددة، وفقًا للالتزامات المنصوص عليها في تعميم المصرف المركزي رقم 2020/103 بشأن تنفيذ مجلس أمن الأمم المتحدة (مجلس الأمن – الأمم

المتحدة) وقرارات مجلس الوزراء في دولة الإمارات العربية المتحدة بشأن مجلس الأمن والقوائم المحلية، وتعديلاتها من وقت لآخر.

Cabinet Resolutions regarding UNSC and Local Lists, as amended from time to time.

9. يجب على مقدمي خدمات الدفع الاسترشاد بمعايير مجموعة العمل المالي الخاصة بمواجهة غسل الأموال ومكافحة تمويل الإرهاب وانتشار التسلح. يجب على مقدمي خدمات الدفع ادراج المراجعة المنتظمة لاتجاهات وأنماط غسل الأموال / تمويل الإرهاب في برامج التدريب حول الامتثال الخاصة بهم وكذلك في إجراءات تحديد المخاطر وتقييمها.

9. Payment Service Providers should also be guided by the Financial Action Task Force (FATF) Standards on anti-money laundering and countering the financing of terrorism and proliferation. Payment Service Providers should incorporate the regular review of ML/FT trends and typologies into their compliance training programmes as well as into their risk identification and assessment procedures.

المادة (13): مخاطر التكنولوجيا وأمن المعلومات

Article (13) Technology Risk and Information Security

1. يجب على مقدمي خدمات الدفع الامتثال لهذه المادة (13) ويتم تشجيعهم للرجوع إلى الملحق 2 للحصول على إرشادات حول أفضل الممارسات الخاصة بمخاطر التكنولوجيا وأمن المعلومات.

1. Payment Service Providers shall comply with this Article (13) and are encouraged to consult Annex II for the Guidance on the best practices for technology risk and information security.

مخاطر التكنولوجيا

Technology Risk

2. ينبغي على مقدمي خدمات الدفع الأخذ بعين الاعتبار أفضل الممارسات والمعايير الدولية عند تصميم وتنفيذ أنظمة وإجراءات إدارة مخاطر التكنولوجيا والمخاطر الخاصة.

2. Payment Service Providers are expected to take into account international best practices and standards when designing and implementing the technology and specific risk management systems and processes.

3. يجب على مقدم خدمات الدفع إنشاء إطار فعال لإدارة مخاطر التكنولوجيا والأمن السيبراني لضمان ملاءمة ضوابط تكنولوجيا المعلومات، المرونة السيبرانية، الجودة والأمان، بما في ذلك موثوقية وقوة واستقرار وتوفر أنظمة الحاسوب لديها بالإضافة إلى سلامة وكفاءة عمليات خدمات الدفع للتجزئة. يجب أن يفي الإطار بالغرض وأن يتناسب مع المخاطر المرتبطة بطبيعة، حجم، تعقيد، ونوع الأعمال والعمليات، ومع التقنيات المعتمدة ونظام إدارة المخاطر الشامل لمقدم خدمات الدفع. وينبغي النظر في اعتماد المعايير والممارسات الدولية المعترف بها عند صياغة إطار إدارة المخاطر.

3. A Payment Service Provider shall establish an effective technology and cyber security risk management framework to ensure the adequacy of IT controls, cyber resilience, the quality and security, including the reliability, robustness, stability and availability, of its computer systems, and the safety and efficiency of the operations of Retail Payment Services. The framework shall be “fit for purpose” and commensurate with the risks associated with the nature, size, complexity and types of business and operations, the technologies adopted and the overall risk management system of the Payment Service Provider. Consideration shall be given to

adopting recognized international standards and practices when formulating such risk management framework.

4. A Payment Service Provider's effective technology risk management framework shall comprise proper IT governance, a continuous technology risk management process and implementation of sound IT control practices.

4. يجب أن يحتوي إطار إدارة مخاطر التكنولوجيا الفعال لمقدم خدمات الدفع على حوكمة مناسبة لتكنولوجيا المعلومات، إجراءات مستمرة لإدارة مخاطر التكنولوجيا وتنفيذ الممارسات السليمة لضوابط تكنولوجيا المعلومات.

5. A Payment Service Provider shall establish a general framework for management of major technology-related projects, such as in-house software development and acquisition of information systems. This framework shall specify, among other things, the project management methodology to be adopted and applied to these projects.

5. يجب على مقدم خدمات الدفع وضع إطار عام لإدارة المشاريع الرئيسية المتعلقة بالتكنولوجيا، مثل تطوير البرمجيات داخلياً واقتناء أنظمة المعلومات. يجب أن يحدد هذا الإطار، من بين أمور أخرى، منهجية إدارة المشاريع التي سيتم اعتمادها وتطبيقها على هذه المشاريع.

6. Payment Service Provider shall apply and meet at a minimum the UAE Information Assurance Standards, as may be amended from time to time.

6. يجب على مقدمي خدمات الدفع الامتثال والتقيد كحد أدنى بمعايير ضمان أمن المعلومات في الدولة، وما قد يطرأ عليها من تعديلات من وقت لآخر.

IT Governance

حوكمة تكنولوجيا المعلومات

7. A Payment Service Provider shall establish a proper IT governance framework. IT governance shall cover various aspects, including a clear structure of IT functions and the establishment of IT control policies. While there could be different constructs, the major functions shall include an effective IT function, a robust technology risk management function, and an independent technology audit function.

7. يجب على مقدم خدمات الدفع وضع إطار حوكمة مناسب لتكنولوجيا المعلومات، على أن تتناول جوانب مختلفة، بما في ذلك هيكل واضح للوظائف وسياسات المراقبة. في حين قد توجد هياكل مختلفة، يجب أن تشمل الوظائف الرئيسية وظيفة فعالة لتكنولوجيا المعلومات، وظيفة قوية لإدارة مخاطر التكنولوجيا، ووظيفة مستقلة للتدقيق بشؤون التكنولوجيا.

8. The Board, or a committee designated by the Board shall be responsible for ensuring that a sound and robust risk management framework is established and maintained to manage technology risks in a manner that is commensurate with the risks posed by the Payment Service Provider's Retail Payment Activities.

8. يكون المجلس، أو اللجنة المعينة من قبله، مسؤول عن ضمان إنشاء إطار سليم وقوي لإدارة المخاطر والمحافظة عليه لإدارة مخاطر التكنولوجيا بطريقة تتناسب مع المخاطر التي تشكلها أنشطة الدفع للتجزئة لمقدم خدمات الدفع.

Security Requirements **المتطلبات الأمنية**

9. A Payment Service Provider must define clearly its security requirements in the early stage of system development or acquisition as part of business requirements and adequately built during the system development stage.

9. يجب على مقدم خدمات الدفع أن يحدد بوضوح متطلباته الأمنية في مرحلة مبكرة من تطوير النظام أو اقتنائه كجزء من متطلبات العمل، وأن يدرج تلك المتطلبات بشكل مناسب خلال مرحلة تطوير النظام.

10. A Payment Service Provider using the Agile methods to accelerate software development must incorporate adequate security practices to ensure the software is not compromised at any stage in its development process.

10. يجب على مقدم خدمات الدفع الذي يستخدم أساليب أجايل لتسريع تطوير البرامج أن يدرج الممارسات الأمنية المناسبة لضمان عدم تعرض البرامج للإختراق في أي مرحلة من مراحل عملية التطوير.

11. A Payment Service Provider that develops an Application Programming Interface (API) or provides an API shall establish safeguards to manage the development and provision of the APIs to secure the interaction and exchange of data between various software applications.

11. يجب على مقدم خدمات الدفع الذي يطور واجهة برمجة التطبيقات (API) أو يوفر واجهة برمجة التطبيقات (API) وضع ضمانات لإدارة التطوير والتوفير لواجهات برمجة التطبيقات لتأمين التفاعل وتبادل البيانات بين تطبيقات البرامج المختلفة.

Network and Infrastructure Management **إدارة الشبكة والبنية التحتية**

12. A Payment Service Provider whose monthly average value of Payment Transactions amounts to ten (10) million Dirhams or above shall clearly assign overall responsibility for network management to individuals who are equipped with expertise to fulfil their duties. Network standards, design, diagrams and operating procedures shall be formally documented, kept up-to-date, communicated to all relevant network staff and reviewed periodically.

12. يجب على مقدم خدمات الدفع الذي يبلغ متوسط القيمة الشهرية لمعاملات الدفع الخاصة به عشرة (10) ملايين درهم أو ما فوق أن يسند بوضوح المسؤولية العامة لإدارة الشبكات الى الأفراد الذين لديهم الخبرة لأداء مهامهم. يجب توثيق معايير الشبكات، تصميمها، مخططاتها وإجراءات تشغيلها رسميًا وتحديثها وإبلاغها لجميع موظفي الشبكات المعنيين ومراجعتها بشكل دوري.

13. A Payment Service Provider shall establish a security administration function and a set of formal procedures for administering the allocation of access rights to system resources and application systems, and monitoring the use of system resources to detect any unusual or unauthorized activities.

13. يجب على مقدم خدمات الدفع إنشاء وظيفة لإدارة أمن البنية التحتية ومجموعة من الإجراءات الرسمية لإدارة تعيين حقوق صلاحيات الدخول إلى موارد النظام وأنظمة التطبيقات، ومراقبة استخدام موارد النظام للكشف عن أي أنشطة غير اعتيادية أو غير مصرح بها.

14. Payment Service Providers shall exercise due care when controlling the use of and access to privileged and emergency IDs. The necessary control procedures include:

14. يجب على مقدمي خدمات الدفع توخي العناية الواجبة عند التحكم باستخدام المعرفات ذات الامتيازات ومعرفات الطوارئ والوصول إليها. تشمل إجراءات التحكم الضرورية ما يلي:

14.1. changing the default password;

14.1 تغيير كلمة المرور الافتراضية؛

14.2. implement strong password control, with minimum password length and history, password complexity as well as maximum validity period;

14.2 وضع ضوابط صارمة لكلمة المرور، مع تحديد حد أدنى لطول كلمة المرور ومرات استخدامها، وتعقيد كلمة المرور بالإضافة إلى فترة الصلاحية القصوى؛

14.3. restricting the number of privileged users;

14.3 تقيد عدد المستخدمين ذوي الامتيازات؛

14.4. implementing strong controls over remote access by privileged users;

14.4 تنفيذ ضوابط صارمة على صلاحيات الدخول عن بعد من قبل المستخدمين ذوي الامتيازات؛

14.5. granting of authorities that are strictly necessary to privileged and emergency IDs;

14.5 منح الصلاحيات الضرورية للغاية للمعرفات ذات الامتيازات ومعرفات الطوارئ؛

14.6. formal approval by appropriate senior personnel prior to being released for usage;

14.6 الموافقة الرسمية من قبل كبار الموظفين المناسبين قبل السماح بالاستخدام؛

14.7. logging, preserving and monitoring of the activities performed by privileged and emergency IDs (e.g. peer reviews of activity logs);

14.7 تسجيل، حفظ ورصد الأنشطة التي يتم تنفيذها بواسطة المعرفات ذات الامتيازات ومعرفات الطوارئ (مثل مراجعة الأقران لسجلات الأنشطة)؛

14.8. prohibiting sharing of privileged accounts;

14.8 حظر مشاركة الحسابات ذات الامتيازات؛

14.9. proper safeguard of privileged and emergency IDs and passwords (e.g. kept in a sealed envelope and locked up inside the data center); and

14.9 الحماية المناسبة للمعرفات وكلمات المرور ذات الامتيازات والطوارئ (مثل الاحتفاظ بها في مظروف مغلق ومقفل داخل مركز البيانات)؛ و

14.10. changing of privileged and emergency IDs' passwords immediately upon return by the requesters.

14.10 تغيير كلمات المرور الخاصة بالمعرفات ذات الامتيازات ومعرفات الطوارئ فور إعادتها بواسطة صاحب الطلب.

Cyber Security Risk

خطر الأمن السيبراني

15. Where a Payment Service Provider is heavily reliant on Internet and mobile technologies to deliver the Retail Payment Services it provides, cyber security risks shall be adequately managed through the Payment Service

15. في حال اعتماد مقدم خدمات الدفع بشكل كبير على تكنولوجيا الإنترنت وأجهزة الهاتف المحمول لتقديم خدمات الدفع للتجزئة التي يوفرها، يجب إدارة مخاطر الأمن السيبراني بشكل مناسب من خلال

عملية إدارة مخاطر التكنولوجيا لمقدم خدمات الدفع. يلتزم مقدم خدمات الدفع أيضًا بتوفير موارد تتمتع بمهارات كافية لضمان قدرته على تحديد المخاطر وحماية خدماته الأساسية من الهجوم، احتواء تأثير حوادث الأمن السيبراني واستعادة الخدمات.

Provider's technology risk management process. The Payment Service Provider shall also commit adequate skilled resources to ensure its capability to identify the risk, protect its critical services against the attack, contain the impact of cyber security incidents and restore the services.

16. يجب على مقدم خدمات الدفع وضع خطة استجابة وإدارة للحوادث السيبرانية لعزل والقضاء على التهديد السيبراني بسرعة واستئناف الخدمات المتأثرة في أقرب وقت ممكن. يجب أن تتضمن الخطة إجراءات الاستجابة لسيناريوهات التهديد السيبراني المعقولة.

16. A Payment Service Provider shall establish a cyber incident response and management plan to swiftly isolate and neutralize a cyber threat and to resume affected services as soon as possible. The plan shall describe procedures to respond to plausible cyber threat scenarios

17. يجب على مقدم خدمات الدفع الذي يبلغ متوسط القيمة الشهرية لمعاملات الدفع الخاصة به عشرة (10) ملايين درهم أو ما فوق أن يقوم بتقييم دوري لضرورة إجراء اختبار محاكاة الاختراق والهجوم السيبراني. يجب أن تستند التغطية ونطاق الاختبار إلى ملف تحديد مخاطر الأمن السيبراني، والمعلومات الاستخباراتية السيبرانية المتاحة، والتي لا تغطي الشبكات (الخارجية والداخلية) وأنظمة التطبيقات فحسب، بل تشمل أيضاً الهندسة الاجتماعية والتهديدات السيبرانية الناشئة. كما يجب على مقدم خدمات الدفع اتخاذ الإجراءات المناسبة للتخفيف من المشاكل، التهديدات والثغرات التي تم تحديدها في اختبار محاكاة الاختراق والهجمات السيبرانية في الوقت المناسب، بناءً على تحليل التأثير والتعرض للمخاطر.

17. Payment Service Providers whose monthly average value of Payment Transactions amounts to ten (10) million Dirhams or above shall regularly assess the necessity to perform penetration and cyber-attack simulation testing. Coverage and scope of testing shall be based on the cyber security risk profile, cyber intelligence information available, covering not only networks (both external and internal) and application systems but also social engineering and emerging cyber threats. A Payment Service Provider shall also take appropriate actions to mitigate the issues, threats and vulnerabilities identified in penetration and cyber-attack simulation testing in a timely manner, based on the impact and risk exposure analysis.

المصادقة على مستخدمي خدمات الدفع للتجزئة

Retail Payment Service User Authentication

18. يجب على مقدم خدمات الدفع اختيار وتنفيذ تقنيات مصادقة موثوقة وفعالة للتحقق من هوية وصلاحية مستخدمي خدمات الدفع للتجزئة. يجب استخدام المصادقة المتعددة العوامل للمعاملات العالية المخاطر.

18. A Payment Service Provider shall select and implement reliable and effective authentication techniques to validate the identity and authority of its Retail Payment Service Users. Multi-factor authentication shall be required for high-risk transactions.

19. يجب اعتماد الترميز من طرف إلى طرف لنقل كلمات مرور مستخدم خدمات الدفع للتجزئة بحيث لا يتم كشفها في أي من التقاطعات الوسيطة بين تطبيق

19. End-to-end encryption shall be implemented for the transmission of Retail Payment Service User passwords so that they are not exposed at any intermediate nodes between the Retail

Payment Service User mobile application or browser and the system where passwords are verified.

أو متصفح جهاز الهاتف المحمول الخاص بمستخدم خدمات الدفع للتجزئة والنظام الذي يتولى التحقق من كلمات المرور.

Login Attempts and Session Management

محاولات تسجيل الدخول وإدارة الجلسات

20. A Payment Service Provider shall implement effective controls to limit the number of login or authentication attempts (e.g. wrong password entries), implementing time-out controls and setting time limits for the validity of authentication. If one-time password is used for authentication purpose, a Payment Service Provider shall ensure that the validity period of such passwords is limited to the strict minimum necessary.

20. يجب على مقدم خدمات الدفع وضع ضوابط فعالة لعدد محاولات تسجيل الدخول والمصادقة (مثل محاولات الدخول بكلمة مرور غير صحيحة)، وتنفيذ ضوابط خاصة لنفاذ وقت جلسة الدخول ووضع قيود زمنية لصلاحية المصادقة. وفي حال استخدام كلمة مرور واحدة بهدف المصادقة، يجب على مقدم خدمات الدفع مراعاة أن تكون صلاحية مدة جلسة الدخول عند استخدام كلمات المرور أقل ما يمكن.

21. A Payment Service Provider shall have processes in place ensuring that all Payment Transactions are logged with an appropriate audit trail.

21. يجب على مقدم خدمات الدفع وضع إجراءات من شأنها ضمان تسجيل جميع عمليات الدفع في سجل تدقيق بالشكل المناسب.

Administration of Retail Payment Service User Accounts

إدارة حسابات مستخدم خدمات الدفع للتجزئة

22. Where a Payment Service Provider providing Payment Account Issuance Services allows a Retail Payment Service User to open a Payment Account through an online channel, a reliable method shall be adopted to authenticate the identity of that Retail Payment Service User. In general, the electronic know your customer (i.e. Retail Payment Service User) (eKYC) processes accepted by the Central Bank for Banks is acceptable for the customer verification and validation processes of Payment Account Issuance Services.

22. يجب على مقدم خدمات الدفع الذي يوفر خدمات إصدار حسابات الدفع عند إجازته لمستخدم خدمات الدفع للتجزئة فتح حساب دفع عن طريق القنوات الالكترونية، إتباع طريقة موثوقة للمصادقة على هوية مستخدم خدمات الدفع للتجزئة. وبشكل عام، فإن الإجراءات المتبعة حالياً لمعرفة العميل إلكترونياً (أي مستخدم خدمات الدفع للتجزئة) (أعرف عميلك إلكترونياً) المعتمدة من المصرف المركزي الخاصة بالبنوك مقبولة للمصادقة على العميل وإجراء عمليات التحقق الخاصة بخدمات إصدار حساب الدفع.

23. A Payment Service Provider shall perform adequate identity checks when any Retail Payment Service User requests a change to the Retail Payment Service User's Payment Account information or contact details that are useful for the Retail Payment Service User to receive important information or monitor the

23. يجب على مقدم خدمات الدفع القيام بالتحقق المناسب من هوية مستخدم خدمات الدفع للتجزئة عند القيام بأي طلب لتغيير معلومات حساب الدفع الخاص به او معلومات الاتصال التي يتلقى من خلالها المعلومات الهامة أو يقوم بواسطتها بمراقبة العمليات المنفذة على حساب الدفع الخاص به.

activities of the Retail Payment Service User's Payment Accounts.

24. A Payment Service Provider shall implement effective controls such as two-factor authentication, to re-authenticate the Retail Payment Service User before effecting each high-risk transaction. High-risk transactions shall, at least, include:

24. يجب على مقدم خدمات الدفع وضع ضوابط فعالة، مثل المصادقة الثنائية، لإعادة المصادقة على مستخدم خدمات الدفع للتجزئة قبل تنفيذ المعاملات العالية المخاطر. يجب أن تشمل المعاملات العالية المخاطر، على الأقل، ما يلي:

24.1 Payment Transactions that exceeded the predefined transaction limit(s);

24.1 معاملات الدفع التي تجاوزت سقف (سقوف) عدد المعاملات المحدد مسبقاً؛

24.2 Change of personal contact details; and

24.2 تغيير بيانات الاتصال الشخصية؛ و

24.3 Unless it is not practicable to implement, Payment Transactions that exceeded the aggregate rolling limit(s) (i.e. total value of Payment Transactions over a period of time).

24.3 ما لم يكن من غير العملي تنفيذه، معاملات الدفع التي تجاوزت سقف القيمة الإجمالية المسموح به (أي القيمة الإجمالية لمعاملات الدفع خلال فترة زمنية محددة).

Business Continuity

استمرارية الأعمال

25. A Payment Service Provider shall have in place an adequate business continuity management program to ensure continuation, timely recovery, or in extreme situations orderly scale-down of critical operations in the event of major disruptions caused by different contingent scenarios. An adequate business continuity management program comprises business impact analysis, recovery strategies, a business continuity plan and alternative sites for business and IT recovery.

25. يجب أن يكون لدى مقدم خدمات الدفع برنامج ملائم لإدارة استمرارية الأعمال لضمان استمرارها، تعافيها في الوقت المناسب أو في الحالات القصوى التقليص المنظم للعمليات الحيوية في حالة حدوث اضطرابات كبيرة ناجمة عن سيناريوهات طارئة مختلفة. يشمل برنامج إدارة استمرارية الأعمال الملائم تحليل التأثير على الأعمال، استراتيجيات التعافي، خطة استمرارية الأعمال والمواقع البديلة لتعافي الأعمال وتكنولوجيا المعلومات.

26. A Payment Service Provider shall put in place a set of recovery strategies to ensure that all critical business functions identified in a business impact analysis can be recovered in accordance with the predefined recovery timeframe. These recovery strategies shall be clearly documented, thoroughly tested and regularly reviewed to ensure achievement of recovery targets.

26. يجب عل مقدم خدمات الدفع وضع مجموعة من استراتيجيات التعافي لضمان أن جميع الوظائف المهمة المحددة ضمن دراسة تحليل التأثير على الأعمال قادرة على التعافي وفقاً للإطار الزمني المحدد مسبقاً. ويجب ان يتم توثيق استراتيجيات التعافي هذه بشكل واضح، وأن يتم اختبارها بدقة ومراجعتها بشكل دوري للحرص على تحقيق أهداف التعافي.

27. A Payment Service Provider shall put in place effective measures to ensure that all business

27. يجب على مقدم خدمات الدفع وضع ضوابط فعالة لضمان أن جميع السجلات الخاصة بالأعمال،

وبشكل خاص سجلات مستخدم خدمات الدفع للتجزئة، يمكن استرجاعها بشكل سريع في حال ضياعها، تلفها أو فقدانها. كما يجب على مقدم خدمات الدفع أن يجيز لمستخدمي خدمات الدفع للتجزئة بالدخول إلى سجلاتهم في وقت مناسب. يجب على مقدم خدمات الدفع إخطار مستخدمي خدمات الدفع للتجزئة عن أي فقدان في سجلاتهم بسبب فشل تشغيلي أو السرقة، وبذل الجهود المعقولة لضمان عدم استخدام السجلات الشخصية المفقودة على نحو خاطئ.

records, in particular Retail Payment Service User records, can be timely restored in case they are lost, damaged, or destroyed. A Payment Service Provider shall also allow Retail Payment Service Users to access their own records in a timely manner. A Payment Service Provider shall notify Retail Payment Service Users of any loss in their records through an operational failure or through theft, and make reasonable effort to ensure that personal records so lost are not used wrongfully.

28. يجب على مقدم خدمات الدفع تطوير خطة استمرارية الأعمال بناءً على تحليل التأثير على الأعمال واستراتيجيات التعافي المرتبطة بها. يجب أن تتضمن خطة إدارة استمرارية الأعمال، على الأقل، ما يلي:

28. A Payment Service Provider shall develop a business continuity plan based on the business impact analysis and related recovery strategies. A business continuity plan shall comprise, at a minimum:

28.1 إجراءات تعافي مفصلة لضمان الإنجاز الكامل لاستراتيجيات تعافي الخدمات؛

28.1. detailed recovery procedures to ensure full accomplishment of the service recovery strategies;

28.2 إجراءات التصعيد وبروتوكول إدارة الكوارث (مثل: إنشاء مركز قيادة، تقديم التقارير للمصرف المركزي في وقت مناسب، إلخ) في حالة توقف الخدمة الحاد أو لمدة طويلة؛

28.2. escalation procedures and crisis management protocol (e.g. set up of a command center, timely reporting to the Central Bank, etc.) in case of severe or prolonged service disruptions;

28.3 استراتيجية استباقية للاتصال (مثل تنبيه مستخدمي خدمات الدفع للتجزئة، الرد الإعلامي، إلخ.)؛

28.3. proactive communication strategies (e.g. Retail Payment Service User notification, media response, etc.);

28.4 تحديث بيانات الاتصال بالأشخاص المهمين المعنيين بخطة استمرارية الأعمال؛ و

28.4. updated contact details of key personnel involved in the business continuity plan; and

28.5 تعيين موظف رئيسي ونائب له لتولي مهام التعافي للأنظمة الهامة.

28.5. assignment of primary and alternate personnel responsible for recovery of critical systems.

29. يجب على مقدم خدمات الدفع اختبار خطة استمرارية الأعمال على الأقل مرة واحدة سنوياً. ويجب أن تشارك الإدارة والموظف الرئيسي ونائبه في

29. A Payment Service Provider shall conduct testing of its business continuity plan at least annually. Its Management, primary and alternate relevant personnel shall participate in

the annual testing to familiarize themselves with their recovery responsibilities.

الاختبار السنوي للتعرف على مسؤولياتهم فيما يخص التعافي.

30. A Payment Service Provider shall review all business continuity planning-related risks and assumptions for relevancy and appropriateness as part of the annual planning of testing. Formal testing documentation, including a test plan, scenarios, procedures and results, shall be produced. A post mortem review report shall be prepared for formal sign-off by Management

30. يجب على مقدم خدمات الدفع مراجعة جميع المخاطر والافتراضات المتعلقة بخطة استمرارية الأعمال لضمان دقتها وملاءمتها كجزء من التخطيط والاختبار السنوي. يجب إعداد تقارير اختبار رسمية تتضمن خطة الاختبار، السيناريوهات، الإجراءات والنتائج. كما يجب إعداد تقرير مراجعة عند الانتهاء ليوقع رسمياً من الإدارة.

Alternate Sites for Business and IT Recovery

مواقع احتياطية لتعافي الأعمال وتكنولوجيا المعلومات

31. A Payment Service Provider shall examine the extent to which key business functions are concentrated in the same or adjacent locations and the proximity of the alternate sites to primary sites. Alternate sites shall be sufficiently distanced to avoid any shared risk and being affected by the same disaster.

31. يجب أن يقوم مقدم خدمات الدفع بدراسة درجة تركيز وتجميع المهام الرئيسية للأعمال في المكان نفسه أو في أماكن مجاورة، والمسافة بين المواقع الاحتياطية والرئيسية. يجب ان تتواجد المواقع الاحتياطية على مسافة وبعد كافٍ لتجنب أي مخاطر مشتركة أو التأثر بنفس الكارثة.

32. A Payment Service Provider's alternate site shall be readily accessible, installed with appropriate facilities and available for occupancy within the time requirement specified in its business continuity plan. Appropriate physical access controls shall be implemented. If certain recovery staff are required to work from home in the event of a disaster, adequate computer systems and communication facilities shall be made available in advance.

32. يجب أن يكون الموقع الاحتياطي لمقدم خدمات الدفع قابل للوصول إليه بسرعة، مجهز بالمرافق اللازمة، متوفر وجاهز لمباشرة العمل بحسب المتطلب الزمني المحدد في خطة استمرارية الأعمال. كما يجب وضع ضوابط تسجيل الدخول إلى المكان. وعند وجوب عمل بعض أفراد فريق العمل من المنزل في حالة وقوع كارثة، يجب توفير بشكل مسبق أنظمة الحاسوب ومعدات الاتصال الملائمة.

33. Alternate sites for IT recovery shall have sufficient technical equipment, including communication facilities, of an appropriate standard and capacity to meet recovery requirements.

33. يجب تجهيز المواقع الاحتياطية لتعافي تكنولوجيا المعلومات بالمعدات التقنية الكافية، بما يشمل معدات الاتصال ذات معايير وقدرة تتناسب مع متطلبات التعافي.

34. A Payment Service Provider shall avoid placing excessive reliance on external vendors in providing business continuity management support, including the provision of the disaster recovery site and back-up equipment and facilities. A Payment Service Provider shall

34. يجب على مقدم خدمات الدفع تجنب الاعتماد بشكل مفرط على المزودين الخارجيين لدعم خطة استمرارية الأعمال، بما يشمل توفير الموقع الاحتياطي والمعدات والمرافق الاحتياطية. يجب على مقدم خدمات الدفع أن يتحقق بنفسه من تمتع كل

satisfy itself that each vendor has the capacity to provide the services when needed, and that the contractual responsibilities of the vendors, including the lead-time to provide necessary emergency services, types of support and capacity, are clearly specified.

مزود خارجي بالقدرة الكافية لتقديم الخدمات المطلوبة عند الحاجة، وتحديد مسؤولياتهم التعاقدية بشكل واضح، وبما يشمل المهلة الزمنية لتقديم خدمات الطوارئ الضرورية، أنواع الدعم والقدرة الاستيعابية.

35. Where a Payment Service Provider is reliant on shared computing services provided by external providers, such as cloud computing, to support its disaster recovery, it shall manage the risk associated with these services.

35. في حال اعتماد مقدم خدمات الدفع بيئة حوسبة مشتركة مقدمة من مزود خدمات خارجي، مثل الاستضافة السحابية، لدعم التعافي من الكوارث، يجب عليه إدارة المخاطرة المتعلقة بهذه الخدمة.

Reputation Risk Management

إدارة مخاطر السمعة

36. A Payment Service Provider shall establish and implement an effective process for managing reputational risk that is appropriate for the size and complexity of its operations.

36. يجب على مقدم خدمات الدفع وضع وتنفيذ إجراءات فعالة لإدارة المخاطر المتصلة بالسمعة بما يتناسب مع حجم وتعقيد عملياته.

Article (14): Obligations Towards Retail Payment Service Users

المادة (14): الالتزامات تجاه مستخدمي خدمات الدفع للتجزئة

1. Payment Service Providers must be operated prudently and with competence in a manner that will not adversely affect the interests of the Retail Payment Service Users or potential Retail Payment Service Users. In addition, they must also observe and comply with the relevant regulatory requirements and standards on consumer protection of the Central Bank. For the avoidance of doubt, in case of discrepancies between this Regulation and the Central Bank's requirements and standards on consumer protection, the respective provisions of this Regulation shall prevail.

1. يجب على مقدمي خدمات الدفع العمل بدقة وكفاءة بحيث لا تتأثر سلباً مصالح مستخدمي خدمات الدفع للتجزئة ومستخدمي خدمات الدفع للتجزئة المحتملين. كما يجب عليهم الامتثال للمتطلبات الرقابية ومعايير حماية المستهلك الصادرة عن المصرف المركزي. لتجنب الشك، في حال وجود تعارض بين أحكام هذا النظام ومتطلبات ومعايير المصرف المركزي الخاصة بحماية المستهلك، تكون الأحكام ذات الصلة من هذا النظام هي الواجبة التطبيق.

Safeguarding of Funds In-Transit

حفظ الأموال أثناء نقلها

2. At no time shall Payment Service Providers hold funds of Retail Payment Service Users unless these are funds in transit.

2. لا يجوز لمقدمي خدمات الدفع في أي وقت الاحتفاظ بأموال مستخدمي خدمات الدفع للتجزئة ما لم تكن هذه أموالاً قيد النقل.

3. Payment Service Providers that settle Payment Transactions within twenty four (24) hours shall

3. يجب على مقدمي خدمات الدفع الذين يقومون بتسوية معاملات الدفع خلال أربع وعشرين (24) ساعة

segregate Retail Payment Service Users' funds in the following ways:

فصل أموال مستخدمي خدمات الدفع للتجزئة بالطرق التالية:

3.1. funds shall not be commingled at any time with the funds of any Person other than the Retail Payment Service Users on whose behalf the funds are held; and/or

3.1 لا يجوز خلط الأموال في أي وقت بأموال أي شخص غير مستخدمي خدمات الدفع للتجزئة الذين يتم الاحتفاظ بالأموال نيابة عنهم؛ و/أو

3.2. funds shall be insulated in the interest of the Retail Payment Service Users against the claims of other creditors of the Payment Service Provider, in particular in the event of insolvency.

3.2 يجب عزل الأموال لصالح مستخدمي خدمات الدفع للتجزئة في مواجهة مطالبات الدائنين الآخرين لمقدم خدمات الدفع، ولا سيما في حالة الإفلاس.

4. Payment Service Providers that settle Payment Transactions after twenty-four (24) hours shall segregate Retail Payment Service Users' funds in the following ways:

4. يجب على مقدمي خدمات الدفع الذين يقومون بتسوية معاملات الدفع بعد أربع وعشرين (24) ساعة فصل أموال مستخدمي خدمات الدفع للتجزئة بالطرق التالية:

4.1. open a separate escrow account with a Bank and restrict any operations and transactions on this account save for the transfer of the deposited Retail Payment Service Users' funds to the end beneficiary; and/or

4.1 فتح حساب عهدة منفصل مع أحد البنوك وتقييد أي عمليات ومعاملات على هذا الحساب باستثناء تحويل أموال مستخدمي خدمات الدفع للتجزئة المودعة إلى المستفيد النهائي؛ و/أو

4.2. funds shall be covered by an insurance policy or by a bank guarantee from a regulated insurance company or Bank which does not belong to the same Group as the Payment Service Provider.

4.2 يجب تغطية وضمان الأموال بواسطة وثيقة تأمين أو ضمان بنكي من شركة تأمين مرخصة بموجب القوانين أو بنك لا ينتمي إلى نفس المجموعة التي ينتمي إليها مقدم خدمات الدفع.

4.3. While Banks, acting as Retail Payment Service Provider, are not required to establish a separate escrow account, an insurance policy or a bank guarantee to safeguard Retail Payment Service Users' funds, a separate bank account under the name of the concerned Retail Payment Service Users must be set up for protecting the funds.

4.3 بما أنه ليس مطلوب من البنوك، المقدمة لخدمات الدفع للتجزئة، فتح حساب عهدة منفصل أو ضمان أموال مستخدمي خدمات الدفع للتجزئة بواسطة وثيقة تأمين أو ضمان بنكي، فيجب عليهم بغرض حماية هذه الأموال فتح حساب مصرفي منفصل تحت اسم مستخدمي خدمات الدفع للتجزئة المعنيين.

شفافية الأحكام التعاقدية **Transparency of Contractual Terms**

5. يجب على مقدمي خدمات الدفع عرض الشروط والأحكام التي تحكم علاقتهم التعاقدية مع:

5. Payment Service Providers shall provide the terms and conditions governing their contractual relationship with:

5.1 كل مستخدم جديد لخدمات الدفع للتجزئة، بوقت كافٍ قبل التعاقد للسماح لمستخدم خدمات الدفع للتجزئة باتخاذ قرار مدروس؛

5.1. each new Retail Payment Service User, sufficiently in advance of entering into the contractual relationship as to allow the Retail Payment Service User to make an informed decision; and

5.2 وكل مستخدم حالي لخدمات الدفع للتجزئة، بناءً على طلبه، خطيًا وتسليمها له وفقًا للقناة المفضلة لديه، بما في ذلك عبر البريد الإلكتروني، تطبيق الهاتف المحمول أو أي طريقة إلكترونية أخرى.

5.2. each existing Retail Payment Service User, at their request in writing and delivered as per the Retail Payment Service User's preference, including through an e-mail, mobile application or any other electronic manner.

6. يجب كتابة الشروط والأحكام المشار إليها في البند (5) بلغة واضحة ومفهومة، وبطريقة غير مضللة ويجب تسليمها لمستخدم خدمات الدفع للتجزئة باللغتين العربية والإنجليزية، وفقاً لطلب مستخدم خدمات الدفع للتجزئة.

6. The terms and conditions referred to in paragraph (5) shall be written in a clear, plain and understandable language, in a manner that is not misleading and shall be provided to the Retail Payment Service User in both Arabic and English, as may be requested by the Retail Payment Service User.

7. يجب على مقدمي خدمات الدفع إبلاغ مستخدم خدمات الدفع للتجزئة بأي تعديلات تطرأ على الشروط والأحكام المشار إليها في البند (5) بوقت كافٍ مسبقاً وبما لا يقل عن 30 يومًا تقويمياً من تاريخ سريان هذه التعديلات.

7. Any changes to the terms and conditions referred to in paragraph (5) shall be communicated to the Retail Payment Service User by the Payment Service Provider sufficiently in advance and at least 30 calendar days prior to any such change becoming effective.

8. يجوز لمستخدم خدمات الدفع للتجزئة إنهاء علاقته التعاقدية مع مقدم خدمات الدفع بدون أي مصاريف في حال عدم موافقته على الشروط والأحكام المعدلة المشار إليها في البند (7).

8. A Retail Payment Service User shall be entitled to terminate its contractual relationship with a Payment Service Provider at no charge where it does not agree with the revised terms and conditions referred to in paragraph (7).

اتفاقية الدفع للتجزئة لمرة واحدة **Single Retail Payment Service Agreements**

9. يجب على مقدمي خدمات الدفع، فيما يخص المعاملات التي سيتم تنظيمها بموجب اتفاقية الدفع للتجزئة لمرة واحدة، تزويد مستخدمي خدمات الدفع للتجزئة بالمعلومات التالية قبل التعاقد:

9. For transactions that are to be concluded under a Single Retail Payment Service Agreement, Payment Service Providers shall provide Retail Payment Service Users with the following information before the entry into a contractual relationship:

9.1. schedule of fees, charges and commissions, including conversion rates and withdrawal charges, where applicable;	9.1 جدول الرسوم، المصاريف والعمولات، بما في ذلك سعر صرف العملات ومصاريف السحب، حيثما ينطبق؛
9.2. contact details of the Payment Service Provider, including legal name and registered address, including the address of the agent or branch, where applicable;	9.2 تفاصيل الاتصال بمقدم خدمات الدفع، بما في ذلك الاسم القانوني والعنوان المسجل، وعنوان الوكيل أو الفرع، حيثما ينطبق؛
9.3. the form and procedure for giving consent to the initiation of a Payment Order or execution of a Payment Transaction and for the withdrawal of consent;	9.3 شكل وإجراءات منح الموافقة على إنشاء أمر الدفع أو تنفيذ معاملة الدفع وسحب الموافقة؛
9.4. the communication channel between the Payment Service Provider and the Retail Payment Service User;	9.4 قناة الاتصال بين مقدم خدمات الدفع ومستخدم خدمات الدفع للتجزئة؛
9.5. the manner in safeguarding of funds as per Article 14(3) and (4) and Reserve of Assets as per Article 11(9);	9.5 طريقة حفظ الأموال وفقاً لأحكام البندين (3) و(4) من المادة 14 واحتياطي الأصول وفقاً للبند (9) من المادة 11؛
9.6. the manner and timeline for notification by the Retail Payment Service User to the Payment Service Provider in case of Unauthorized or incorrectly initiated or executed Payment Transaction;	9.6 الآلية والجدول الزمني لقيام مستخدم خدمات الدفع للتجزئة بإخطار مقدم خدمات الدفع عن تنفيذ أو إنشاء أي معاملة دفع غير مصرح بها أو بطريقة غير صحيحة؛
9.7. information on Payment Service Provider's and Retail Payment Service User's liability for Unauthorized Payment Transactions;	9.7 معلومات عن مسؤولية مقدم خدمات الدفع ومستخدم خدمات الدفع للتجزئة عن معاملات الدفع غير المصرح بها؛
9.8. the service level for the provision of the Retail Payment Service;	9.8 مستوى الخدمة لتنفيذ خدمات دفع للتجزئة؛
9.9. information on the Payment Service Provider's complaint procedure; and	9.9 معلومات عن إجراءات الشكاوى الخاصة بمقدم خدمات الدفع؛ و
9.10. the Payment Service Provider's procedure for reporting of Unauthorized Payment Transactions.	9.10 الإجراءات المعتمدة من مقدم خدمات الدفع للإبلاغ عن معاملات الدفع غير المصرح بها.

10. The information required in paragraph (9) shall be provided immediately after the execution of the Payment Transaction where it is concluded at a Payment Service User's request using a Means of Distance Communication which does not allow for the provision of such information before the entry into a contractual relationship.

10. يجب توفير المعلومات المطلوبة في البند (9) فورًا بعد تنفيذ معاملة الدفع بناءً على طلب مستخدم خدمات الدفع عند استخدامه وسيلة اتصال عن بعد لا تسمح بتوفير هذه المعلومات قبل الدخول في التعاقد.

Framework Agreements **الاتفاقيات الإطارية**

11. For transactions that are concluded under a Framework Agreement, Payment Service Providers shall provide to Retail Payment Service Users the following information before the Retail Payment Service User consents to the entry into a Payment Transaction as well as at any other time the Retail Payment Service User requests this information, and within (5) Business Days of such request:

11. يجب على مقدمي خدمات الدفع، بالنسبة للمعاملات التي يتم تنظيمها بموجب اتفاقية إطارية، تزويد مستخدمي خدمات الدفع للتجزئة بالمعلومات التالية قبل موافقة مستخدم خدمات الدفع للتجزئة على إتمام معاملة دفع وكذلك في أي وقت آخر قد يطلب فيه مستخدم خدمات الدفع للتجزئة هذه المعلومات وذلك ضمن (5) أيام عمل من هذا الطلب:

11.1. schedule of fees, charges and commissions, including conversion rates and withdrawal charges, where applicable;

11.1 جدول الرسوم والمصاريف والعمولات، بما في ذلك سعر صرف العملات ومصاريف السحب، حيثما ينطبق؛

11.2. contact details of the Payment Service Provider, including legal name and registered address, including address of the agent or branch, where applicable;

11.2 تفاصيل الاتصال بمقدم خدمات الدفع، بما في ذلك الاسم القانوني والعنوان المسجل، وعنوان الوكيل أو الفرع، حيثما ينطبق؛

11.3. the form and procedure for giving consent to the initiation of a Payment Order or execution of a Payment Transaction and for the withdrawal of consent;

11.3 شكل وإجراءات منح الموافقة على إنشاء أمر الدفع أو تنفيذ معاملة الدفع وسحب الموافقة؛

11.4. the communication channel between the Payment Service Provider and the Retail Payment Service User;

11.4 قناة الاتصال بين مقدم خدمات الدفع ومستخدم خدمات الدفع للتجزئة؛

11.5. the manner in safeguarding of funds as per Article 14(3) and (4) and Reserve of Assets as per Article 11(9);

11.5 حفظ الأموال وفقاً لأحكام البندين (3) و(4) من المادة 14 واحتياطي الأصول وفقاً للبند (9) من المادة 11؛

11.6. the manner and timeline for notification by the Retail Payment Service User to the Payment Service

11.6 الآلية والجدول الزمني لقيام مستخدم خدمات الدفع للتجزئة بإخطار مقدم خدمات

Provider in case of Unauthorized or incorrectly initiated or executed Payment Transaction;	الدفع عن تنفيذ أو إنشاء أي معاملة دفع غير مصرح بها أو بطريقة غير صحيحة؛
11.7. information on Payment Service Provider's and Retail Payment Service User's liability for Unauthorized Payment Transactions;	11.7 معلومات عن مسؤولية مقدم خدمات الدفع ومستخدم خدمات الدفع للتجزئة عن معاملات الدفع غير المصرح بها؛
11.8. information relating to terms under which a Payment Service User may be deemed to have accepted changes to the terms and conditions, the duration of the contract and the rights of the parties to terminate the Framework Agreement;	11.8 المعلومات المتعلقة بالشروط التي بموجبها يمكن اعتبار أن مستخدم خدمات الدفع قد قبل بالتعديلات التي طالت الشروط والأحكام، ومدة العقد وحقوق الأطراف من أجل إنهاء الاتفاقية الإطارية؛
11.9. the service level for the execution of the Retail Payment Service;	11.9 مستوى الخدمة لتنفيذ خدمات دفع للتجزئة؛
11.10. information on the Payment Service Provider's complaint procedure; and	11.10 معلومات عن إجراءات الشكاوى الخاصة بمقدم خدمات الدفع؛ و
11.11. the Payment Service Provider's procedure for reporting of Unauthorized Payment Transactions.	11.11 الإجراءات المعتمدة من مقدم خدمات الدفع للإبلاغ عن معاملات الدفع غير المصرح بها.
12. The information required in paragraph (11) shall be provided immediately after the execution of the Payment Transaction where it is concluded at a Payment Service User's request using a Means of Distance Communication which does not allow for the provision of such information before the entry into a contractual relationship.	12. يجب توفير المعلومات المطلوبة في البند (11) فورًا بعد تنفيذ معاملة الدفع بناءً على طلب مستخدم خدمات الدفع عند استخدامه وسيلة اتصال عن بعد لا تسمح بتوفير هذه المعلومات قبل الدخول في التعاقد.
13. Payment Service Providers shall provide Retail Payment Service Users with a written statement of the Payment Transactions under a Framework Agreement at least once per month free of charge, including details of the amounts, fees, charges and commissions, the dates and times of execution and the reference numbers for each Payment Transaction.	13. يجب على مقدمي خدمات الدفع تزويد مستخدمي خدمات الدفع للتجزئة بكشف مكتوب عن معاملات الدفع التي تتم بموجب اتفاقية إطارية على الأقل مرة واحدة شهريًا دون رسوم، بما في ذلك تفاصيل المبالغ، الرسوم، المصاريف، العمولات، تواريخ وأوقات التنفيذ والأرقام المرجعية لكل معاملة دفع.

Information Requirements **متطلبات المعلومات**

14. Immediately after the receipt of an order for a Payment Transaction, the Payment Service Provider of the Payer shall provide a receipt for Retail Payment Service Users with:

14. فور استلام أمر معاملة الدفع، يجب على مقدم خدمات الدفع المرتبط بالدافع تقديم إيصال لمستخدمي خدمات الدفع للتجزئة مع ما يلي:

14.1. confirmation of the successful or unsuccessful initiation and execution of the Payment Transaction;

14.1 تأكيد نجاح أو عدم نجاح إنشاء معاملة الدفع وتنفيذها؛

14.2. acknowledgement and reference number to track the status of the Payment Transaction, including:

14.2 إقرار ورقم مرجعي لتتبع حالة معاملة الدفع، بما في ذلك:

14.2.1. the date and amount of the Payment Transaction; and

14.2.1 تاريخ وقيمة معاملة الدفع؛ و

14.2.2. information relating to the Payee;

14.2.2 المعلومات المتعلقة بالمدفوع له؛

14.3. the amount of the Payment Transaction, any related fees or charges, including the actual currency and conversion rates used, and withdrawal charges, where applicable; and

14.3 قيمة معاملة الدفع وأي رسوم أو مصاريف ذات صلة، بما في ذلك العملة الفعلية وأسعار صرف العملات المستخدمة ومصاريف السحب، حيثما ينطبق؛ و

14.4. the date on which the Payment Service Provider received the Payment Order.

14.4 التاريخ الذي تلقى فيه مقدم خدمات الدفع أمر الدفع.

15. The Payee's Payment Service Provider shall, immediately after the execution of the Payment Transaction, provide to the Payee with a statement with the following information:

15. يجب على مقدم خدمات الدفع المرتبط بالمدفوع له، فور تنفيذ معاملة الدفع، أن يزود المدفوع له بكشف يتناول المعلومات التالية:

15.1. reference enabling the Payee to identify the Payment Transaction and, where appropriate, the Payer and any information transferred with the Payment Transaction;

15.1 مرجع يمكّن المدفوع له من تحديد معاملة الدفع، وحيثما ينطبق، الدافع وأي معلومات تم نقلها مع معاملة الدفع؛

15.2. the amount of the Payment Transaction in the currency in which the funds are to be dispersed disbursed to the Payee;

15.2 قيمة معاملة الدفع بالعملة التي سيتم بها تسليم الأموال للمدفوع له؛

15.3. the amount of any fees or charges for the Payment Transaction payable by the Payee;

15.3 قيمة أي رسوم أو مصاريف مرتبطة بمعاملة الدفع مستحقة على المدفوع له؛

15.4. where applicable, the currency exchange rate used in the Payment Transaction by the Payee's Payment Service Provider; and

15.4 حيثما ينطبق، سعر صرف العملة المستخدم في معاملة الدفع من قبل مقدم خدمات الدفع المرتبط بالمدفوع له؛ و

15.5. the date on which the amount of a Payment Transaction is credited to a Payee's Payment Account.

15.5 التاريخ الذي يتم فيه إضافة قيمة معاملة الدفع إلى حساب الدفع الخاص بالمدفوع له.

16. The Payer's Payment Service Provider shall ensure that Payment Orders are accompanied by the necessary information so that they can be processed accurately and completely, and also, be easily identified, verified, reviewed, audited and for any subsequent investigation if needed.

16. يجب على مقدم خدمات الدفع المرتبط بالدافع التأكد من أن أوامر الدفع مصحوبة بالمعلومات الضرورية لمعالجتها بدقة وبشكل كامل، وأيضًا لكي يكون من الممكن تحديدها، التحقق منها، مراجعتها، تدقيقها والقيام بأي تحقيق لاحق بشأنها بسهولة، إذا لزم الأمر.

17. The Payee's Payment Service Provider shall implement procedures to detect when any necessary information is missing or inaccurate for a Payment Transaction.

17. يجب على مقدم خدمات الدفع المرتبط بالمدفوع له تنفيذ إجراءات للكشف عن فقدان أو عدم صحة أي معلومات ضرورية لمعاملة الدفع.

Protection of Payment and Personal Data

حماية بيانات الدفع والبيانات الشخصية

18. Payment Service Providers shall have in place and maintain adequate policies and procedures to protect:

18. يجب أن يقوم مقدمو خدمات الدفع بوضع والحفاظ على سياسات وإجراءات مناسبة لحماية:

18.1. Payment Data and identify, prevent and resolve any data security breaches; and

18.1 بيانات الدفع وتحديد، منع وحل أي اختراقات لأمن البيانات؛ و

18.2. Personal Data.

18.2 البيانات الشخصية.

19. Payment Service Providers may disclose Payment and Personal Data to:

19. يجوز لمقدمي خدمات الدفع الافصاح عن بيانات الدفع والبيانات الشخصية الى:

19.1. a third party where the disclosure is made with the prior written consent of the Retail Payment Service User or is required pursuant to applicable laws;

19.1 طرف ثالث متى كان الإفصاح بموجب موافقة خطية مسبقة من مستخدم خدمات الدفع للتجزئة أو كان مفروضاً بموجب القوانين المطبقة؛

19.2. to the Central Bank;

19.2 للمصرف المركزي؛

19.3. other regulatory authorities upon request/following prior approval of the Central Bank;

19.3 للسلطات الرقابية الأخرى بناءً على طلب / تبعاً لموافقة المصرف المركزي المسبقة؛

19.4. a court of law; and

19.4 المحكمة؛ و

19.5. other government bodies who have lawfully authorized rights of access.

19.5 الهيئات والكيانات الحكومية الأخرى التي لها حق الوصول قانوناً الى هذه المعلومات.

20. In addition to the envisaged in paragraph (19), Payment Service Providers may also disclose Personal Data to its corresponding Data Subject.

20. إضافةً لما تم بيانه في البند (19)، يجوز لمقدمي خدمات الدفع أيضًا الإفصاح عن البيانات الشخصية للأشخاص موضوع البيانات.

21. Payment Service Providers shall have in place and maintain Payment and Personal Data protection controls.

21. يجب على مقدمي خدمات الدفع وضع والحفاظ على ضوابط حماية بيانات الدفع والبيانات الشخصية.

22. Personal and Payment Data shall be stored and maintained in the State. Payment Service Providers must also establish a safe and secure backup of all Personal and Payment Data in a separate location for the required period of retention of (5) years.

22. يجب تخزين البيانات الشخصية وبيانات الدفع والاحتفاظ بها في الدولة. يجب على مقدمي خدمات الدفع أيضًا إعداد نسخة احتياطية آمنة ومؤمنة لجميع البيانات الشخصية وبيانات الدفع في مكان منفصل لفترة الاحتفاظ المطلوبة والبالغة (5) سنوات.

23. Payment Service Providers shall comply with applicable regulatory requirements and standards on data protection. They shall control, process and retain only Personal Data that is necessary for the provision of Retail Payment Services and upon obtaining the explicit consent of the Retail Payment Service User.

23. يجب على مقدمي خدمات الدفع الامتثال للمتطلبات الرقابية المطبقة والمعايير المتعلقة بحماية البيانات. يجب عليهم ضبط البيانات الشخصية الضرورية فقط لتوفير خدمات الدفع للتجزئة ومعالجتها والاحتفاظ بها بعد الحصول على موافقة صريحة من مستخدم خدمات الدفع للتجزئة.

Liability for Unauthorized Payment Transactions and Refunds

المسؤولية عن معاملات الدفع غير المصرح بها والاسترداد

24. Payment Service Providers shall be fully liable for any fraudulent or Unauthorized Payment Transaction, whether before or after the Payer informs the Payment Service Provider of any potential or suspected fraud, except where there is evidence that:

24. يتحمل مقدمو خدمات الدفع المسؤولية الكاملة عن أي معاملة دفع مشبوهة أو غير مصرح بها، سواء قبل أو بعد أن يقوم الدافع بإبلاغ مقدم خدمات الدفع عن أي احتيال محتمل أو مشتبه به، إلا إذا كان هناك دليل على ما يلي:

24.1. the Payer acts fraudulently; or

24.1 إحتيال الدافع؛ أو

24.2. the Payer acted with gross negligence and did not take reasonable steps to keep its personalized security credentials safe.

24.2 تصرف الدافع بإهمال فادح وعدم اتخاذه الخطوات المعقولة للحفاظ على أمن بيانات الأمان الخاصة به.

Refunds **الاسترداد**

25. The Payment Service Provider shall refund the amount of the Unauthorized Payment Transaction to the Payer and, where applicable, restore the debited Payment Account to the state it would have been in had the Unauthorized Payment Transaction not taken place.

25. يجب على مقدم خدمات الدفع رد مبلغ معاملة الدفع غير المصرح بها إلى الدافع، وحيثما ينطبق، إعادة حساب الدفع الذي تم الخصم منه إلى الحالة التي كان عليها لو لم يتم إجراء معاملة الدفع غير المصرح بها.

26. The Payment Service Provider shall provide a refund under paragraph (25) as soon as practicable and in any event no later than the end of the Business Day following the day on which it becomes aware of the Unauthorized Payment Transaction.

26. يجب على مقدم خدمات الدفع أن يقوم برد المبالغ بموجب البند (25) في أقرب وقت ممكن عمليًا وعلى أي حال في موعد لا يتجاوز نهاية يوم العمل التالي لليوم الذي أخبر فيه بمعاملة الدفع غير المصرح بها.

27. Paragraphs (25), (26) and (30) do not apply where the Payment Service Provider has reasonable grounds to suspect fraudulent behavior by the Retail Payment Service User and notifies the Central Bank of those grounds in writing.

27. لا تسري أحكام البنود (25) و(26) و(30) عندما يكون لدى مقدم خدمات الدفع أسباب معقولة للاشتباه في إتباع مستخدم خدمات الدفع للتجزئة سلوك مشبوه وعليه إخطار المصرف المركزي بهذه الأسباب خطيا.

28. When crediting a Payment Account under paragraph (30), a Payment Service Provider shall ensure that the date on which the amount of a Payment Transaction is credited to a Payee's Payment Account is no later than the date on which the amount of the Unauthorized Payment Transaction was debited.

28. عند إضافة رصيد إلى حساب دفع بموجب الفقرة (30)، يجب على مقدم خدمات الدفع التأكد من أن التاريخ الذي يتم فيه إيداع مبلغ معاملة الدفع في حساب الدفع الخاص بالمدفوع له لا يتجاوز التاريخ الذي تم فيه خصم مبلغ معاملة الدفع غير المصرح بها.

29. Where an Unauthorized Payment Transaction was initiated through a Payment Initiation Service Provider, the Payment Service Provider providing Payment Account Issuance Services shall comply with paragraph (30). In addition, if the Payment Initiation Service Provider is liable for the Unauthorized Payment Transaction, it shall, on the request of the Payment Service Provider providing Payment Account Issuing Services, compensate the Payment Service Provider providing Payment Account Issuing Services immediately for the losses incurred or sums paid as a result of complying with paragraph (30), including the amount of the Unauthorized Payment Transaction.

29. في حالة إنشاء معاملة دفع غير مصرح بها من خلال مقدم خدمة إنشاء الدفع، يجب على مقدم خدمات الدفع الذي يوفر خدمات إصدار حساب الدفع الامتثال للبند (30). بالإضافة إلى ذلك، إذا كان مقدم خدمة إنشاء الدفع مسؤولاً عن معاملة الدفع غير المصرح بها، فيجب عليه، بناءً لطلب مقدم خدمات الدفع الذي يقدم خدمات إصدار حساب الدفع، تعويض مقدم خدمات الدفع الذي يقدم خدمات إصدار حساب الدفع فورًا عن الخسائر المتكبدة أو المبالغ المدفوعة نتيجة الامتثال للبند (30)، بما في ذلك مبلغ معاملة الدفع غير المصرح بها.

30. فيما عدا الحالات المشار إليها ضمن البنود (25) إلى (29)، عند انتهاء مقدم خدمات الدفع من التحقيق المطلوب في خطأ أو شكوى، يتعين على مقدم خدمات الدفع دفع أي مبالغ واجبة الرد أو تعويض نقدي مستحق للعميل في غضون (7) أيام تقويمية من تاريخ التوصل الى هذه النتيجة أو تلقي التعليمات بهذا الشأن. في حالة التأخر في سداد أي مبلغ واجب الرد أو أي تعويض، يجب على مقدم خدمات الدفع إطلاع العميل عن الوقت المتوقع لإيداع المبلغ المستحق، مع تبرير التأخير.

30. Other than in relation to the circumstances contemplated in paragraphs (25) to (29), on conclusion of an investigation by a Payment Service Provider into an error or Complaint, a Payment Service Provider shall pay any refund or monetary compensation due to a customer within (7) calendar days of such conclusion or instruction. In case of a delay in payment of any refund or compensation, the Payment Service Provider shall update the customer with the expected time for crediting the amount due, along with a justification for the delay.

المادة (15): استخدام الوكلاء والفروع

1. في حال اعتزام مقدم خدمات الدفع تقديم خدمات الدفع للتجزئة من خلال وكيل أو فرع، يجب عليه إجراء تقييم لهذا الترتيب وتقديم تقرير سنوي إلى المصرف المركزي بما يلي:

1.1 اسم وعنوان الوكيل أو الفرع؛

1.2 تقييم مدى ملاءمة إجراءات الرقابة الداخلية التي سيعتمدها الوكيل من أجل الامتثال لمتطلبات مواجهة غسل الأموال ومكافحة تمويل الإرهاب؛

1.3 تقييم الأشخاص المسؤولين عن إدارة الوكيل أو الفرع، وإثبات كونهم يستوفون المتطلبات الملائمة المحددة من قبل المصرف المركزي؛ و

1.4 نطاق خدمات الدفع للتجزئة التي تم تفويض الوكيل أو الفرع لتقديمها.

2. يجب على مقدمي خدمات الدفع إلزام الوكلاء تعاقدياً بالإفصاح عن تخويلهم بالتصرف نيابةً عنهم لمستخدمي خدمات الدفع للتجزئة.

Article (15): Use of Agents and Branches

1. Where a Payment Service Provider intends to provide Retail Payment Services through an Agent or branch, it must conduct an assessment of such arrangement and provide a report on an annual basis to the Central Bank of the following:

1.1. name and address of the Agent or branch;

1.2. assessment of the adequacy of the internal control mechanisms that will be used by the Agent in order to comply with AML/CTF requirements;

1.3. assessment of the Persons responsible for the Management of the Agent or branch, and evidence that they fulfil the fit and proper requirements specified by the Central Bank; and

1.4. the scope of Retail Payment Services for which the Agent or branch is mandated.

2. Payment Service Providers shall contractually ensure that Agents acting on their behalf disclose this fact to the Retail Payment Service Users.

3. يجب على مقدمي خدمات الدفع إخطار المصرف المركزي فوراً بأي تغيير يتعلق باستخدام الوكلاء أو الفروع.

3. Payment Service Providers shall immediately notify the Central Bank of any change regarding the use of Agents or branches.

المادة (16): التعهيد

1. يجب على مقدمي خدمات الدفع الذين يقومون بتعهيد الخدمات والعمليات لمقدمي خدمات، وكلاء أو شركات المجموعة ضمان التزام الأطراف الثالثة تعاقديًا بالامتثال لمتطلبات هذا النظام، أحكام المستوى الثاني والقوانين الأخرى ذات الصلة.

2. يخضع التعهيد بموجب البند (1) لموافقة المصرف المركزي المسبقة. علاوةً على ذلك، يجب على مقدمي خدمات الدفع تقديم تقرير سنوي إلى المصرف المركزي يتناول تفاصيل عن جميع ترتيبات التعهيد بموجب البند (1).

3. يبقى مقدمو خدمات الدفع مسؤولين مسؤولية كاملة عن أي أعمال يقوم بها أي وكيل، فرع أو مقدم خدمة تم تعهيده لتقديم خدمات الدفع للتجزئة.

4. يكون مقدمو خدمات الدفع مسؤولين عن ضمان والحفاظ على التدريب والمؤهلات المناسبة لوكلائهم.

Article (16): Outsourcing

1. Payment Service Providers outsourcing services and processes to service providers, Agents or Group entities shall be obliged to contractually ensure that such third parties comply with the requirements of this Regulation, Level 2 Acts and other relevant laws.

2. The outsourcing under paragraph (1) shall be subject to the prior approval of the Central Bank. Furthermore, Payment Service Providers shall provide details on all outsourcing under paragraph (1) in a report on an annual basis to the Central Bank.

3. Payment Service Providers shall remain fully liable for any acts of any Agent, branch or service provider to which a Retail Payment Service has been outsourced.

4. Payment Service Providers shall be responsible for ensuring and maintaining appropriate training and qualifications of their Agents.

المادة (17): الترتيبات التعاقدية

الوصول الى حسابات الدفع

1. يجوز لمقدمي خدمات الدفع الذين يقدمون خدمات إصدار حساب الدفع و/أو البنوك الموافقة على التعاقد مع مقدمي خدمات الدفع الذين يقدمون خدمات إنشاء الدفع وخدمات معلومات حساب الدفع لتأمين الوصول، بشكل مباشر أو غير مباشر، إلى حسابات الدفع لديهم بما يجيز لهم بتقديم خدمات إنشاء الدفع وخدمات معلومات حساب الدفع بطريقة فعالة دون عوائق.

Article (17): Contractual Arrangements

Access to Payment Accounts

1. Payment Service Providers providing Payment Account Issuance Services and/or Banks may agree to contract with Payment Service Providers providing Payment Initiation and Payment Account Information Services for the provision of access, direct or indirect, to the Payment Accounts held with them in order to allow such Payment Service Providers to provide Payment Initiation and Payment Account Information Services in an unhindered and efficient manner.

2. The contractual arrangements under paragraph (1) shall:

2. يجب أن تكون الترتيبات التعاقدية بموجب البند (1) منظمة كما يلي:

2.1. have a sound legal basis and be legally enforceable;

2.1 أن يكون لها أساس قانوني سليم وأن تكون قابلة للإنفاذ بموجب القانون؛

2.2. clearly describe the rights and obligations of the counterparties;

2.2 أن تصف بوضوح حقوق والتزامات الأطراف المتعاقدة؛

2.3. clearly define the allocation of liability between the counterparties, including in cases of fraud, unauthorized access or Data Breach, in a manner that each counterparty takes responsibility for the respective parts of the Payment Transaction under its control;

2.3 أن تحدد توزيع المسؤولية بوضوح بين الأطراف المتعاقدة، بما في ذلك في حالات الاحتيال، الوصول غير المصرح به أو خرق البيانات، بحيث يتحمل كل طرف المسؤولية عن الأجزاء ذات الصلة من معاملة الدفع التي تحت مسؤوليته؛

2.4. specify the reasons for denying access to Payment Accounts related to unauthorized or fraudulent access by Payment Service Providers providing Payment Initiation and Payment Account Information Services; and

2.4 أن تحدد أسباب رفض الوصول إلى حسابات الدفع في حالة الوصول غير المصرح به أو المشبوه من قبل مقدمي خدمات الدفع الذين يقدمون خدمات إنشاء الدفع وخدمات معلومات حساب الدفع؛ و

2.5. explicitly oblige the counterparties to comply with Article (13) on Technology Risk and Information Security.

2.5 أن تلزم الأطراف المتعاقدة صراحةً بالامتثال لأحكام المادة (13) بشأن مخاطر التكنولوجيا وأمن المعلومات.

3. The choice of Payment Service Providers providing Payment Initiation and Payment Account Information Services shall be at the sole discretion of the Payment Service Providers providing Payment Account Issuance Services and/or Banks.

3. يكون اختيار مقدمي خدمات الدفع الذين يقدمون خدمات إنشاء الدفع وخدمات معلومات حساب الدفع وفقًا للتقدير الخاص بمقدمي خدمات الدفع الذين يقدمون خدمات إصدار حساب الدفع و/أو البنوك.

4. Payment Service Providers providing Payment Initiation and Payment Account Information Services shall:

4. يجب على مقدمي خدمات الدفع الذين يقدمون خدمات إنشاء الدفع وخدمات معلومات حساب الدفع الالتزام بما يلي:

4.1. provide services only where based on the Retail Payment Service User's explicit consent;

4.1 تقديم الخدمات فقط بموجب الموافقة الصريحة لمستخدم خدمات الدفع للتجزئة؛

4.2. ensure that the personalized security credentials of the Retail Payment Service User are not, with the exception

4.2 التأكد من أن بيانات الأمان المخصصة لمستخدم خدمات الدفع للتجزئة ليست في

متناول أطراف أخرى، باستثناء مستخدم خدمات الدفع للتجزئة ومصدر بيانات الأمان المخصصة، وأنه يتم ارسالها عبر قنوات آمنة وفعالة؛

of the Retail Payment Service User and the issuer of the personalized security credentials, accessible to other parties and that they are transmitted through safe and efficient channels;

4.3 عدم طلب أو تخزين بيانات الدفع الحساسة لمستخدم خدمات الدفع للتجزئة؛

4.3. not request or store Sensitive Payment Data of the Retail Payment Service User;

4.4 عدم استخدام أي بيانات أو الوصول إليها أو تخزينها لأغراض أخرى فيما عدا توفير خدمات إنشاء الدفع وخدمات معلومات حساب الدفع، على النحو المطلوب صراحةً من قبل مستخدم خدمات الدفع للتجزئة؛ و

4.4. not use, access or store any data for purposes other than for the provision of the Payment Initiation or Payment Account Information Services, as explicitly requested by the Retail Payment Service User; and

4.5 الامتثال لمتطلبات المادة (13) بشأن مخاطر التكنولوجيا وأمن المعلومات، حيث ينشأ الدافع معاملة دفع إلكترونية أو ينفذ أي إجراء من خلال قناة عن بعد، مما قد ينطوي على مخاطر الاحتيال في الدفع أو أي تجاوزات أخرى.

4.5. comply with the requirements of Article (13) on Technology Risk and Information Security where the Payer initiates an electronic Payment Transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

5. بالإضافة إلى المتطلبات المنصوص عليها في البند (4)، يجب على مقدمي خدمات الدفع الذين يقدمون خدمات معلومات حساب الدفع الوصول فقط إلى المعلومات من حسابات الدفع المحددة ومعاملات الدفع المرتبطة بها.

5. In addition to the requirements set out in paragraph (4), Payment Service Providers providing Payment Account Information Services shall access only the information from designated Payment Accounts and associated Payment Transactions.

6. بالإضافة إلى المتطلبات المنصوص عليها في البند (4)، لا يجوز لمقدمي خدمات الدفع الذين يقدمون خدمات إنشاء الدفع تعديل المبلغ، المدفوع له أو أي خاصية أخرى لمعاملة الدفع.

6. In addition to the requirements set out in paragraph (4), Payment Service Providers providing Payment Initiation Services shall not modify the amount, the Payee or any other feature of the Payment Transaction.

Article (18): Card Schemes

المادة (18): منظومات البطاقات

Card Scheme License

ترخيص منظومة البطاقات

1. Card Schemes operating within the State shall obtain a License by the Central Bank prior to commencing operations.

1. يجب على منظومات البطاقات العاملة في الدولة الحصول على ترخيص من المصرف المركزي قبل بدء العمليات.

2. Applicants shall be subject to the procedure envisaged in the Central Bank's Licensing Guidelines.

2. يخضع مقدمو الطلبات للإجراءات المنصوص عليها في إرشادات الترخيص الصادرة عن المصرف المركزي.

3. The Central Bank shall determine whether to grant or refuse to grant a License to a Card Scheme Applicant and indicate this in writing to the Applicant within (90) calendar days from the receipt of the full set of documents and information requested under the Application.

3. يجب على المصرف المركزي تحديد ما إذا كان سيتم منح أو رفض منح ترخيص منظومة البطاقات لمقدم الطلب بإشعار خطي خلال (90) يوم تقويمي من تاريخ استلامه كافة المستندات والمعلومات المحددة ضمن الطلب.

4. The Central Bank may grant a License under paragraph (1) with or without conditions or restrictions attached to it, or refuse to grant a License at its discretion.

4. يجوز للمصرف المركزي منح الترخيص المشار إليه في البند (1) مع أو بدون شروط أو قيود ملحقة به، أو رفض منح الترخيص بحسب تقديره.

5. The Central Bank shall notify the Card Scheme of the decision taken under paragraph (3). In case of a refusal to grant a License, the Central Bank shall indicate the reasons for such refusal.

5. يخطر المصرف المركزي منظومة البطاقات بالقرار المتخذ بموجب البند (3). في حالة رفض منح الترخيص، على المصرف المركزي بيان أسباب هذا الرفض.

6. The Central Bank reserves the sole right to issue Card Issuer (Bank) Identification Numbers (BIN) in accordance with ISO/IEC 7812, as may be amended or supplemented from time to time.

6. يحتفظ المصرف المركزي حصريا بحق بإصدار أرقام تعريف مصدر البطاقات (البنك) وفقًا لمعيار آيزو/آي أي سي 7812، وفقاً لأي تعديل أو إضافة قد تطرأ عليه من وقت لآخر.

License Conditions

شروط الترخيص

7. The Central Bank shall grant a License to a Card Scheme under this Article (18) upon the fulfilment of the following conditions:

7. يمنح المصرف المركزي ترخيصًا لمنظومة البطاقات بموجب هذه المادة (18) عند استيفاء الشروط التالية:

7.1. the Central Bank has been provided with all necessary documents and information as it may request, in the form and within the timeframe specified by it, to allow it to assess the adequacy, efficiency and soundness of a Card Scheme, including:

7.1 تزويد المصرف المركزي بجميع المستندات والمعلومات اللازمة التي قد يطلبها، بالشكل وفي الإطار الزمني المحدد من قبله، بما يجيز له تقييم ملاءمة، كفاءة وسلامة منظومة البطاقات، بما في ذلك:

7.1.1. the business model and business strategy;

7.1.1 نموذج واستراتيجية العمل؛

7.1.2. the corporate governance structure;

7.1.2 هيكل الحوكمة المؤسسية؛

7.1.3. the Management contact details;

7.1.3 تفاصيل الاتصال بالإدارة؛

7.1.4. the ownership and Group structure;

7.1.4 هيكل الملكية والمجموعة؛

7.1.5. the financial and operational resources; and

7.1.5 الموارد المالية والتشغيلية؛ و

7.1.6. the description of key risks, including conduct of business and money laundering and terrorist financing risks;

7.1.6 وصف للمخاطر الرئيسية، بما في ذلك إدارة الأعمال ومخاطر غسل الأموال وتمويل الإرهاب؛

7.2. the Management of the Card Scheme fulfil the fit and proper requirements specified by the Central Bank, including that each member of Management:

7.2 يجب أن تستوفي إدارة منظومة البطاقات المتطلبات المناسبة والملائمة المحددة من المصرف المركزي، بما في ذلك أن كل عضو من أعضاء الإدارة:

7.2.1. possesses the necessary knowledge, skills, and experience;

7.2.1 يمتلك المعرفة والمهارات والخبرة اللازمة؛

7.2.2. has a record of integrity and good repute;

7.2.2 يتمتع بسجل يدل على النزاهة والسمعة الجيدة؛

7.2.3. has sufficient time to fully discharge the responsibilities under this Regulation and Level 2 Acts; and

7.2.3 لديه الوقت الكافي للاضطلاع بالتزاماته بالكامل بموجب هذا النظام وأحكام المستوى الثاني؛

7.2.4. has a record of financial soundness.

7.2.4 ويتمتع بسجل من السلامة المالية.

Reporting Requirements

متطلبات الإبلاغ ورفع التقارير

8. A Card Scheme that has been granted a License shall:

8. يجب على منظومة البطاقات التي تم منحها الترخيص التقيد بما يلي:

8.1. report to the Central Bank the information contained in Annex III on a quarterly basis;

8.1 رفع التقارير الى المصرف المركزي بشأن المعلومات الواردة في الملحق 3 على أساس ربع سنوي؛

8.2. provide additional information or become subject to more frequent reporting, as deemed necessary by the Central Bank; and

8.2 تقديم معلومات إضافية أو الخضوع لمتطلب إبلاغ ورفع تقارير أكثر تكرارًا، حسبما يراه المصرف المركزي ضروريًا؛ و

8.3. report immediately any changes that affect or are likely to affect its business model or financial viability, or which may otherwise be deemed to be material in nature such as significant increase or decrease in transaction volumes.

8.3 الإبلاغ فورًا عن أي تغييرات تؤثر أو من المحتمل أن تؤثر على نموذج أعماله أو جدواه المالية، أو التي يمكن اعتبارها ذات طبيعة جوهرية مثل الزيادة أو النقصان الملحوظ في حجم المعاملات.

Ongoing Requirements

الالتزامات المستمرة

Governance

الحوكمة

9. The Board and Management of a Card Scheme shall be responsible for ensuring that a licensed Card Scheme has an internal control framework that is adequate to establish a properly controlled operating environment for the conduct of its business, taking into account its risk profile.

9. يكون مجلس إدارة منظومة البطاقات وإدارتها مسؤولين عن التأكد من أن منظومة البطاقات المرخصة تتوفر على إطار رقابة داخلي ملائم يضمن بيئة تشغيل مراقبة بشكل صحيح لتسيير الأعمال، مع مراعاة ملف المخاطر الخاص بالمنظومة.

10. Management shall be responsible for developing an internal control framework that identifies, measures, monitors and controls all risks faced by the Card Scheme.

10. تكون الإدارة مسؤولة عن تطوير إطار رقابة داخلي يحدد، يشرف على ويراقب كافة المخاطر التي تواجهها منظومة البطاقات.

11. Licensed Card Schemes shall have organizational structures that incorporate a “three lines of defense” approach comprising the business lines, the support and control functions and an independent internal audit function.

11. يجب أن تعتمد منظومات البطاقات المرخصة هيكل تنظيمي يتضمن نهج "خطوط الدفاع الثلاثة" التي تشمل خطوط الأعمال، وظائف الدعم والرقابة ووظيفة التدقيق الداخلي المستقلة.

Compliance Function

وظائف الامتثال

12. The Board shall be responsible for ensuring that a Card Scheme has an independent, permanent and effective compliance function to monitor and report on observance of all applicable laws, regulations and standards and on adherence by

12. يكون المجلس مسؤولاً عن ضمان توفر منظومة البطاقات على وظيفة امتثال مستقلة ودائمة وفعالة لرصد ورفع التقارير حول الالتزام بجميع القوانين واللوائح والمعايير المعمول بها وعن التزام الموظفين

staff and members of the Board to legal requirements, proper codes of conduct and policy on conflicts of interest.

وأعضاء المجلس بالمتطلبات القانونية وقواعد السلوك والسياسات المناسبة بشأن تضارب المصالح.

13. The Card Payment Scheme shall have a Board-approved compliance policy that is communicated to all staff specifying the purpose, standing and authority of the compliance function within the Card Scheme.

13. يجب أن تعتمد منظومة البطاقات سياسة امتثال معتمدة من المجلس يتم إبلاغها لجميع الموظفين مع تحديد غرض، مكانة وسلطة وظيفة الامتثال ضمن منظومة البطاقات.

14. Card Schemes shall establish appropriate policies, procedures and controls pertaining to the internal reporting by their Management and staff of suspicious transactions, including the provision of the necessary records and data, to the designated Anti-Money Laundering and Combating the Financing of Terrorism compliance officer for further analysis and reporting decisions. Card Schemes shall report transactions to the competent authority when there are suspicions, or reasonable grounds to suspect, that the proceeds are related to a crime, or to the attempt or intention to use funds or proceeds for the purpose of committing, concealing or benefitting from a crime.

14. يجب على منظومات البطاقات وضع سياسات، إجراءات وضوابط مناسبة فيما يتعلق بقيام الإدارة والموظفين بالإبلاغ داخلياً عن المعاملات المشبوهة، بما في ذلك توفير السجلات والبيانات اللازمة، لموظف الامتثال المعين لمواجهة غسل الأموال ومكافحة تمويل الإرهاب لمزيد من التحليل وإعداد التقارير بهذا الشأن. يجب على منظومات البطاقات إبلاغ السلطة المختصة عن المعاملات المشبوهة أو في حالة وجود أسباب معقولة للاشتباه في أن العائدات مرتبطة بجريمة، أو بمحاولة أو نية لاستخدام الأموال أو العائدات لغرض ارتكاب، إخفاء أو الاستفادة من جريمة.

Internal Audit Function

وظيفة التدقيق الداخلي

15. The Board shall be responsible for ensuring that the Card Scheme has an independent, permanent and effective internal audit function commensurate with the size, nature of operations and complexity of its organization.

15. يكون المجلس مسؤولاً عن ضمان توفر منظومة البطاقات على وظيفة تدقيق داخلي مستقلة، دائمة وفعالة تتناسب مع حجم وطبيعة العمليات ومدى تعقيد المؤسسة.

16. The internal audit function shall provide independent assurance to the Board and Management on the quality and effectiveness of the Card Scheme's internal controls, risk management, compliance, corporate governance, and the systems and processes created by the business units, support and control functions.

16. يجب أن توفر وظيفة التدقيق الداخلي ضماناً مستقلاً للمجلس والإدارة بشأن جودة وفعالية الضوابط الداخلية، إدارة المخاطر، الامتثال، الحوكمة المؤسسية، الأنظمة والعمليات التي أنشأتها وحدات الأعمال، ووظائف الدعم والرقابة الخاصة بمنظومة البطاقات.

17. The Card Scheme shall have an internal audit charter approved by the Board audit committee that articulates the purpose, standing and

17. يجب أن يكون لمنظومة البطاقات ميثاق تدقيق داخلي معتمد من قبل لجنة التدقيق التابعة للمجلس والذي

authority of the internal audit function within the Card Scheme.

يوضح الغرض من وظيفة التدقيق الداخلي، مكانتها وسلطتها في منظومة البطاقات.

Risk Management

إدارة المخاطر

18. Card Schemes shall have an adequately resourced risk management function headed by a chief risk officer or equivalent. The function shall be independent of the management and decision-making of the Card Scheme's risk-taking functions. The risk management function shall include policies, procedures, systems and controls for monitoring and reporting risks, and to ensure that risk exposures are aligned with the entity's strategy and business plan.

18. يجب أن يكون لمنظومات البطاقات وظيفة إدارة مخاطر ذات موارد كافية برئاسة مسؤول المخاطر الرئيسي أو ما يعادله. يجب أن تكون الوظيفة مستقلة عن الإدارة وعن آلية اتخاذ القرار في الوظائف التي تحتوي على مخاطر لدى منظومة البطاقات. يجب أن تشتمل وظيفة إدارة المخاطر على سياسات، إجراءات، أنظمة وضوابط لمراقبة المخاطر والإبلاغ عنها، ولضمان تناسب حالات التعرض للمخاطر مع استراتيجية المؤسسة وخطة عملها.

Risk Strategy

استراتيجية المخاطر

19. Card Schemes shall have a clearly defined business strategy, risk appetite and defined corporate culture that has been approved by the Board and reviewed at least annually. Management shall ensure full compliance of this articulated strategy across all business lines and the Board will be ultimately responsible for such compliance.

19. يجب أن يكون لمنظومات البطاقات استراتيجية أعمال محددة بوضوح، وقدرة على قبول المخاطر، وثقافة مؤسسية محددة معتمدة من قبل المجلس ويتم مراجعتها سنوياً على الأقل. يجب أن تضمن الإدارة الامتثال الكامل لهذه الاستراتيجية المفصلة في جميع مجالات الأعمال وسيكون المجلس مسؤولاً في النهاية عن هذا الامتثال.

Information Security

أمن المعلومات

20. A Card Scheme shall apply and meet at a minimum the Payment Card Industry Data Security Standard ('PCI DSS') and UAE Information Assurance Standards, as may be amended from time to time.

20. يجب أن تطبق منظومة البطاقات وتمتثل كحد أدنى لمعايير أمن البيانات في صناعة بطاقات الدفع ومعايير ضمان أمن المعلومات في الدولة، وتعديلاتها من وقت لآخر.

21. A compliance report regarding the Card Scheme's adherence to the standards referred to in paragraph (20) shall be presented to the Board at least annually as well as transmitted to the Central Bank.

21. يجب تقديم تقرير الامتثال بشأن التزام منظومة البطاقات بالمعايير المشار إليها في البند (20) إلى المجلس سنوياً على الأقل وإرساله إلى المصرف المركزي.

22. In the case of a Data Breach, the Card Scheme shall notify the Central Bank without undue delay and not later than (72) hours after having become aware of such Data Breach.

22. في حال حدوث خرق للبيانات، يجب على منظومة البطاقات إخطار المصرف المركزي دون تأخير غير مبرر وفي موعد لا يتجاوز (72) ساعة بعد علمها بخرق البيانات.

Disaster Recovery and Business Continuity Management

التعافي من الكوارث وإدارة استمرارية الأعمال

23. Card Schemes shall have disaster recovery and business continuity plans in place to ensure their ability to operate on an ongoing basis and limit losses in the event of a severe business disruption. Such plans must be commensurate with the risk profile, nature, size and complexity of the Card Scheme's business and structure and take into account different scenarios to which the Card Scheme may be vulnerable.

23. يجب أن تعتمد منظومات البطاقات على خطط للتعافي من الكوارث واستمرارية الأعمال لضمان قدرتها على العمل بشكل مستمر والحد من الخسائر في حالة حدوث اضطراب شديد في الأعمال. يجب أن تكون هذه الخطط متناسبة مع ملف تعريف المخاطر وطبيعة وحجم وتعقيد أعمال وهيكل منظومة البطاقات وأن تأخذ في الاعتبار السيناريوهات المختلفة التي قد تكون منظومة البطاقات عرضة لها.

24. Disaster recovery and business continuity plans shall ensure that critical business functions of the Card Scheme can be maintained and recovered in a timely manner to minimize the financial, legal, regulatory, reputational and other risks that may arise from a disruption.

24. يجب أن تضمن خطط التعافي من الكوارث واستمرارية الأعمال إمكانية الحفاظ على وظائف الأعمال الحيوية لمنظومة البطاقات وتعافيها في الوقت المناسب لتقليل المخاطر المالية، القانونية والتنظيمية وتلك المتعلقة بالسمعة والمخاطر الأخرى التي قد تنشأ عن أي خلل.

25. The Board shall ensure there is a periodic independent review of the Card Scheme's disaster recovery and business continuity plans to ensure adequacy and consistency with current operations, risks and threats, recovery levels and priorities.

25. يجب على المجلس التأكد من القيام بمراجعة دورية مستقلة لخطط التعافي من الكوارث واستمرارية الأعمال في منظومة البطاقات لضمان الملاءمة والتوافق مع العمليات، المخاطر والتهديدات الحالية، مستويات التعافي والأولويات.

Risk Assessment

تقييم المخاطر

26. Card Schemes shall regularly assess risks through the identification of new risks, measurement of known risks and prioritization of risks through thorough understanding of the business and the market.

26. يجب أن تقوم منظومات البطاقات بتقييم المخاطر بانتظام من خلال تحديد المخاطر الجديدة، قياس المخاطر المعروفة وتحديد أولويات المخاطر من خلال الفهم المتكامل للأعمال والسوق.

Risk Mitigation

تخفيف المخاطر

27. Card Schemes shall mitigate risks through the implementation of:

27. يجب على منظومات البطاقات التخفيف من المخاطر من خلال تنفيذ التالي:

27.1. risk mitigation programs and technologies;

27.1 برامج وتقنيات تخفيف المخاطر؛

27.2. the effective management of risk principles; operation with risk management in mind; and

27.2 الإدارة الفعالة لمبادئ المخاطر؛ والتشغيل مع مراعاة إدارة المخاطر؛ و

27.3. outsourcing of risk functions that cannot be performed in-house.

27.3 تعهيد لوظائف المخاطر التي لا يمكن أداؤها داخلياً.

Monitoring

المراقبة

28. Card Schemes shall perform regular monitoring of all risks and mitigation programs on at least an annual basis to ensure the robustness of the risk management procedures and programs. Continuous monitoring reports, including dashboards, shall be presented to the Management and the Board to ensure that all levels of management are aware of the current risk situation, including potential fraud, in the Card Scheme.

28. يجب أن تقوم منظومات البطاقات بمراقبة دورية لجميع المخاطر وبرامج تخفيف المخاطر على أساس سنوي على الأقل لضمان قوة إجراءات وبرامج إدارة المخاطر. يجب عرض تقارير المراقبة المستمرة، بما في ذلك لوحات المعلومات، على الإدارة والمجلس للتأكد من أن جميع مستويات الإدارة على دراية بالوضع الحالي للمخاطر، بما في ذلك الاحتيال المحتمل، في منظومة البطاقات.

Assurance

الضمان

29. Card Schemes shall give assurance to all stakeholders through external and internal audits.

29. يجب أن تعطي منظومات البطاقات ضمانات لجميع الجهات المعنية من خلال التدقيق الخارجي والداخلي.

Winding Down

تصفية الأعمال

30. Where a Card Scheme intends to terminate its operation in the State, it shall obtain an approval from the Central Bank to this effect.

30. يجب على منظومة البطاقات في حال اعتزامها وقف العمل في الدولة، الحصول على موافقة المصرف المركزي في هذا الشأن.

31. A Card Scheme shall notify the Central Bank in advance of (3) months from the intended termination of its operations, and provide an orderly wind-down plan.

31. يجب على منظومة البطاقات إخطار المصرف المركزي مسبقًا قبل (3) أشهر من تاريخ الإنهاء المزمع لأعمالها، وتقديم خطة تصفية منظمة.

Supervisory Examinations

التفتيش الرقابي

32. The Central Bank may conduct periodic examinations of the operation of Card Schemes to ensure their financial soundness and compliance with the requirements of this Regulation and Level 2 Acts.

32. يجوز للمصرف المركزي إجراء تفتيش دوري لأعمال منظومات البطاقات للتأكد من سلامتها المالية وامتثالها لمتطلبات هذا النظام وأحكام المستوى الثاني.

33. Card Schemes shall provide the Central Bank with full and unrestricted access to their accounts, records and documents, and shall supply such information and facilities as may be required to conduct the examination referred to in paragraph (32).

33. يجب أن توفر منظومات البطاقات للمصرف المركزي الوصول الكامل وغير المقيد إلى حساباتها، سجلاتها ووثائقها، كما يجب أن توفر المعلومات والتسهيلات التي قد تكون مطلوبة لإجراء التفتيش المشار إليه في البند (32).

Fees and Charges

الرسوم والمصاريف

34. The Central Bank has the right to receive information on any fees and charges of Card Schemes and regulate such fees and charges as it considers appropriate.

34. للمصرف المركزي الحق في تلقي معلومات عن أية رسوم ومصاريف خاصة بمنظومات البطاقات وتنظيم هذه الرسوم والمصاريف حسبما يراه مناسباً.

35. The Central Bank may publicly disclose the fees and charges of Card Schemes referred to in paragraph (34).

35. يجوز للمصرف المركزي الإفصاح للجمهور عن رسوم ومصاريف منظومات البطاقات المشار إليها في البند (34).

Article (19): Access to the Wages Protection System

المادة (19): الوصول الى نظام حماية الأجور

Eligibility and Conditions

التأهيل والشروط

1. Payment Service Providers are eligible to apply to the Central Bank to participate in and, be given access to the Wages Protection System. They shall be given access to the Wages Protection System subject to an approval granted by the Central Bank.

1. يعتبر مقدمو خدمات الدفع مؤهلين لتقديم طلب إلى المصرف المركزي للمشاركة والوصول الى نظام حماية الأجور. ويتم منحهم حق الوصول إلى نظام حماية الأجور بشرط موافقة المصرف المركزي.

2. To allow wages to be credited to an account that can store and maintain the funds, Payment Service Providers may engage with an SVF scheme or a Bank for the provision of such account. Payment Service Providers that apply for participation in and access to the Wages Protection System shall demonstrate, among other things, that they have stringent security measures put in place so as to minimize the risks to the Wages Protection System.

2. للسماح بإيداع الأجور في حساب يمكن من خلاله تخزين الأموال والاحتفاظ بها، يجوز لمقدمي خدمات الدفع التعامل مع منظومة تسهيلات القيم المخزنة أو بنك لتوفير هذا الحساب. يجب على مقدمي خدمات الدفع الذين يتقدمون للمشاركة في نظام حماية الأجور والوصول إليه، على سبيل المثال لا الحصر، إثبات اعتمادهم إجراءات أمنية صارمة لتقليل المخاطر على نظام حماية الأجور.

3. Upon being given access to the Wages Protection System, Payment Service Providers shall be entitled to open WPS Payment Accounts.

3. يجوز لمقدمي خدمات الدفع فتح حسابات دفع في نظام حماية الأجور، لدى منحهم حق الوصول إلى نظام حماية الأجور.

4. The requirements in this Article (19) are without prejudice to other requirements of this Regulation to which Payment Service Providers are subject.

4. لا تلغي المتطلبات الواردة في هذه المادة (19) المتطلبات الأخرى لهذا النظام التي يخضع لها مقدمو خدمات الدفع.

Obligations

الالتزامات

5. Payment Service Providers that have been given access to the Wages Protection System under paragraph (1) shall:

5. يجب على مقدمي خدمات الدفع الذين نالوا حق الوصول إلى نظام حماية الأجور بموجب البند (1) القيام بما يلي:

5.1. organize marketing campaigns targeting the unbanked and underbanked segments with the objective of educating WPS Payment Account Holders on the benefits and risks associated with the services provided by the Payment Service Providers;

5.1 تنظيم حملات تسويقية تستهدف القطاعات غير القادرة على الوصول الى الخدمات البنكية أو التي تعتمد على الخدمات المالية غير البنكية بهدف توعية أصحاب حسابات الدفع في نظام حماية الأجور بشأن الفوائد والمخاطر المرتبطة بالخدمات المقدمة من مقدمي خدمات الدفع؛

5.2. conduct workshops with the objective of raising awareness of Employers on the salary information file (SIF) format to be submitted, penalties and related procedures and regulatory requirements;

5.2 عقد ورش عمل بهدف توعية أصحاب العمل حول ملف معلومات الراتب الواجب تقديمه، والعقوبات والإجراءات والمتطلبات الرقابية ذات الصلة؛

5.3. ensure that they provide WPS Payment Account Holders with a transaction statement in a timely manner;

5.3 ضمان تزويد أصحاب حسابات الدفع في نظام حماية الأجور بكشف معاملة في الوقت المناسب؛

5.4. execute the payments to WPS Payment Account Holders in a timely manner and acknowledge such execution in accordance with the WPS Rulebook;

5.4 تنفيذ الدفعات لأصحاب حسابات الدفع في نظام حماية الأجور في الوقت المناسب والإقرار بهذا التنفيذ تماشيا مع دليل قواعد نظام حماية الأجور؛

5.5. not hold WPS Payment Account Holders liable for any fraudulent or Unauthorized Payment Transactions, and shall guarantee the full amount of funds; and

5.5 عدم تحميل أصحاب حسابات الدفع في نظام حماية الأجور المسؤولية عن أي معاملات دفع مشبوهة أو غير مصرح بها، ويجب عليهم ضمان المبلغ الكامل للأموال؛ و

5.6. provide a dedicated Retail Payment Service User service and complaints team for WPS Payment Account Holders that are separate from the equivalent teams servicing other Retail

5.6 توفير فريق متخصص يتولى خدمة وشكاوى مستخدمي خدمات الدفع للتجزئة لأصحاب حسابات الدفع في نظام حماية الأجور؛ على أن يكون هذا الفريق منفصل

عن الفرق المماثلة التي تقدم خدمات الدفع للتجزئة الأخرى التي قد يتم توفيرها من قبل مقدمي خدمات الدفع.

Payment Services that may be provided by the Payment Service Providers.

6. يخضع مقدمو خدمات الدفع الذين لا يمتثلون لمتطلبات البند (5.4) للعقوبات المحددة في دليل قواعد نظام حماية الأجور.

6. Payment Service Providers that fail to comply with the requirements of paragraph (5.4) shall be subject to the penalties specified in the WPS Rulebook.

7. يجوز للمصرف المركزي أن يطلب من مقدمي خدمات الدفع الذين تم منحهم حق الوصول إلى نظام حماية الأجور بموجب البند (1) التالي:

7. The Central Bank may request from the Payment Service Providers that have been given access to the Wages Protection System under paragraph (1) to:

7.1 إعداد وتقديم تقارير ربع سنوية حول متوسط قيمة معاملات الدفع لكل صاحب حساب دفع في نظام حماية الأجور؛ و

7.1. prepare and provide quarterly reports on the average Payment Transactions value per WPS Payment Account Holder; and

7.2 إعداد وتقديم تقارير ربع سنوية عن عدد أصحاب حسابات الدفع في نظام حماية الأجور الذين تقدم لهم الخدمة.

7.2. prepare and provide quarterly reports on the number of WPS Payment Account Holders being serviced.

المادة (20): الإنفاذ والجزاءات

قد تعرض مخالفة أي من أحكام هذا النظام أو القيام بأي من المخالفات المنصوص عليها في قانون المصرف المركزي مقدم خدمات الدفع أو منظومة البطاقات للجزاءات الإدارية والمالية والعقوبات التي يراها المصرف المركزي مناسبة.

Article (20): Enforcement and sanctions

Violation of any provision of this Regulation or committing any of the violations provided for under the Central Bank Law may subject the Payment Service Provider or Card Scheme to administrative and financial sanctions and penalties as deemed appropriate by the Central Bank.

المادة (21): الفترة الانتقالية

تبدأ فترة انتقالية، مدتها سنة واحدة، من تاريخ نفاذ هذا النظام. يجوز للمصرف المركزي الأمر بوقف تقديم خدمات الدفع للتجزئة أو تشغيل منظومة البطاقات إذا لم يحصل مقدم خدمات الدفع أو منظومة البطاقات المعني على الترخيص ذات الصلة من المصرف المركزي قبل انتهاء الفترة الانتقالية. يجوز للمصرف المركزي، وفقاً لتقديره، تمديد الفترة الانتقالية لمقدم الطلب.

Article (21): Transition Period

A one-year transitional period will commence on the date this Regulation comes into force. The Central Bank may order the cessation of provision of the Retail Payment Services or the operations of the Card Scheme if the Payment Service Provider or the Card Scheme concerned has not obtained the relevant License from the Central Bank before the end of the transition period. The Central Bank may extend the transition period for the Applicant at its own discretion.

المادة (22): تفسير هذا النظام

تكون دائرة تطوير الأنظمة الرقابية في المصرف المركزي المرجع لتفسير أحكام هذا النظام.

Article (22): Interpretation of Regulation

The Regulatory Development Division of the Central Bank shall be the reference for interpretation of the provisions of this Regulation.

المادة (23): النشر والتطبيق

1. يُنشر هذا النظام في الجريدة الرسمية باللغتين العربية والانجليزية، ويُعمل به بعد شهر من تاريخ نشره. في حال وجود أي تعارض بين النصين العربي والانجليزي، يسود النص المحرر باللغة العربية.

Article (23): Publication & application

1. This Regulation shall be published in the Official Gazette in both Arabic and English and shall come into effect one month from the date of publication. In case of any discrepancy between the Arabic and the English, the Arabic version will prevail.

خالد محمد بالعمى

محافظ مصرف الإمارات العربية المتحدة المركزي

Khaled Mohamed Balama

Governor of the Central Bank of the United Arab Emirates

Annex I: Retail Payment Services

1. Payment Account Issuance Service
2. Payment Instrument Issuance Service
3. Merchant Acquiring Service
4. Payment Aggregation Service
5. Domestic Fund Transfer Service
6. Cross-border Fund Transfer Service
7. Payment Token Service
8. Payment Initiation Service
9. Payment Account Information Service

الملحق 1: خدمات الدفع للتجزئة

1. خدمة إصدار حساب الدفع
2. خدمة إصدار أداة الدفع
3. خدمة تحصيل المعاملات
4. خدمة تجميع الدفع
5. خدمة تحويل الأموال محلياً
6. خدمة تحويل الأموال عبر الحدود
7. خدمة رمز الدفع
8. خدمة إنشاء الدفع
9. خدمة معلومات حساب الدفع

Annex II: Guidance on the Best Practices for Technology Risk and Information Security

The following best practices will enable Payment Service Providers to operate adaptive and responsive cyber resilience processes. Payment Service Providers are encouraged to discuss and consider their application to improve their technology risk, information security and cyber resilience preparedness.

Technology Risk

An incident management framework with sufficient management oversight to ensure effective incident response and management capability to deal with significant incidents properly should include:

(i) timely reporting to the Central Bank of any confirmed technology-related fraud cases or major security breaches, including cyber-attacks, cases of prolonged disruption of service and systemic incidents where Retail Payment Service Users suffer from monetary loss or Retail Payment Service Users' interests are being affected (e.g. data leakage); and

الملحق 2: إرشادات حول أفضل الممارسات الخاصة بمخاطر التكنولوجيا وأمن المعلومات

تمكّن أفضل الممارسات التالي ذكرها مقدمي خدمات الدفع من التوفر على مرونة سيبرانية متكيفة وسريعة الاستجابة. يتم تشجيع مقدمي خدمات الدفع على مناقشة طلباتهم ومراجعتها لتحسين مخاطر التكنولوجيا، أمن المعلومات وجاهزية المرونة السيبرانية لديهم.

مخاطر التكنولوجيا

يجب أن يتضمن إطار إدارة الحوادث ذات الإشراف الإداري المناسب لضمان الاستجابة الفعالة للحوادث والقدرة الإدارية للتعامل مع الحوادث الكبيرة بشكل ملائم ما يلي:

(أ) إبلاغ المصرف المركزي في الوقت المناسب بأي حالات احتيال مرتبطة بالتكنولوجيا أو اختراقات أمنية كبيرة مؤكدة، بما في ذلك الهجمات السيبرانية وحالات انقطاع الخدمة لفترات طويلة والحوادث النظامية التي يعاني على اثرها مستخدمو خدمات الدفع للتجزئة من خسارة مالية أو تأثير على مصالحهم (على سبيل المثال تسرب البيانات)؛ و

(ب) استراتيجية اتصال لمعالجة أية مخاوف للجهات المعنية التي قد تنشأ عن الحوادث، وإصلاح الضرر الذي قد يلحق بالسمعة بسبب هذه الحوادث.

(ii) a communication strategy to address the concerns any stakeholders may have arising from the incidents and restore the reputational damage that the incidents may cause.

إدارة التغيير

يتم تشجيع مقدمي خدمات الدفع الذين يبلغ متوسط قيمة معاملات الدفع الشهرية الخاصة بهم (10) ملايين درهم أو أكثر على التالي:

Change Management

Payment Service Providers whose monthly average value of Payment Transactions amounts to (10) million Dirham or above are encouraged to:

(أ) تطوير إجراءات رسمية لإدارة التغيير لضمان سلامة وموثوقية البيئة التشغيلية وأن التغييرات التي تطرأ على أنظمة التطبيقات، وبرامج النظام (مثل أنظمة التشغيل والمرافق)، والأجهزة وأنظمة الشبكات وغيرها من مرافق ومعدات تكنولوجيا المعلومات مناسبة وليس لها أي تأثير غير مرغوب فيه على البيئة التشغيلية. يجب أيضاً وضع إجراءات رسمية لإدارة التغييرات الطارئة (بما في ذلك حفظ السجلات وترتيبات المصادقة) لتمكين معالجة المشاكل غير المتوقعة في الوقت المناسب وبطريقة محكمة؛ و

(i) develop a formal change management process to ensure the integrity and reliability of the production environment and that the changes to application systems, system software (e.g. operating systems and utilities), hardware, network systems and other IT facilities and equipment, are proper and do not have any undesirable impact on the production environment. Formal procedures for managing emergency changes (including the record keeping and endorsement arrangement) should also be established to enable unforeseen problems to be addressed in a timely and controlled manner; and

(ب) التوثيق المناسب والدقيق لإجراءات التحكم ومتطلبات الأمن الأساسية، بما في ذلك جميع التكوينات والإعدادات لأنظمة التشغيل وبرامج النظام وقواعد البيانات والخوادم وأجهزة الشبكة. يجب إجراء مراجعات دورية حول امتثال إعدادات الأمن لمعايير الأمان الأساسية.

(ii) adequately and accurately document control procedures and baseline security requirements, including all configurations and settings of operating systems, system software, databases, servers and network devices. They are also expected to perform periodic reviews on the compliance of the security settings with the baseline standards.

دورة حياة المشروع

يجب اعتماد وتطبيق منهجية لدورة حياة المشروع كاملة تحكم عمليات تطوير، تنفيذ وصيانة الحواسب.

Project Life Cycle

A full project life cycle methodology governing the process of developing, implementing and maintaining major computer should be established.

يجب وضع عمليات رسمية لاقتناء البرمجيات من أجل إدارة المخاطر الناشئة عن الاقتناء، مثل انتهاك اتفاقية ترخيص البرمجيات أو انتهاك براءة الاختراع، وذلك في حالة اقتناء برمجيات من مزودين خارجيين.

Where a software package is acquired from vendors, a formal software package acquisition process should be established to manage risks associated with acquisitions, such as breach of software license agreement or patent infringement.

يجب إجراء عمليات التأكد من الجودة في المشاريع الكبيرة المتعلقة بالتكنولوجيا من قبل جهة مستقلة بالاستعانة بوظائف الامتثال والشؤون القانونية.

Quality assurance reviews of major technology-related projects by an independent party, with the assistance of the legal and compliance functions should be conducted.

حوكمة تكنولوجيا المعلومات

يجب وضع مجموعة من سياسات التحكم في تكنولوجيا المعلومات التي تناسب نموذج الأعمال وتطبيقات التكنولوجيا. يجب اعتماد سياسات التحكم في تكنولوجيا المعلومات التي تحدد القواعد الأساسية لضوابط تكنولوجيا المعلومات رسمياً من قبل الإدارة وتنفيذها بشكل صحيح من قبل كل من وحدات وظائف تكنولوجيا المعلومات والأعمال. كما يجب أيضاً تحديد العمليات المستخدمة للتحقق من الامتثال مع سياسات التحكم في تكنولوجيا المعلومات وعملية الحصول على الموافقة المناسبة من قبل الإدارة للإعفاء من سياسات التحكم في تكنولوجيا المعلومات، وتنفيذ النتائج والعواقب المرتبطة بأي فشل في الالتزام بهذه العلميات.

IT Governance

A set of IT control policies that fits the business model and technology applications should be implemented. The IT control policies which establish the ground rules for IT controls should be formally approved by Management and properly implemented among IT functions and business units. Processes used to verify compliance with IT control policies and the process for seeking appropriate approval by Management for dispensation from IT control policies are also be clearly specified, and consequences associated with any failure to adhere to these processes should be effected.

المتطلبات الأمنية

يجب وضوع مبادئ توجيهية ومعايير لتطوير البرمجيات وفقاً للممارسات المقبولة عموماً بشأن التطوير الآمن. يجب إجراء مراجعة رمز البرمجة (مثل مراجعة الأقران ومراجعة التحليل الآلي)، التي يمكن أن تكون قائمة على المخاطر، كجزء من عملية ضمان جودة البرمجيات.

Security Requirements

Guidelines and standards for software development are adopted with reference to industry generally accepted practices on secure development. Source code reviews (e.g. peer review and automated analysis review), which could be risk-based, as part of a software quality assurance process should be conducted.

يجب إجراء عمليات اختبار وقبول رسمية للأنظمة للتأكد من أنه يتم الترويج فقط للأنظمة المختبرة والمعتمدة بشكل صحيح في البيئة التشغيلية. يجب أن يغطي نطاق الاختبارات قوانين عمل النظام، والضوابط الأمنية وأداء النظام في ظل سيناريوهات اختبارات الإجهاد المختلفة وظروف تعافي النظام.

Formal testing and acceptance processes should be conducted to ensure that only properly tested and approved systems are promoted to the production environment. The scope of tests covers business logic, security controls and system performance under various stress-load scenarios and recovery conditions.

يجب الحفاظ على بيئات منفصلة لأغراض التطوير، الاختبار والتشغيل الفعلي. يجب إجراء اختبار النظام واختبار قبول المستخدم بشكل صحيح في بيئة الاختبار. لا ينبغي استخدام بيانات البيئة التشغيلية في التطوير أو اختبار القبول ما لم يتم التحقق من حساسية البيانات والحصول على موافقة مسبقة من مالك المعلومات.

Segregated environments for development, testing and production purposes should be maintained. System testing and user acceptance testing (UAT) should be properly carried out in the testing environment. Production data should not be used in development or acceptance testing unless the data has been desensitized and prior approval from the information owner has been obtained.

A segregation of duties among IT teams should be introduced. Developers should not be permitted to access to production libraries and promote programming code into the production environment. If automated tools are used for the promotion of programming code, adequate monitoring, reviews and checks by independent teams should be done. Vendor accesses to the UAT environment, if necessary, should be closely monitored.

يجب اعتماد فصل الواجبات بين فرق تكنولوجيا المعلومات. يجب ألا يُسمح للمطورين الوصول إلى مكتبات ونشر شفرات البرمجيات على البيئة التشغيلية. في حالة استخدام إجراءات تلقائية لنشر الشفرات على البيئة التشغيلية، يجب إجراء المراقبة الكافية والمراجعات والفحوصات من قبل فرق مستقلة. كذلك يجب مراقبة عن كثب صلاحيات دخول المزودين الخارجيين إلى بيئة اختبار قبول المستخدم، إذا لزم الأمر.

An inventory of end-user developed applications and where necessary, control practices and responsibilities with respect to end-user computing to cover areas such as ownership, development standards, data security, documentation, data/file storage and backup, system recovery, audit responsibilities and training should be established.

يجب الاحتفاظ بقائمة جرد للبرمجيات المطورة للمستخدم النهائي، وعند الحاجة، تحديد ضوابط المراقبة والمسؤوليات فيما يتعلق بحوسبة المستخدم النهائي لتغطية مجالات مثل الملكية، معايير التطوير، أمن البيانات، التوثيق، تخزين البيانات / الملفات والنسخ الاحتياطية، واستعادة النظام، بالإضافة الى مسؤوليات التدقيق والتدريب.

A problem management process to identify, classify, prioritize and address all IT problems in a timely manner should be established. It should perform a trend analysis of past incidents regularly to facilitate the identification and prevention of similar problems.

يجب وضع إجراءات إدارة المشاكل لتحديد، تصنيف، ترتيب الأولويات ومعالجة جميع مشاكل تكنولوجيا المعلومات في الوقت المناسب. يجب إجراء تحليل اتجاهي بشكل منتظم عن الحوادث الماضية لتسهيل تحديد والوقاية من المشاكل المماثلة.

Network and Infrastructure Management

إدارة الشبكة والبنية التحتية

Network security devices such as firewalls at critical junctures of its IT infrastructure should be installed to secure the connection to untrusted external networks, such as the Internet and connections with third parties.

يتم وضع أجهزة أمن الشبكة، مثل جدران الحماية، عند نقاط الربط الحرجة لبنيتها التحتية لتكنولوجيا المعلومات، لتأمين الاتصال بالشبكات الخارجية غير الموثوق بها، مثل الإنترنت والاتصالات مع أطراف ثالثة.

Where mobile devices are provided to employees, policies and procedures covering, among others, requisition, authentication, hardening, encryption, data backup and retention should be established.

في الحالات التي يتم فيها توفير أجهزة الهاتف المحمول للموظفين، يجب وضع سياسات وإجراءات تغطي سلسلة من الأمور منها طلبات الشراء، المصادقة، التشديد، الترميز، والنسخ الاحتياطية للبيانات والاحتفاظ بها.

Adequate measures to maintain appropriate segregation of databases for different purposes to prevent unauthorized or unintended access or retrieval and robust access controls should be enforced to ensure the confidentiality and integrity of the databases. In respect of any Personal Data of Retail Payment Service Users, including Merchants, the relevant data protection laws as well as any

يجب اعتماد تدابير مناسبة للحفاظ على الفصل المناسب لقواعد البيانات الخاصة بأغراض مختلفة لمنع الدخول غير المصرح به أو غير المقصود أو الاسترجاع، كما يجب فرض ضوابط وصول قوية لضمان حفظ سرية وسلامة قواعد البيانات. أما فيما يتعلق بأي بيانات شخصية خاصة بمستخدمي خدمات الدفع للتجزئة، بما في ذلك التجار، يجب أن يتم تقييم قوانين حماية البيانات ذات

relevant codes of practice, guidelines or best practice issued by the Central Bank or any other relevant authorities should be assessed from time to time.

الصلة وكذلك أي قواعد، إرشادات أو أفضل الممارسات ذات الصلة الصادرة عن المصرف المركزي أو أي من السلطات المختصة من وقت لآخر.

Access to the information and application systems should be restricted by an adequate authentication mechanism associated with access control rules. A role-based access control framework should be adopted and access rights should be granted on a need-to-have basis.

يجب تقييد الوصول إلى المعلومات وأنظمة التطبيقات من خلال آلية مصادقة مناسبة مرتبطة بقواعد التحكم في الوصول .ويجب اعتماد إطار عمل للتحكم في صلاحيات الدخول قائم على الأدوار والمهام ومنح صلاحيات الدخول فقط على أساس الحاجة للحصول عليها.

Cyber Security Risk

The trends in cyber threats should be considered, including subscribing to quality cyber threat intelligence services, which are relevant to the provision of Retail Payment Services to enhance ability to precisely respond to new type of threats in a timely manner. The Payment Service Provider may also seek opportunities to collaborate with other organizations to share and gather cyber threat intelligence with the aim of facilitating the Retail Payment Services industry to better prepare and manage cyber security risks.

مخاطر الأمن السيبراني

يجب مواكبة تطورات وتوجهات التهديدات السيبرانية، بما في ذلك الاشتراك في خدمات معلومات التهديد السيبراني ذات الصلة بتقديم خدمات الدفع للتجزئة، وذلك لتعزيز القدرة على الاستجابة بدقة لأي نوع جديد من التهديدات في الوقت المناسب. قد يبحث مقدم خدمات الدفع عن فرص للتعاون مع جهات أخرى لمشاركة وجمع معلومات عن التهديدات السيبرانية بهدف تسهيل استعداد وجاهزية قطاع خدمات الدفع للتجزئة لمواجهة وإدارة مخاطر الأمن السيبراني بشكل أفضل.

Monitoring or surveillance systems to ensure being alerted to any suspicious or malicious system activities such as multiple sessions of same account from different geographic locations should be carried out. Real-time monitoring of cyber events for critical systems should be performed to facilitate the prompt detection of anomalous activities.

يجب وضع أنظمة مراقبة أو إشراف لضمان التنبه لأي أنشطة نظامية مشبوهة أو ضارة مثل الاستخدامات المتعددة للحساب نفسه من مواقع جغرافية مختلفة. يتم تنفيذ المراقبة فوريا دون أي تأخر للأحداث السيبرانية التي تطال الأنظمة الهامة لتسهيل الكشف الفوري عن الأنشطة غير المعتادة.

Close attention should be paid to evolving risks related to accessing critical IT infrastructure and appropriate measures are accordingly taken.

يجب الانتباه الشديد للمخاطر المتطورة المتعلقة بالوصول إلى البنية التحتية الحيوية لتكنولوجيا المعلومات واتخاذ التدابير المناسبة بشأنها.

Payment Acceptance Devices

Retail Payment Service User devices should be assumed to be exposed to security vulnerabilities and appropriate measures when designing, developing and maintaining Retail Payment Services should be taken. Security measures to guard against different compromising situations, including unauthorized device access, malware or virus attack, compromised or unsecure status of mobile device and unauthorized mobile applications should be taken.

أجهزة قبول الدفع

يجب افتراض ان أجهزة مستخدمي خدمات الدفع للتجزئة معرضة للاختراق الأمني واتخاذ التدابير اللازمة بناء على ذلك عند تصميم، تطوير أو صيانة خدمات الدفع للتجزئة. يجب مراعاة وجود ضوابط أمنية للحماية ضد سيناريوهات الاختراق المختلفة بما في ذلك الوصول غير المصرح به الى الأجهزة، البرامج الضارة أو الفيروسات، وحالات عدم وجود حماية او التعرض للمخاطر الخاصة

بأجهزة الهاتف المحمول او الاستخدام غير المصرح لتطبيقات أجهزة الهاتف المحمول.

Where Merchants use mobile devices to accept a Payment Service Provider's Retail Payment Services, additional security measures should be implemented to safeguard the mobile payment acceptance solution, including the detection of abnormal activities and logging them in reports, and the provision of Merchant identification for Retail Payment Service Users to validate identity.

في حال قيام التجار باستخدام أجهزة الهاتف المحمول لقبول عمليات الدفع للتجزئة الخاصة بمقدمي خدمات الدفع، يجب تنفيذ تدابير أمنية اضافية لحماية حلول قبول عمليات الدفع بواسطة أجهزة الهاتف المحمول، بما يشمل كشف العمليات غير المعتادة، وتسجيلها في تقارير، وتقديم معلومات وافية عن هوية التاجر لمستخدمي خدمات الدفع للتجزئة للتأكد من صحة الهوية.

Retail Payment Service User Authentication

Retail Payment Service User authentication based on a multi-factor authentication by combining any two or more of the following three factors is adopted:

(i) verification information specified by Retail Payment Service User knows (e.g. user IDs and passwords);

(ii) verification information a Retail Payment Service User has provided or possesses (e.g. one-time passwords generated by a security token or a Payment Service Provider's security systems); and

(iii) physical verification information belonging to a Retail Payment Service User (e.g. retina, fingerprint or voice recognition).

مصادقة مستخدمي خدمات الدفع للتجزئة

تطبيق آلية متعددة المعايير للمصادقة على مستخدمي خدمات الدفع للتجزئة من خلال اعتماد إثنين أو أكثر من المعايير الثلاث المحددة أدناه:

(أ) معلومات التحقق المحددة من مستخدم خدمات الدفع للتجزئة (مثل المعرفات الشخصية وكلمات المرور).

(ب) معلومات التحقق المملوكة من مستخدم خدمات الدفع للتجزئة (مثل كلمات المرور لمرة واحدة الصادرة بواسطة رمز الأمان، أو أنظمة أمان خاصة بمقدم خدمات الدفع)؛

(ج) ومعلومات تحقق مادية خاصة بمستخدم خدمات الدفع للتجزئة (مثل شبكة العين، بصمة الاصبع أو التعرف على الصوت).

If a password (including a personal identification number) is used as one factor of authentication, adequate controls related to the strength of the password (e.g. minimum password length) should be put in place.

يجب اعتماد ضوابط مناسبة فيما يتعلق بقوة كلمة المرور (كوضع حد أدنى لطول كلمة المرور) في حال استخدام كلمة المرور (بما يشمل رقم التعريف الشخصي) كرمز وحيد للدخول.

Login attempts and session management

Robust log files allowing retrieval of historical data including a full audit trail of additions, modifications or deletions of transactions are provided. Access to such tools, including privileged responsibilities, should only be available to authorized personnel and is appropriately logged.

محاولات تسجيل الدخول وإدارة الجلسات

يجب توفير سجل قوي يجيز استرجاع أي بيانات سابقة بما في ذلك جميع التفاصيل الخاصة بالإضافات، التعديلات او عمليات الحذف التي طالت المعاملات المختلفة. يجب أن يكون الوصول والاستفادة من هذه الأدوات، بما في ذلك

المسؤوليات المميزة، مسموحاً به فقط للأفراد المجاز لهم من خلال إجراءات ولوج مناسبة.

يجب منح مستخدمي خدمات الدفع للتجزئة القنوات المناسبة لمراجعة عمليات الدفع السابقة الخاصة بهم.

Retail Payment Service Users should be provided with channels to check their Past Payment Transactions.

أنظمة كشف الاحتيال

يجب تشغيل آليات مراقبة معاملات الدفع المصممة لمنع، وكشف وحظر أي معاملات دفع مشبوهة من قبل مقدمي خدمات الدفع الذين يقدمون خدمات رمز الدفع ومقدمي خدمات الدفع الذين يبلغ متوسط قيمة معاملات الدفع الشهرية الخاصة بهم عشرة (10) ملايين درهم أو ما فوق. تخضع المعاملات المشبوهة أو العالية المخاطر لعملية الفحص والتنقية والتقييم.

Fraud Detection Systems

Payment Transaction monitoring mechanisms designed to prevent, detect and block fraudulent Payment Transactions should be operated by Payment Service Providers providing Payment Token Services and Payment Service Providers whose monthly average value of Payment Transactions amounts to ten (10) million Dirhams or above. Suspicious or high-risk transactions are subject to a specific screening, filtration and evaluation procedure.

Annex III: Information to be reported by Card Schemes in English and Arabic

I. ATM data:

Field Name	Max Size	Type	Field Details
Primary Account Number (PAN)	16-19	Numeric	PAN is a series of digits used to identify a Retail Payment Service User account or relationship
Transaction Code	2	Numeric	Transaction Code - 31 (Balance Enquiry), 01 (Cash Withdrawal).
Transaction Amount	12	Numeric	Transaction amount gives the value of the funds requested by the cardholder in the local currency of the acquirer or source location of the transaction.
Transaction Currency Code	3	Alphabet (or) Numeric	Identifies the local currency of the acquirer or source location of the transaction. See ISO 4217.
Transmission Date and Time	10	Numeric	MM/DD/hh/mm/ss format The date used is the current calendar day in Greenwich Mean Time (GMT) that the transaction occurred (not Business Day)
Systems Trace Audit Number	6	Numeric	Contains a number assigned by the transaction acquirer to identify uniquely a transaction. The trace number remains unchanged for all messages throughout the life of the transaction.
Merchant's Type	4	Numeric	Contains the classification of the merchant's type (ATM/web/etc) of business product or service.
Acquiring Institution Country Code	3	Numeric	Contains the code of the country where the acquiring institution is located (see ISO 3166)
Point of Service Entry Mode	3	Numeric	Contains two numeric to indicate the method by which the primary account number was entered into the system and one numeric to indicate the PIN entry capabilities.
Acquiring Institution Identification Component	11	Numeric	Contains a code identifying the acquiring institution (e.g. merchant bank) or its agent.
Card Acceptor Name/Location	40	Alpha Numeric Special Char	Contains the name and location of the card acceptor (i.e. the merchant or ATM).
Card Acceptor Terminal Identification	15	Alpha Numeric Special Char	Contains a unique code identifying a terminal at the card acceptor location.
Authorization Identification Response	6	Alpha Numeric	Contains the response identification assigned by the authorizing institution. This field is often referred to as "auth-code".

Response Code	2	Alpha Numeric	Contains a code, which defines the disposition of a message.

II. PoS data:

Field Name	Max Size	Type	Field Details
Primary Account Number (PAN)	16-19	Numeric	PAN is a series of digits used to identify a Retail Payment Service User account or relationship
Transaction Code	2	Numeric	Transaction Code - 00 (Purchase/Sale), 20 (Refund), 31 (Balance Enquiry).
Transaction Amount	12	Numeric	Amount of funds requested by the cardholder.
Transaction Currency Code	3	Numeric	Code that indicates the local currency of the acquirer or source location of the transaction. This defines the currency that applies to the transaction amount.
Transmission Date and Time	10	Numeric	MMDDhhmmss format Generated and sent by the message initiator. It is expressed in GMT.
Systems Trace Audit Number	6	Numeric	Unique identifier assigned to the transaction by the message sender. It remains unchanged for all messages within a transaction between the two parties. This is used to provide an audit trail for every message sent by the acquirer for a given business date.
Merchant Category Code	4	Numeric	Contains the classification of the merchant's type of business product or service.
Acquiring Institution Country Code	3	Numeric	Contains the code of the country where the acquiring institution is located (see ISO 3166)
Point of Service Entry Mode	3	Numeric	Contains two numeric to indicate the method by which the primary account number was entered into the system and one numeric to indicate the PIN entry capabilities.
POS Condition Code	2	Numeric	Contains an identification of the condition under which the transaction takes place at the point of service. 00 - Normal Presentment 59 - eCommerce
Authorization Identification Response	6	Alpha Numeric	Contains the response identification assigned by the authorizing institution. This field is often referred to as "auth-code".
Card Acceptor Terminal ID	16	Alpha Numeric Special Char	Unique code identifying the terminals at the acquirer location

Card Acceptor Identification Code	15	Alpha Numeric Special Char	Unique code identifying the card acceptor
Card Acceptor Name and Location	40	Alpha Numeric Special Char	Used to hold the name and location of the card acceptor as known to the cardholder.
Response Code	2	Alpha Numeric	Contains a code, which defines the disposition of a message.

III. Fraud data:

Field Name	**Max Size**	**Type**	**Field Details**
Primary Account Number (PAN)	16-19	Numeric	PAN is a series of digits used to identify a Retail Payment Service User account or relationship
Transaction Code	2	Numeric	Transaction Code - 00 (Purchase/Sale), 20 (Refund), 31 (Balance Enquiry).
Transaction Amount	12	Numeric	Amount of funds requested by the cardholder.
Transaction Currency Code	3	Numeric	Code that indicates the local currency of the acquirer or source location of the transaction. This defines the currency that applies to the transaction amount.
Transmission Date and Time	10	Numeric	MMDDhhmmss format Generated and sent by the message initiator. It is expressed in GMT.
Systems Trace Audit Number	6	Numeric	Unique identifier assigned to the transaction by the message sender. It remains unchanged for all messages within a transaction between the two parties. This is used to provide an audit trail for every message sent by the acquirer for a given business date.
Merchant Category Code	4	Numeric	Contains the classification of the merchant's type of business product or service.
Acquiring Institution Country Code	3	Numeric	Contains the code of the country where the acquiring institution is located (see ISO 3166)
Point of Service Entry Mode	3	Numeric	Contains two numeric to indicate the method by which the primary account number was entered into the system and one numeric to indicate the PIN entry capabilities.
POS Condition Code	2	Numeric	Contains an identification of the condition under which the transaction takes place at the point of service. 00 - Normal Presentment

			59 - eCommerce
Authorization Identification Response	6	Alpha Numeric	Contains the response identification assigned by the authorizing institution. This field is often referred to as "auth-code".
Card Acceptor Terminal ID	16	Alpha Numeric Special Char	Unique code identifying the terminals at the acquirer location
Card Acceptor Identification Code	15	Alpha Numeric Special Char	Unique code identifying the card acceptor
Card Acceptor Name and Location	40	Alpha Numeric Special Char	Used to hold the name and location of the card acceptor as known to the cardholder.
Response Code	2	Alpha Numeric	Contains a code, which defines the disposition of a message.

الملحق 3: المعلومات الواجب ارسالها من قبل منظومات البطاقات باللغتين الانجليزية والعربية

أولاً – بيانات الصراف الآلي

المجال	الحجم الأقصى	النوع	تفاصيل المجال
رقم الحساب الأساسي (PAN)	19-16	رقمي	رقم الحساب الأساسي عبارة عن سلسلة من الأرقام المعتمدة لتحديد حساب أو علاقة مستخدم خدمات الدفع للتجزئة.
رمز المعاملة	2	رقمي	رمز المعاملة - 31 (الاستعلام عن الرصيد) ، 01 (السحب النقدي).
قيمة المعاملة	12	رقمي	تحدد قيمة المعاملة مبلغ الأموال التي يطلبها حامل البطاقة بالعملة المحلية للمحصل أو موقع مصدر المعاملة.
رمز عملة المعاملة	3	أبجدي (أو) رقمي	يحدد العملة المحلية للمحصل أو موقع مصدر المعاملة. راجع آيزو 4217.
تاريخ ووقت الإرسال	10	رقمي	يتبع التنسيق الشهر/اليوم/الساعة/الدقيقة/الثانية التاريخ المستخدم هو يوم التقويم الحالي بتوقيت غرينتش الذي تمت فيه المعاملة (وليس يوم العمل)

رقم التدقيق في أنظمة التتبع	6	رقمي	يحتوي على رقم محدد من قبل محصل المعاملة لتحديد معاملة بشكل خاص. يبقى رقم التتبع دون تغيير لجميع الرسائل طوال فترة سريان وتنفيذ المعاملة.
نوع التاجر	4	رقمي	يحتوي على تصنيف نوع المنتج أو الخدمة الخاصة بأعمال التاجر (جهاز صراف آلي / موقع إلكتروني / إلخ).
رمز دولة الجهة المحصلة	3	رقمي	يحتوي على رمز الدولة التي توجد فيها الجهة المحصلة (راجع آيزو 3166).
صيغة دخول نقطة الخدمة	3	رقمي	يحتوي على رقمين للإشارة إلى الطريقة التي تم بها إدخال رقم الحساب الأساسي في النظام ورقم واحد للإشارة إلى إمكانات إدخال رقم التعريف الشخصي.
عنصر تحديد الجهة المحصلة	11	رقمي	يحتوي على رمز يحدد الجهة المحصلة (مثل بنك التجار) أو وكيله.
إسم/موقع متلقي البطاقة	40	أبجدي رقمي ورموز خاصة	يحتوي على اسم وموقع متلقي البطاقة (أي التاجر أو مكينة الصراف الآلي).
تحديد محطة متلقي البطاقة	15	أبجدي رقمي ورموز خاصة	يحتوي على رمز فريد يحدد محطة في موقع متلقي البطاقة.
رد تصريح التعريف	6	أبجدي رقمي	يحتوي على الرد على تعريف الهوية المحدد من قبل الطرف المرخص. غالبًا ما يُشار إلى هذا المجال بعبارة "رمز المصادقة".
رمز الاستجابة	2	أبجدي رقمي	يحتوي على رمز يحدد محتوى الرسالة.

ثانياً – بيانات نقطة البيع

المجال	الحجم الأقصى	النوع	تفاصيل المجال
رقم الحساب الأساسي (PAN)	19-16	رقمي	رقم الحساب الأساسي عبارة عن سلسلة من الأرقام المعتمدة لتحديد حساب أو علاقة مستخدم خدمات الدفع للتجزئة.
رمز المعاملة	2	رقمي	رمز المعاملة - 00 (شراء / بيع)، 20 (استرداد)، 31 (استعلام عن الرصيد).
قيمة المعاملة	12	رقمي	قيمة الأموال التي يطلبها حامل البطاقة.
رمز عملة المعاملة	3	رقمي	رمز يحدد العملة المحلية للمحصل أو موقع مصدر المعاملة. كما يحدد العملة المعتمدة لقيمة المعاملة.
تاريخ ووقت الإرسال	10	رقمي	يتبع التنسيق الشهر/اليوم/الساعة/الدقيقة/الثانية صادر ومرسل من منشئ الرسالة. يحدد بتوقيت جرينتش.

رقم التدقيق في أنظمة التتبع	6	رقمي	يحتوي على رقم فريد للمعاملة محدد من قبل مرسل الرسالة. يبقى رقم التتبع دون تغيير لجميع الرسائل ضمن المعاملة الواحدة بين الطرفين. ويستخدم لتأمين مسار التدقيق والمتابعة لكل رسالة يرسلها المحصل في تاريخ عمل معين.
رمز نوع التاجر	4	رقمي	يحتوي على تصنيف نوع المنتج أو الخدمة الخاصة بأعمال التاجر.
رمز دولة الجهة المحصلة	3	رقمي	يحتوي على رمز الدولة التي توجد فيها الجهة المحصلة (راجع آيزو 3166).
صيغة دخول نقطة الخدمة	3	رقمي	يحتوي على رقمين للإشارة إلى الطريقة التي تم بها إدخال رقم الحساب الأساسي في النظام ورقم واحد للإشارة إلى إمكانات إدخال رقم التعريف الشخصي.
رمز حالة نقطة الدفع	2	رقمي	يحتوي على تحديد للحالة التي تتم بموجبها المعاملة في نقطة الخدمة. 00 - التقديم العادي 59 - التجارة الإلكترونية
رد تصريح التعريف	6	أبجدي رقمي	يحتوي على الرد على تعريف الهوية المحدد من قبل الطرف المرخص. غالبًا ما يُشار إلى هذا المجال بعبارة "رمز المصادقة".
معرفات محطة متلقي البطاقة	16	أبجدي رقمي ورموز خاصة	رمز فريد يحدد المحطات في موقع المحصل.
رمز تعريف متلقي البطاقة	15	أبجدي رقمي ورموز خاصة	رمز فريد يحدد متلقي البطاقة.
إسم وموقع متلقي البطاقة	40	أبجدي رقمي ورموز خاصة	يستخدم لتحديد اسم وموقع متلقي البطاقة كما هو معروف لحامل البطاقة.
رمز الاستجابة	2	أبجدي رقمي	يحتوي على رمز يحدد محتوى الرسالة.

ثالثاً – بيانات الاحتيال

المجال	الحجم الأقصى	النوع	تفاصيل المجال
رقم الحساب الأساسي (PAN)	19-16	رقمي	رقم الحساب الأساسي عبارة عن سلسلة من الأرقام المعتمدة لتحديد حساب أو علاقة مستخدم خدمات الدفع للتجزئة.
رمز المعاملة	2	رقمي	رمز المعاملة - 00 (شراء / بيع)، 20 (استرداد)، 31 (استعلام عن الرصيد).
قيمة المعاملة	12	رقمي	قيمة الأموال التي يطلبها حامل البطاقة.

رمز عملة المعاملة	3	رقمي	رمز يحدد العملة المحلية للمحصل أو موقع مصدر المعاملة. كما يحدد العملة المعتمدة لقيمة المعاملة.
تاريخ ووقت الإرسال	10	رقمي	يتبع التنسيق الشهر/اليوم/الساعة/الدقيقة/الثانية صادر ومرسل من منشئ الرسالة. يحدد بتوقيت جرينتش.
رقم التدقيق في أنظمة التتبع	6	رقمي	يحتوي على رقم فريد للمعاملة محدد من قبل مرسل الرسالة. يبقى رقم التتبع دون تغيير لجميع الرسائل ضمن المعاملة الواحدة بين الطرفين. ويستخدم لتأمين مسار التدقيق والمتابعة لكل رسالة يرسلها المحصل في تاريخ عمل معين.
رمز نوع التاجر	4	رقمي	يحتوي على تصنيف نوع المنتج أو الخدمة الخاصة بأعمال التاجر.
رمز دولة الجهة المحصلة	3	رقمي	يحتوي على رمز الدولة التي توجد فيها الجهة المحصلة (راجع آيزو 3166).
صيغة دخول نقطة الخدمة	3	رقمي	تحتوي على رقمين للإشارة إلى الطريقة التي تم بها إدخال رقم الحساب الأساسي في النظام ورقم واحد للإشارة إلى إمكانات إدخال رقم التعريف الشخصي.
رمز حالة نقطة الدفع	2	رقمي	يحتوي على تحديد للحالة التي تتم بموجبها المعاملة في نقطة الخدمة. 00 - التقديم العادي 59 - التجارة الإلكترونية
رد تصريح التعريف	6	أبجدي رقمي	يحتوي على الرد على تعريف الهوية المحدد من قبل الطرف المرخص. غالبًا ما يُشار إلى هذا المجال بعبارة "رمز المصادقة".
معرفات محطة متلقي البطاقة	16	أبجدي رقمي ورموز خاصة	رمز فريد يحدد المحطات في موقع المحصل.
رمز تعريف متلقي البطاقة	15	أبجدي رقمي ورموز خاصة	رمز فريد يحدد متلقي البطاقة.
اسم وموقع متلقي البطاقة	40	أبجدي رقمي ورموز خاصة	يستخدم لتحديد اسم وموقع متلقي البطاقة كما هو معروف لحامل البطاقة.
رمز الاستجابة	2	أبجدي رقمي	يحتوي على رمز يحدد محتوى الرسالة.