International
Comparative
Legal Guides

Practical cross-border insights into anti-money laundering law

Anti-Money Laundering 2023

Sixth Edition

Contributing Editors:
Stephanie L. Brooker & M. Kendall Day
Gibson, Dunn & Crutcher LLP

sifma
ICLG.com

Industry Chapter

1 Hot Topics in AML and Financial Crimes for Broker-Dealers
Bernard Canepa, SIFMA

Expert Analysis Chapters

6 Key BSA/AML Compliance Trends in the Securities Industry
Stephanie L. Brooker & Chris Jones, Gibson, Dunn & Crutcher LLP
Bernard Canepa, SIFMA

16 A Primer on Navigating Source of Wealth Issues
Jonah Anderson & Joel M. Cohen, White & Case LLP

21 Anti-Money Laundering and Cryptocurrency: Legislative Reform and Enforcement
Kevin Roberts, Alix Prentice, Duncan Grieve & Charlotte Glaser, Cadwalader, Wickersham & Taft LLP

28 Money Laundering Risk and AML Programmes for Non-Regulated Sectors
Brian T. Markley, Brock B. Bosson & Jennifer W. Potts, Cahill Gordon & Reindel LLP

32 Evolution of Financial Services and Art: AML Practitioners – Ignore Progress at Your Peril
Stella M. Mendes & Michael Buffardi, FTI Consulting

39 The Convergence of AML Programmes for Non-Regulated Sectors, Trade-Based Money Laundering, and Data-Driven Technical Solutions
Jamal El-Hindi, David D. DiBari, Gerson Raiser & Dorothée Vermeiren, Clifford Chance

48 Compliance Issues Facing Financial Institutions When Accessing FinCEN's Beneficial Ownership Database Under the CTA
Matthew Biben, Shas Das & Jeff Telep, King & Spalding

53 Anti-Money Laundering in the Asia-Pacific Region: An Overview of the International Law Enforcement and Regulatory Frameworks
Dennis Miralis & Phillip Gibson, Nyman Gibson Miralis

67 AML and CFT Compliance in South Korea for Financial Institutions, Cryptocurrencies and NFTs
Hyun-il Hwang & Jaecheong Oh, Shin & Kim LLC

Q&A Chapters

72 Australia
King & Wood Mallesons: Kate Jackson-Maynes & Sam Farrell

81 Brazil
Joyce Roysen Advogados: Joyce Roysen & Veridiana Vianna

89 China
King & Wood Mallesons: Stanley Zhou & Yu Leimin

97 Colombia
Fabio Humar Abogados: Fabio Humar

104 France
Bonifassi Avocats: Stéphane Bonifassi & Sinem Paksut

112 Germany
Herbert Smith Freehills LLP: Dr. Dirk Seiler & Dr. Daisy Hullmeine

120 Greece
Anagnostopoulos: Ilias Anagnostopoulos & Alexandros Tsagkalidis

128 Hong Kong
K&L Gates: Sacha Cheong & Christopher Tung

136 India
Cyril Amarchand Mangaldas: Cyril Shroff, Faraz Sagar, Sara Sundaram & Pragati Sharma

150 Ireland
Matheson: Joe Beashel & Ian O'Mara

157 Isle of Man
DQ Advocates Limited: Chris Jennings & Sinead O'Connor

164 Liechtenstein
Marxer & Partner Attorneys at Law: Laura Negele-Vogt, Dr. Stefan Wenaweser, Dr. Sascha Brunner & Katharina Hasler

173 Malaysia
Skrine: Lim Koon Huan, Manshan Singh & Elizabeth Goh

183 Malta
Ganado Advocates: Mario Zerafa, Luigi Farrugia & Bettina Gatt

191 Mozambique
MDR Advogados: Mara Rupia Lopes & Duarte Santana Lopes

Q&A Chapters Continued

198 **Nigeria**
Threshing Fields Law: Frederick Festus Ntido

205 **Portugal**
Morais Leitão, Galvão Teles, Soares da Silva & Associados: Tiago Geraldo & Teresa Sousa Nunes

215 **Romania**
Enache Pirtea & Associates: Simona Pirtea & Mădălin Enache

223 **Singapore**
Drew & Napier LLC: Gary Low & Terence Tan

233 **Switzerland**
Kellerhals Carrard: Dr. Florian Baumann & Lea Ruckstuhl

243 **Taiwan**
Lee and Li, Attorneys-at-Law: Robin Chang & Eddie Hsiung

251 **United Kingdom**
White & Case LLP: Jonah Anderson

261 **USA**
Gibson, Dunn & Crutcher LLP: M. Kendall Day, Linda Noonan & Ella Alves Capone

ICLG.com

AML and CFT Compliance in South Korea for Financial Institutions, Cryptocurrencies and NFTs

Hyun-il Hwang

Jaecheong Oh

Shin & Kim LLC

Introduction

The economic development and financial growth of South Korea has been rapid and dynamic following the temporary end to the Korean War with the Korean Armistice Agreement in 1953, leading to the Miracle on the Han River and making South Korea a leading country among the global markets in trade and investment in 2022. In this time, the South Korean government introduced and continued to develop a sophisticated financial framework, and today it is the 10th largest economy in the world.

South Korea has played a critical role from economic, financial, political and social perspectives in Northeast Asia and throughout the world, creating a robust environment with a multitude of transactions occurring within and outside the country each day. Given the ongoing developments in commerce and advancements in technology – including payment systems, virtual assets, innovative approaches to transactions and methods for the transfer of funds – South Korea continues to address, investigate and prosecute individuals and companies for money laundering and terrorism financing through its monetary policies and laws/regulations.

AML/CFT Legal Framework in South Korea

Anti-money laundering ("**AML**") refers to the policies, laws and regulations in place to prevent money laundering.[1] AML regulations seek to deter financial criminals from aggressively deterring illegally obtained monies, and require financial institutions, along with other regulated entities, to monitor transactions and report suspicious financial activity. Combatting the financing of terrorism ("**CFT**") refers to a set of government laws, regulations and other tools created to restrict access to funding and financial services for terrorists.[2]

Government and regulatory authorities in South Korea[3]

The Korea Financial Intelligence Unit ("**KoFIU**") was established under the Financial Services Commission ("**FSC**") and is the primary governmental agency responsible for implementing AML/CFT compliance and enforcement in South Korea. The KoFIU works as an institutional link between financial institutions and law enforcement agencies, and receives suspicious transaction reports ("**STRs**") from reporting entities as required by law. The KoFIU can seek cooperation to investigate, review, analyse and report on findings from other law enforcement agencies for further actions to be taken, not only in South Korea but also with cooperative jurisdictions including INTERPOL. The KoFIU is also responsible for formulating, implementing and supervising AML/CFT policies, standards, rules and regulations in the country. The KoFIU may also seek cooperation with the National Police Agency, Prosecutor General and the Korea Customs Office to initiate special investigations for AML/CFT efforts.

Compliance with IMF and FATF standards

South Korea is a Member State of the International Monetary Fund ("**IMF**") and is subject to compliance assessments in accordance with the *Methodology for Assessing Compliance with the FATF 40+9 Recommendations*.[4] In the event of deficiencies, the IMF will make recommendations and offer corrective measures so that the Member State can come into compliance with the Financial Action Task Force ("**FATF**") standards.

South Korea received its first assessment from the FATF in 2008, and most recently in 2020. The last report noted that there has been a significant improvement since its prior assessment, and found that "South Korea has a sound legal framework to tackle money laundering and terrorist financing and to confiscate funds involved, but it needs to do more to stop government and public officials from laundering the proceeds of corruption".[5]

Applicable laws; financial institutions and other regulated entities

The main bodies of law for AML/CFT are (1) the *Act on Reporting and Using Specified Financial Transaction Information* ("**AML Act**"), and (2) the *Act on Prohibition against Financing of Terrorism and Proliferation of Weapons of Mass Destruction*, which is based on the *International Convention for the Suppression of the Financing of Terrorism* as promulgated by the United Nations in 1999. Other relevant laws include the *Act on the Regulation and Punishment of Criminal Proceeds Concealment*, the *Act on Special Cases Concerning the Prevention of Illegal Trafficking in Narcotics*, the *Act on Real Name Financial Transactions and Confidentiality* and the *Foreign Exchange Transactions Act* ("**FETA**"). On 21 June 2010, the KoFIU implemented the *Anti-Money Laundering and Counter-Financing Business Terrorism Regulation* concerning customer due diligence ("**CDD**") and other related preventive measures to be undertaken by financial institutions, such as know-your-customer ("**KYC**") protocols.

In accordance with the foregoing framework, financial institutions as licensed by the FSC and the Financial Supervisory Service ("**FSS**") as its "executive arm" are required to: (i) conduct CDD, including the identification and verification of customer information for financial transactions; (ii) file STRs for transactions suspected of constituting illegal assets or involving money laundering or terrorist financing; (iii) file a foreign exchange transaction report for transactions involving cash or cash equivalent

© Published and reproduced with kind permission by Global Legal Group Ltd, London

in amounts greater than or equal to USD 10,000; and (iv) establish internal controls and compliance programmes to effectively implement AML/CFT policies.

As suggested above, money laundering activities in South Korea may involve financial institutions such as banks, securities firms, asset management companies and insurers, as well as other regulated businesses, as conduits to legitimise transactions irrespective of their source and purpose. The AML Act imposes strict AML/CFT obligations not only on financial institutions, but also on the Bank of Korea as the national central bank, the Korea Post as the national postal service, casino operators, electronic financial companies and virtual asset service providers ("**VASPs**"), etc. (collectively, "**financial institutions and regulated entities**").[6] The AML Act reflects the rules and guidelines of the FATF and is in line with other laws in other countries applying in principle the same obligations, standards and procedures, while achieving uniformity with FATF recommendations.

Implementation of internal control systems for AML/CFT

The AML Act imposes obligations on all financial institutions and regulated entities to establish an internal control system for the filing of STRs, cash transaction reports for amounts greater than or equal to KRW 10 million ("**CTR**"), and KYC verification protocols. The internal control system must include, at a minimum: (i) the designation of roles and responsibilities to appropriate teams and individuals of the financial institution or regulated entity preparing STRs, CTRs and KYC protocols; (ii) an independent audit system; (iii) management supervision and evaluation protocols; (iv) the education and training of employees; (v) know-your-employee verification protocols; and (vi) AML procedures for new products and services.

The board of directors of the financial institution or regulated entity shall supervise internal control systems for AML/CFT while periodically reviewing the operation and efficacy of the same. The executive management is responsible for the design, operation and evaluation of the internal control system, as well as to implement rules and regulations for AML/CFT. The company shall have a reporting officer in charge of reporting STRs and CTRs, with daily oversight of KYC protocols while educating and training employees on AML and CFT. Lastly, a dedicated AML/CFT team shall monitor transactions to prepare STRs and other KoFIU reports, report to executive management on the internal control system, and assist in the drafting and compliance of internal rules and regulations.

STRs

A financial institution or a regulated entity must prepare and file a STR to the KoFIU upon suspicion that a financial transaction may be illegal or that there is an attempt to launder money. The reporting requirement is triggered if (i) reasonable grounds exist to suspect that assets received in connection with the transaction are sourced from illegal funds or assets, (ii) reasonable grounds exist to suspect that the transaction violates AML/CFT provisions (e.g., illegal transactions in violation of the *Act on Real Name Financial Transactions and Confidentiality*[7]), or (iii) the financial institution or regulated entity has made a report to the competent investigative agency of an alleged concealment of criminal proceeds, CFT, etc. Upon receipt of the STR, the KoFIU may follow-up with questions or request additional information from the financial institution or regulated entity to confirm whether the STR was reasonably made, and ultimately determine if further action must be taken in relation to the transaction.

A financial institution or regulated entity must establish appropriate criteria as determined by the financial institutions for its AML/CFT internal monitoring system ("**STR Rules**"). It is advised that persons responsible for making a STR apply the STR Rules strictly and as appropriately as possible to determine if an STR should be made to the KoFIU. There are precedents where sanctions were imposed for: (i) the misapplication of the STR Rules; (ii) the absence of a suspicious transaction as a result of the misapplication of industry-specific risks to the STR Rules; (iii) the overlapping or redundancy of applied AML/CFT standards; (iv) an insufficient number of persons screening suspicious transactions; (v) errors and deficiencies in computer design and virtual asset-related screening programs; (vi) the validity of the STR Rules as questionable; and (vii) modifications that were improperly applied to the STR Rules.

A STR must be made without delay,[8] and the supervisory regulations stipulate that suspicious transactions should be reported within three business days from the date the suspicious transaction is discovered. In the past, the KoFIU has instructed non-compliant companies to monitor for suspicious transactions on a daily basis, and in another instance imposed sanctions on a company for delays of up to 30–45 days before identifying suspicious transactions subject to STRs.

CTRs

Financial institutions and regulated entities must report to the KoFIU transactions in amounts greater or equal to KRW 10 million in cash, or cheques in excess of KRW 1 million,[9] per transaction made by a person during a single day,[10] subject to certain exemptions (e.g., *bona fide* transactions with governmental agencies and certain financial institutions).

A CTR, unlike a STR, has objective and uniform standards for which reports are automatically generated using information extracted from transactions that meet certain criteria. CTR obligations may apply even to transactions that are divided into two or more transactions to avoid the triggering of a CTR.

KYC verification procedures

A financial institution or regulated entity must initiate KYC verification procedures when a customer establishes a new account or seeks to complete a transaction in amount greater than or equal to KRW 1,000,000 for virtual assets and USD 10,000 for foreign exchange transactions. In this case, the company must engage in CDD to confirm the: (i) real name, address and contact information in the case of a person; (ii) corporate name, business type, location of its head office and business place, contact information, representative, date of establishment and nationality (including the purpose of establishment for a non-profit organisation) in the case of a corporation; and (iii) place of residence or office in South Korea, including the foregoing in (i) or (ii) as the case may be for foreigners and foreign corporations. Financial institutions and regulated entities must also confirm the real name, nationality, etc. of the natural persons who have ultimate control of the customer (e.g., a shareholder with 25% or more of the outstanding stock, the largest shareholder, a majority shareholder, etc.).

A financial institution or regulated entity must also conduct enhanced due diligence ("**EDD**") when there is a risk of an AML/CFT violation. For example, EDD will be triggered to confirm whether the customer is the actual owner of the monies or assets, or the validity of the source funds to the transaction must be disclosed and identified.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Consequences, fines and penalties

The AML Act imposes both criminal and administrative sanctions for violations of the AML/CFT laws and regulations. The individual may be subject to imprisonment of up to one year and/or a criminal fine of up to KRW 10 million. The individual may also be subject to an additional administrative fine of up to KRW 100 million, as well as removal from office, suspension from engaging in office duties and responsibilities for up to six months, salary reduction, reprimand, warnings and/or cautions as imposed by the KoFIU. A financial institution or regulated entity may be vicariously liable for the failure of its employee(s) to comply with the requirements and procedures under the applicable laws and regulations related to AML/CFT, also imposed by the KoFIU. In this regard, the financial institution may be subject to a criminal fine of up to KRW 10 million.

Pursuant to the *Proceeds of Crime Act*, AML/CFT proceeds shall be confiscated, including the possibility of imprisonment of up to five years or a fine not exceeding KRW 30 million for any person who disguises or conceals the acquisition or disposition of such proceeds.

VASPs

The AML Act was revised on 14 March 2020 to implement new regulations on VASPs. The AML Act defines a "virtual asset" as "an electronic certificate that has economic value and can be traded or transferred electronically". However, virtual assets are not: (i) electronic certificates that cannot be exchanged for money, goods, services, etc. or information about the certificate where the issuer has restricted the place and manner in which it is to be used; (ii) tangible and intangible items acquired through electronic games; and (iii) prepaid electronic payment methods and electronic money as defined under the *Electronic Financial Transactions Act*. A VASP refers to "a person who conducts business such as the sale, purchase, exchange, transfer, storage, management, brokerage, mediation, etc. of virtual assets in a continuous and repetitive manner while pursuing a profit", and VASPs must report to the KoFIU before conducting business.

In South Korea, there are three common VASP businesses. First, a virtual asset trader operates a platform to facilitate the sale and exchange of virtual assets. Second, a virtual asset storage and management operator stores and manages virtual assets for others as a custodian and consignment business. Third, a virtual asset wallet service provider provides storage and management services for virtual assets. However, a wallet service provider is not regulated as a VASP if it only provides software for personal storage encryption keys and does not have independent control, as well as having no involvement in the sale, purchase, exchange and transfer of virtual assets or if it manufactures or sells cold wallets offline.

Application to overseas entities

The AML Act has long-arm authority and applies to offshore financial transactions of VASPs. In other words, the AML Act will apply to a VASP transaction that originates in a foreign country and is subject to the laws of South Korea. Accordingly, even for virtual asset exchanges that are operated outside of South Korea, the VASP must report the transaction to the KoFIU if it (i) provides services in South Korea, (ii) provides payment services in KRW, or (iii) conducts sales or marketing activities for South Korean nationals or residents.

VASP reporting requirements

A VASP must report its trade name, representative's name, location of business and contact information to the KoFIU. The validity period of the report is three years, and after the expiration of the validity period, if the VASP intends to continue engaging in the same activity, it must provide an updated report to the KoFIU. In addition, a VASP must secure (i) an information security management system, also known as "**ISMS**", certification from the Korea Internet & Security Agency ("**KISA**"), and (ii) confirmation of the real name of the owner of the deposit and withdrawal account[11] from a local bank in South Korea. In the event that the services provided by a VASP do not include an exchange between fiat currency and virtual assets, the real name verification requirement above does not apply. In other words, VASPs that do not provide deposits and withdrawals in fiat currency or brokerage and mediation services of virtual assets through fiat currency, instead only providing brokerage and mediation services for the buying and selling of virtual assets in exchange for other virtual assets, do not need to receive a real name verified deposit and withdrawal account from a bank. Although it is not impossible for foreign VASPs to report to the KoFIU as a VASP, they must have a separate place of business in South Korea to do so.

All obligations under the AML Act, such as KYC and STR obligations imposed on financial institutions and regulated entities, apply similarly to VASPs. Accordingly, VASPs must make STRs and CTRs, verify customers, establish internal systems, preserve data, etc. Additionally, VASPs must separate and manage transaction details for each customer for STR and CTR purposes. VASPs transferring virtual assets must also provide the transfer-related information to the recipient, otherwise known as the "Travel Rule". Accordingly, when transferring virtual assets for a customer, a VASP must provide the remitting party's name and his/her virtual asset address and the receiving party's name and his/her virtual asset address to the receiving VASP.

Issues and Trends

Accusation Offshore VASPs of unreported VASP business activities in Korea

Foreign VASPs must report to the Commissioner of the KoFIU and fulfil their reporting obligations under the Korean AML Law if they conduct business related to virtual asset services for Korean residents. KoFIU determines whether a foreign VASP provides virtual asset services for Korean residents by considering the following: (i) whether the VASP provides services in Korean language; (ii) whether the VASP conducts marketing and promotional activities targeting Korean residents; and (iii) whether the VASP supports a Korean currency payment or transaction system.

In 2021, Financial Service Commission ("**FSC**") sent an official notice to 27 foreign VASPs which FSC deemed to operate their business to Korean residents. in August 2022, the KoFIU found 16 unreported foreign VASPs and requested Korea Communications Commission to block their IP addresses. KoFIU also demanded Korean VASPs to cease transmission of any virtual assets to the unreported foreign VASPs.

Cross-border transactions

The FETA imposes a duty to report the import and export of payment sources or securities of USD 10,000 or more, and

© Published and reproduced with kind permission by Global Legal Group Ltd, London

stipulates that persons who engage in the business of foreign exchange shall be registered and maintain certain facilities and manpower as overseen by the Ministry of Economy and Finance in South Korea. In this regard, a question arises as to overseas remittances of virtual assets and whether such activities involve a transaction obligating a business to report as a foreign exchange business under the FETA. A South Korean court reviewed a case involving a standard overseas remittance of virtual assets brokered by a company. The precise question presented was whether the persons brokering the transaction must be registered as a foreign exchange business. In its ruling, the court held that that "there is room for interpretation that [the company] does not fall within the definition of a foreign exchange business as claimed by the defendant company", where it alleged that it merely sent Bitcoin[s] from a local exchange, trading the cryptocurrency to an overseas company. The Korean court appeared to take the position that Bitcoin does not, in itself, correspond to a source and method of payment given the application of "Kimchi Premium" and arbitrage that is engaged in by Bitcoin traders.

On the other hand, and as discussed above, virtual assets used in cross-border transactions are essentially virtual assets, such as Bitcoin, under the current South Korean legal framework, recent court decisions, and the position and policies of the regulatory authorities. Moreover, the rationale for such position is based on the premise that electronic money or prepaid electronic payment sources and methods are not virtual assets according to the *Financial Investment Services and Capital Markets Act* and the *Electronic Financial Transactions Act*, and are not considered as securities, bonds and (external) payment methods under the FETA. At present, the question as to whether the same rationale applies to virtual assets remains unclear.

Non-fungible tokens

Non-fungible tokens ("**NFTs**") have appeared in South Korea as they have in many other countries, attracting interest as an innovative funding model utilising digital certificates for security and authentication of almost anything that can be reduced to a digital medium. NFTs are commonly associated with art, music, literary works, video games and other collectibles.

It is unclear as to whether NFTs are viewed as virtual assets subject to regulation under the *Specific Financial Information Act*. The FSC issued an official position on 23 November 2021, announcing that "general NFTs are not virtual assets, but when used as a form of payment or investment, they may correspond to virtual assets". The FSC has taken the position that NFTs are more characteristic of virtual assets, as the reality is that NFTs are most commonly used as payment sources rather than as collectible assets. Based on the foregoing interpretation of NFTs, the FSC announced in November 2021 that it does not intend to regulate NFTs in the country in accordance with the definition of "virtual assets" as promulgated by the FATF. Moreover, the FATF view NFTs as digital assets that are unique and not interchangeable, and as collectibles, not financial instruments.

However, starting from 2025, NFTs will be taxable in Korea. There will be a 20% tax on income from virtual assets that exceed KRW 2.5 million (USD 2,100), as of the start of 2025.

Proactive measures by the South Korean government

South Korean authorities have stepped up their monitoring activities over cryptocurrencies, especially in light of daily transactions involving greater amounts of cryptocurrencies in relation to retail stock investments. In doing so, the Office of Government Policy Coordination has taken a multipronged approach to address illegal activities and strengthen AML/CFT in the country with the support and oversight of the FSC and the FSS as its "executive arm", the Financial Intelligence Unit and the National Police Agency. On a related note, beginning in 2021, the National Tax Service began an aggressive crackdown on tax evaders in relation to cryptocurrency and NFTs as a result of source income derived therefrom by individuals.

Endnotes

1. https://www.investopedia.com/terms/a/aml.asp.
2. https://www.investopedia.com/terms/c/combating-financing-terrorism-cft.asp.
3. https://www.kofiu.go.kr/eng/regime/framework.do.
4. https://www.imf.org/external/np/leg/amlcft/eng/aml2.htm.
5. Documents – FATF (https://www.fatf-gafi.org).
6. See Article 2 of the AML Act.
7. In Korea, the *Act on Real Name Financial Transactions and Confidentiality* was enacted to enforce using real names in financial transactions, and financial companies, etc. are required to verify the real names of parties of financial transactions.
8. See Article 4 of the AML Act.
9. Provided, however, remittances of KRW 1 million or less, purchase/sale of foreign currency of KRW 1 million or less, and receipts such as utility bills are excluded.
10. Provided, however, in the case of casino operated, per case.
11. This refers to a service that allows deposits and withdrawals between accounts of VASPs opened at a specific bank, when a customer opens an account with their real name at such bank.

Acknowledgments

The authors would like to thank associates Miryung YANG and Christina GEE for their assistance in the research and writing of this chapter.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Hyun-il Hwang is a partner at Shin & Kim and a licensed attorney in South Korea. He is a key member of the firm's Finance Practice Group and leads the Fintech Team and Virtual Asset Team at the firm. He regularly advises on financial regulatory compliance matters, including market abuse in capital markets and derivative product transactions. In addition, he has been working with many market players in the metaverse sphere, dealing with blockchain, cryptocurrency and non-fungible tokens.

Mr. Hwang is highly regarded in the legal and business markets, representing many of the large local and foreign financial institutions in South Korea. Mr. Hwang's prior experience as a former financial regulator at the FSC helps him to address complex regulatory issues as a counsellor for Shin & Kim LLC to deal with regulatory compliance matters, transactions and financial disputes.

Prior to joining Shin & Kim LLC, Mr. Hwang was a regulator, having served as a Deputy Director for the Capital Markets Investigation Unit at the FSC. He also participated in legislative initiatives related to the enactment of the Enforcement Decree to the *Act on the Online Investment-linked Financial Business Protection of its Users* ("**P2P Act**"), worked on the Innovative Financial Service Scheme dealing with new and developing financial services, products and business models, as well as other key regulatory endeavours in the rapidly evolving financial markets. He is also former in-house counsel at Samsung Securities Co., Ltd. Mr. Hwang earned his undergraduate degree at Korea University and his law degree from Sogang University.

Shin & Kim LLC
23F, D-Tower (D2)
17 Jongno 3-gil, Jongno-gu
Seoul 03155
Korea

Tel: +82 2 316 4453
Email: hihwang@shinkim.com
URL: www.shinkim.com

Jaecheong Oh is a partner at Shin & Kim LLC, one of Korea's leading law firms. He specialises in financial regulation and advises clients on various matters related to traditional finance, virtual assets, fintech, and dispute resolution. He has extensive experience working with financial institutions, VASPs, virtual asset-related project teams, and fintech companies. He also has outstanding research skills and has participated in the revision and design of laws and regulations by governmental bodies and the Supreme Court. Mr. Oh is a highly accomplished legal professional who provides top-notch legal services to domestic and foreign clients.

Shin & Kim LLC
23F, D-Tower (D2)
17 Jongno 3-gil, Jongno-gu
Seoul 03155
Korea

Tel: +82 2 316 1782
Email: jcoh@shinkim.com
URL: www.shinkim.com

Shin & Kim is a top-tier law firm in South Korea with a stellar record as a trusted advisor to the world's leading South Korean and multinational corporations, financial institutions and government agencies for critical and ground-breaking mandates impacting businesses on a global scale. It is one of the largest law firms with 700+ professionals, including South Korean and foreign attorneys, patent attorneys, tax attorneys, certified public accountants, customs specialists, and other advisors. The professionals work in close-knit teams to deliver client-focused results through its offices in South Korea, including satellite offices in Beijing, Shanghai, Ho Chi Min, Hanoi and Jakarta, while leveraging its unrivalled network of leading international firms and consultants to collaborate on matters. The venerable Finance Practice Group with approximately 60 members enjoys a stellar reputation where its clients rely on the firm's commitment to quality and the pursuit of their commercial objectives.

www.shinkim.com

SHIN & KIM

© Published and reproduced with kind permission by Global Legal Group Ltd, London

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: glg global legal group