

Regulatory Framework for Opening, Operating and Closing a Business

Disclaimer: Any information rendered in this document is for general references only and should not be considered as legal advice. Users are strongly advised to seek independent legal advice if they are in doubt of their legal position.

Financial Services – Electronic Payments

No.	Regulatory Framework	Link
<i>Risk Management for Bank Payment Service Providers - External Review</i>		
1.	There are provisions in the regulatory framework that mandate external review of regulatory compliance by bank payment service providers	<ul style="list-style-type: none"> ➤ Section 12B, Cap. 584 Payment Systems and Stored Value Facilities Ordinance ➤ Section 59(2), Cap. 155 Banking Ordinance
2.	The scope of the review of bank payment service providers covers: <ul style="list-style-type: none"> • Anti-money laundering/combating of financing of terrorism audit • IT (information technology) risk management review • Data protection and privacy review • Operational and security risk management review • Financial risk management review • Regulatory reporting review (evaluate whether regulatory reporting requirements are met in a timely manner) 	<ul style="list-style-type: none"> ➤ Section 12, Cap. 584 Payment Systems and Stored Value Facilities Ordinance ➤ Section 11.3, Guideline issued pursuant to section 54, Cap. 584 Payment Systems and Stored Value Facilities Ordinance ➤ Section 59(2), Cap. 155 Banking Ordinance
<i>Risk Management for Non-Bank Payment Service Providers - External Review</i>		
3.	There are provisions in the regulatory framework that mandate external review of regulatory compliance by non-bank payment service providers	<ul style="list-style-type: none"> ➤ Sections 12 and 12B, Cap. 584 Payment Systems and Stored Value Facilities Ordinance ➤ Pages 6 and 7 of Explanatory Note on Licensing for Stored Value Facilities

No.	Regulatory Framework	Link
4.	The scope of the review of non-bank payment service providers covers IT (information technology) risk management review	<ul style="list-style-type: none"> ➤ Sections 12 and 12B, Cap. 584 Payment Systems and Stored Value Facilities Ordinance ➤ Pages 6 and 7 of Explanatory Note on Licensing for Stored Value Facilities
Internal Controls		
5.	The regulatory framework requires the implementation of internal controls to safeguard the integrity, authenticity, and confidentiality of data and operating processes of bank payment service providers	<ul style="list-style-type: none"> ➤ Paragraph 10 of the Seventh Schedule, Cap. 155 Banking Ordinance ➤ Various Supervisory Policy Manual modules (e.g., TM-E-1 on Risk Management of E-banking, TM-G-1 on General Principles for Technology Risk Management, TM-G-2 on Business Continuity Planning)
6.	The regulatory framework requires the implementation of internal controls to safeguard the integrity, authenticity, and confidentiality of data and operating processes of non-bank payment service providers	<ul style="list-style-type: none"> ➤ Section 5(1) of Part 2 of Schedule 3, Cap. 584 Payment Systems and Stored Value Facilities Ordinance

No.	Regulatory Framework	Link
Cybersecurity and Operational Risk		
7.	The regulatory framework sets cybersecurity requirements for bank payment service providers	<ul style="list-style-type: none"> ➤ Section 8, Cap. 584 Payment Systems and Stored Value Facilities Ordinance ➤ Section 7.5, Guideline issued pursuant to section 54, Cap. 584 Payment Systems and Stored Value Facilities Ordinance ➤ Paragraph 10 of the Seventh Schedule, Cap. 155 Banking Ordinance ➤ Various Supervisory Policy Manual modules (e.g., TM-E-1 on Risk Management of E-banking, TM-G-1 on General Principles for Technology Risk Management, TM-G-2 on Business Continuity Planning, TM-C-1 on Supervisory Approach on Cyber Risk Management)
8.	The regulatory framework sets cybersecurity requirements for non-bank payment service providers	<ul style="list-style-type: none"> ➤ Page 19 (section 14) of the Explanatory Note on Licensing for Stored Value Facilities
9.	The regulatory framework for e-payments requires the development of contingency plans and business continuity procedures in the event of systems and technology failures for bank payment service providers (for example, backup site or process, cyber resilience framework)	<ul style="list-style-type: none"> ➤ Paragraph 10 of the Seventh Schedule, Cap. 155 Banking Ordinance ➤ Various Supervisory Policy Manual modules (e.g., TM-E-1 on Risk Management of E-banking, TM-G-1 on General Principles for Technology Risk Management, TM-G-2 on Business Continuity Planning, TM-C-1 on Supervisory Approach on Cyber Risk Management, OR-2 on Operational Resilience)

No.	Regulatory Framework	Link
10.	The regulatory framework for e-payments requires the development of contingency plans and business continuity procedures in the event of systems and technology failures for non-bank payment service providers (for example, backup site or process, cyber resilience framework)	➤ Guideline 7.4.1 of Guideline on Supervision of Stored Value Facility Licensees issued pursuant to the Cap. 584 Payment Systems and Stored Value Facilities Ordinance
Liquidity Risk		
11.	The legal or regulatory framework requires bank payment service providers to guarantee customers' access to their funds on demand for withdrawal and payments subject to reasonable restrictions	➤ Section 2, Cap. 155 Banking Ordinance ➤ Section 2, Cap. 584 Payment Systems and Stored Value Facilities Ordinance
12.	The legal or regulatory framework requires non-bank payment service providers to guarantee customers' access to their funds on demand for withdrawal and payments subject to reasonable restrictions	➤ Section 8 of Part 2 of Schedule 3, Cap. 584 Payment Systems and Stored Value Facilities Ordinance
13.	The regulatory framework provides for customer usage limits for users of bank electronic payment services, directly or through a contractual relationship	➤ Paragraph 10 of the Seventh Schedule, Cap. 155 Banking Ordinance
14.	The regulatory framework provides for customer usage limits for users of non-bank electronic payment services, directly or through a contractual relationship	➤ Guideline 8.3.3 of Guideline on Supervision of Stored Value Facility Licensees issued pursuant to the Cap. 584 Payment Systems and Stored Value Facilities Ordinance

No.	Regulatory Framework	Link
15.	For bank payment service providers, the regulatory framework establishes the obligations of the payment service user in relation to payment instruments and personalized security credentials, directly or through contractual relationship	<ul style="list-style-type: none"> ➤ Supervisory Policy Manual CR-S-5 ➤ Paragraph 1.5 of Supervisory Policy Manual CR-S-5 ➤ Paragraph 1.4.2 of Supervisory Policy Manual TM-E-1 ➤ Paragraph 10 of the Seventh Schedule, Cap. 155 Banking Ordinance ➤ Section 35, 38.1, 49 and 50.1 of Code of Banking Practice
16.	For non-bank payment service providers, the regulatory framework establishes the obligations of the payment service user in relation to personalized security credentials, directly or through contractual relationship	<ul style="list-style-type: none"> ➤ Page 46 of Practice Note on Supervision of Stored Value Facility Licensees
17.	The bank payment service provider is required to verify the identity of a payment service user (authentication) prior to the execution of payment transactions	<ul style="list-style-type: none"> ➤ Paragraph 10 of the Seventh Schedule, Cap. 155 Banking Ordinance ➤ Supervisory Policy Manual TM-E-1 on Risk Management of E-banking
18.	The non-bank payment service provider is required to verify the identity of a payment service user (authentication) prior to the execution of payment transactions	<ul style="list-style-type: none"> ➤ Guideline 7.3.5 of Guideline on Supervision of Stored Value Facility Licensees issued pursuant to the Cap. 584 Payment Systems and Stored Value Facilities Ordinance
<i>Consumer Protection - Erroneous Transactions, and Protection of Funds</i>		
19.	The regulatory framework includes provisions that protect customer funds held with non-bank payment service providers	<ul style="list-style-type: none"> ➤ Section 7 of Part 2 of Schedule 3, Cap. 584 Payment Systems and Stored Value Facilities Ordinance ➤ Section 6 of Guideline on Supervision of Stored Value Facility Licensees issued pursuant to the Cap. 584 Payment Systems and Stored Value Facilities Ordinance

No.	Regulatory Framework	Link
20.	The regulation requires separation of funds of the customer from the funds of non-bank payment service provider	<ul style="list-style-type: none"> ➤ Section 7 of Part 2 of Schedule 3, Cap. 584 Payment Systems and Stored Value Facilities Ordinance ➤ Guideline 6.3.5 of Guideline on Supervision of Stored Value Facility Licensees issued pursuant to the Cap. 584 Payment Systems and Stored Value Facilities Ordinance
21.	The regulation prohibits the use of customer funds for purposes other than redeeming e-money and executing fund transfers	<ul style="list-style-type: none"> ➤ Guideline 6.2.1 of Guideline on Supervision of Stored Value Facility Licensees issued pursuant to the Cap. 584 Payment Systems and Stored Value Facilities Ordinance
22.	The regulation requires prudential supervision of the non-bank payment service providers	<ul style="list-style-type: none"> ➤ Section 5 of Part 2 of Schedule 3, Cap. 584 Payment Systems and Stored Value Facilities Ordinance ➤ Guideline 4.1.1 of Guideline on Supervision of Stored Value Facility Licensees issued pursuant to the Cap. 584 Payment Systems and Stored Value Facilities Ordinance
23.	The regulation explicitly protects customer funds from the potential bankruptcy/insolvency of the non-bank payment service provider	<ul style="list-style-type: none"> ➤ Guideline 6.3.1 of Guideline on Supervision of Stored Value Facility Licensees issued pursuant to the Cap. 584 Payment Systems and Stored Value Facilities Ordinance
Consumer Protection - Unauthorized Payments		
24.	The regulatory framework for bank payment service providers requires a notification about suspicious activity	<ul style="list-style-type: none"> ➤ Paragraph 10 of the Seventh Schedule, Cap. 155 Banking Ordinance ➤ Supervisory Policy Manual TM-E-1 on Risk Management of E-banking

No.	Regulatory Framework	Link
25.	The regulatory framework for non-bank payment service providers requires a notification about suspicious activity	➤ Guideline 7.3.5 of Guideline on Supervision of Stored Value Facility Licensees issued pursuant to the Cap. 584 Payment Systems and Stored Value Facilities Ordinance
26.	The regulatory framework for bank payment service providers requires a rectification of unauthorized or incorrectly executed e-payment transactions	<ul style="list-style-type: none"> ➤ Paragraph 1.5 of Supervisory Policy Manual CR-S-5 ➤ Section 37.4 of Code of Banking Practice ➤ HKMA circular “Handling Procedures for Following up Mis-transfer of Funds” ➤ HKMA circular “Enhanced Measures on Real-Time Fund Transfers Made by Customers”
27.	The regulatory framework for non-bank payment service providers requires a rectification of unauthorized or incorrectly executed e-payment transactions	➤ Guideline 8.3.8 of Guideline on Supervision of Stored Value Facility Licensees issued pursuant to the Cap. 584 Payment Systems and Stored Value Facilities Ordinance
28.	The regulatory framework includes provisions on liability for fraud related to e-payments	<ul style="list-style-type: none"> ➤ Guideline 8.3.5 of Guideline on Supervision of Stored Value Facility Licensees issued pursuant to the Cap. 584 Payment Systems and Stored Value Facilities Ordinance ➤ Supervisory Policy Manual CR-S-5
29.	The regulatory framework defines the bank payment service provider’s liability for unauthorized payment transactions	<ul style="list-style-type: none"> ➤ Paragraph 1.5 of Supervisory Policy Manual CR-S-5 ➤ Paragraph 1.4.2 of Supervisory Policy Manual TM-E-1 ➤ Sections 39, and 51 of Code of Banking Practice
30.	The regulatory framework sets a maximum amount of the consumer’s financial liability for unauthorized payment transactions, where the consumer did not act fraudulently	<ul style="list-style-type: none"> ➤ Paragraph 1.5 of Supervisory Policy Manual CR-S-5 ➤ Section 39.3 of Code of Banking Practice

No.	Regulatory Framework	Link
<i>Consumer Protection - Disclosures and Terms of Usage</i>		
31.	<p>The regulatory framework requires the following from bank payment service providers:</p> <ul style="list-style-type: none"> • The disclosure of all fees for the use of e-payment • Notifying user about changes in fees • Disclosure of liability • Disclosure of the use of customer data • Written policies for complaints handling procedure and system 	<p>➤ Section 6.1 of Code of Banking Practice</p>
<i>Environmental Sustainability of Wastewater Treatment</i>		
32.	<p>The regulatory framework requires the following from non-bank payment service providers:</p> <ul style="list-style-type: none"> • The disclosure of all fees for the use of e-payment • Notifying user about changes in fees • Disclosure of liability • Disclosure of the use of customer data • Written policies for complaints handling procedure and system • General terms of services (for example, speed of processing, resolution time for any errors, etc.) 	<p>➤ Guideline 8.3.4 of Guideline on Supervision of Stored Value Facility Licensees issued pursuant to the Cap. 584 Payment Systems and Stored Value Facilities Ordinance</p> <p>➤ Pages 58 and 59 of Practice Note on Supervision of Stored Value Facility Licensees</p>
<i>Consumer Protection - Dispute Mechanism</i>		
33.	<p>The regulatory framework requires bank payment service providers to make available a dispute resolution mechanism</p>	<p>➤ https://www.fdrc.org.hk/index.php?lang=en</p>

No.	Regulatory Framework	Link
34.	The bank payment service provider is required to acknowledge receipt of dispute notice	➤ https://www.fdc.org.hk/index.php?lang=en
35.	Bank payment service providers are required to have an independent unit or a representative in charge of dispute resolution	➤ https://www.fdc.org.hk/index.php?lang=en
36.	The regulatory framework establishes an independent governmental authority that parties can resort to in case the dispute was not resolved internally with the bank payment service provider	➤ https://www.fdc.org.hk/index.php?lang=en
<i>Interoperability and Promotion of Competition</i>		
37.	<p>The level and extent of interoperability of bank payment service providers characterized in the jurisdiction:</p> <ul style="list-style-type: none"> • A payer can make a payment to payees in all payment service providers, including non-bank payment service providers 	➤ Cap. 584 Payment Systems and Stored Value Facilities Ordinance
38.	<p>The level and extent of interoperability of non-bank payment service providers is characterized in the jurisdiction:</p> <ul style="list-style-type: none"> • A payer can make payment to payees in most payment service providers 	➤ Cap. 584 Payment Systems and Stored Value Facilities Ordinance
39.	The regulatory framework grants new payment service providers, instruments, products, business models and channels equal access to the market as to the existing participants	➤ Cap. 584 Payment Systems and Stored Value Facilities Ordinance and Explanatory Note on Licensing for Stored Value Facilities

No.	Regulatory Framework	Link
40.	The rules/procedures for registration and licensing apply for all new payment service providers, instruments, products, business models and channels, in a fair and proportionate manner and ensure a level playing field	➤ Cap. 584 Payment Systems and Stored Value Facilities Ordinance
41.	The regulatory framework set functional requirements for payment service providers	➤ Cap. 584 Payment Systems and Stored Value Facilities Ordinance ➤ Page 30 of Practice Note on Supervision of Stored Value Facility Licensees
42.	The functional requirements are applied proportionately to all payment service providers	➤ Cap. 584 Payment Systems and Stored Value Facilities Ordinance
<i>Cross-Border Electronic Payments</i>		
43.	The legal framework does not impose specific charges to incoming cross-border electronic payments, such as direct or indirect taxes, regulatory border fees, or foreign exchange fees imposed by the Central Bank or the monetary authority	➤ Article 112 of the Basic Law
44.	The legal framework does not impose any specific charges to outgoing cross-border electronic payments, such as direct or indirect taxes, regulatory border fees, or foreign exchange fees imposed by the Central Bank or the monetary authority	➤ Article 112 of the Basic Law
45.	The legal framework dose not impose limits on the value of the transactions for cross border electronic payments	➤ Article 112 of the Basic Law