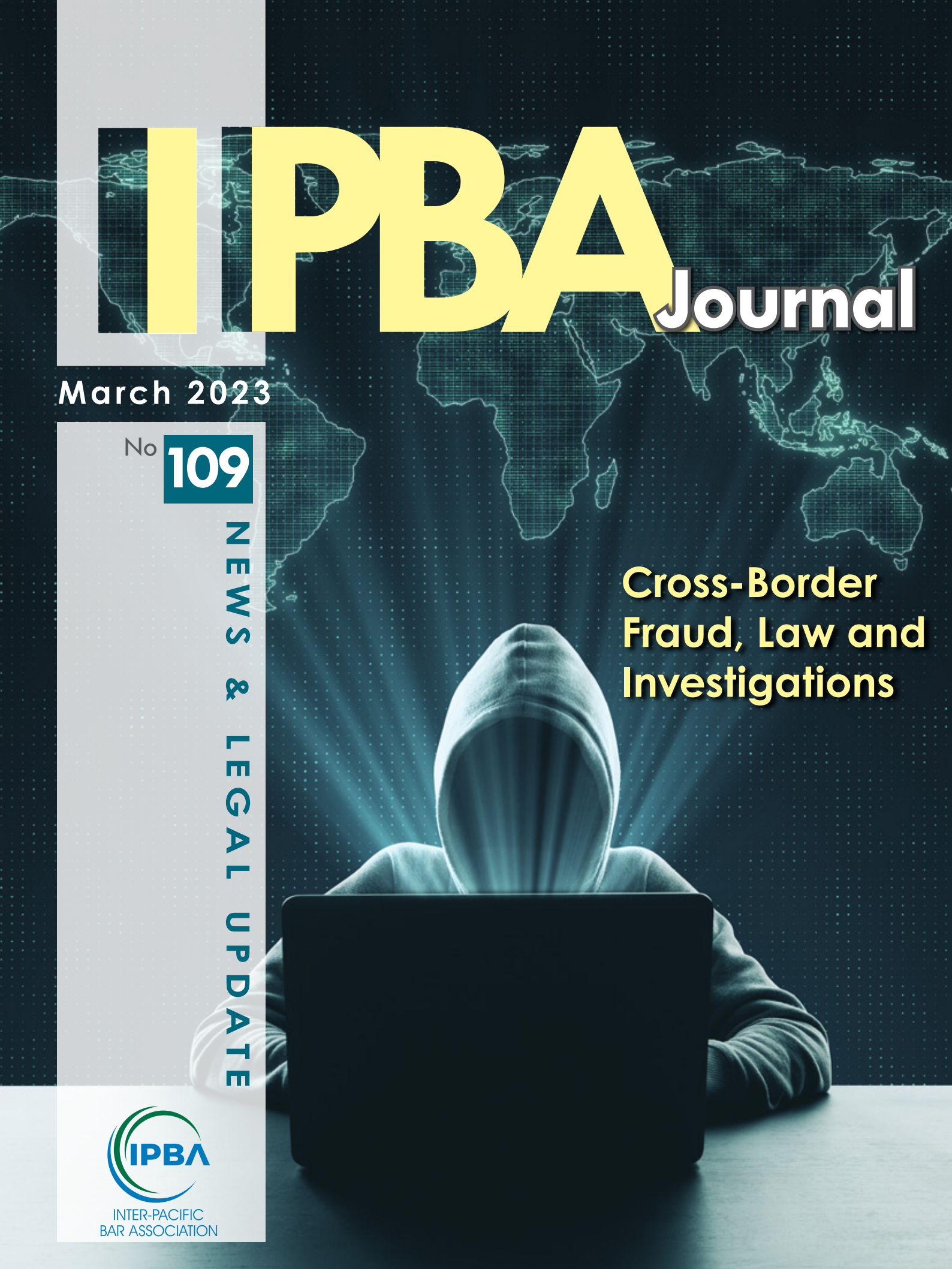
IPBA Journal

March 2023

No 109

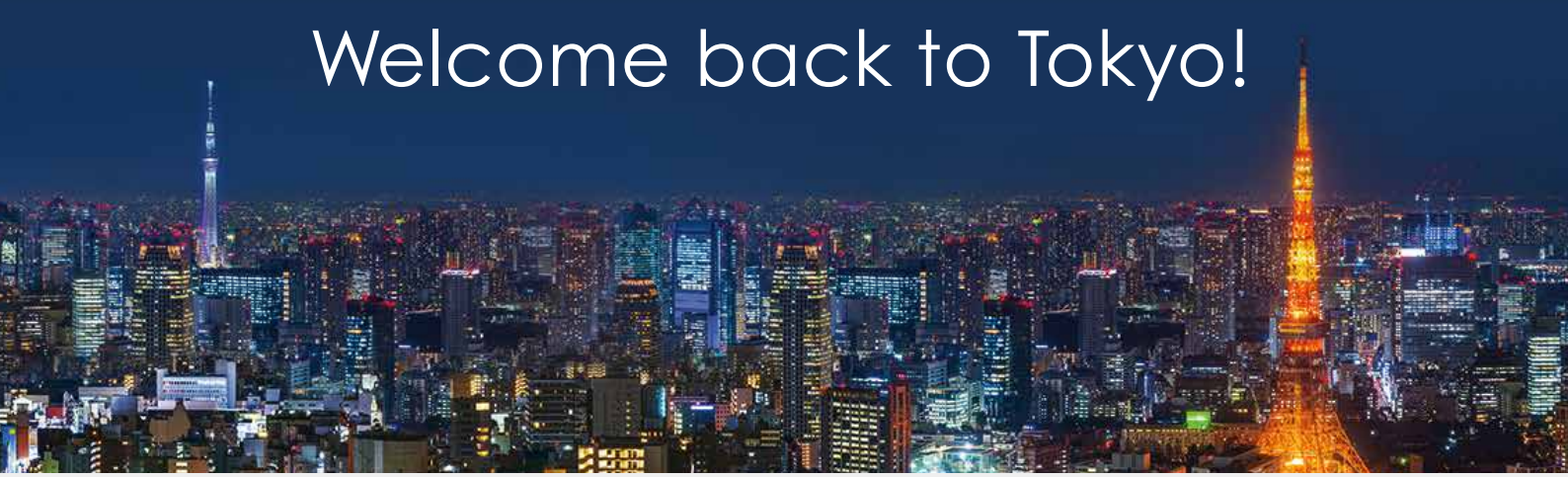
NEWS & LEGAL UPDATE

Cross-Border Fraud, Law and Investigations



INTER-PACIFIC BAR ASSOCIATION

Welcome back to Tokyo!



IPBA
TOKYO 2024
24-27 APRIL

Online Registration started for the IPBA Annual Conference 2024 in TOKYO!

IPBA Annual Meeting and Conference 2024 in Tokyo

New World, New Wisdom

Date
April 24-27, 2024

Venue
The Okura Tokyo, JAPAN

IPBA2024 Secretariat

c/o JTB Communication Design, Inc.
ipba2024@jtbcom.co.jp

IPBA 2024 Tokyo

The Inter-Pacific Bar Association (IPBA) established in April 1991 at an inaugural conference held in Tokyo is an international association of business and commercial lawyers who live, or have a strong interest, in the Asia-Pacific region. IPBA 2024 TOKYO provides the collaboration of Inter-Pacific countries, seeing a more integrated approach of doing business and creating opportunities across and even beyond its reach.

Be part of this gathering of industry leaders and experts and discover why it's more fun in Tokyo, Japan!

https://www.ipba2024.com/

IPBA Journal

The Official Publication of the Inter-Pacific Bar Association

Publisher	Ninehills Media Limited
Editor	Paul Davis
Editorial	Kiri Cowie Julie Yao
Design	Ester Wensing

Advertising Sales

Jennifer Luk
E: jennifer@ninehillsmedia.com
Frank Paul
E: frank@ninehillsmedia.com
T: +852 3796 3060

ninehills media

Ninehills Media Limited

Level 12, Infinitus Plaza,
199 Des Voeux Road,
Sheung Wan, Hong Kong
Tel: +852 3796 3060
Fax: +852 3020 7442
Email: enquiries@ninehillsmedia.com
Internet: www.ninehillsmedia.com

ISSN 1469-6495

IPBA is incorporated in Singapore.
Company registration number:
201526931R

Images: iStock

Cover painting: Arthur Williams

Contents

March 2023 No 109

INTER-PACIFIC BAR ASSOCIATION

IPBA Leadership March 2023

Officers

President
Richard Briggs
Hadef & Partners, *Dubai*

President-Elect
Miyuki Ishiguro
Nagashima, Ohno & Tsunematsu, *Tokyo*

Vice-President
Michael Chu
McDermott Will & Emery, *Chicago, IL*

Secretary-General
Yong-Jae Chang
Lee & Ko, *Seoul*

Deputy Secretary-General
Jose Cochingyan III
Cochingyan & Partners, *Manila*

Programme Coordinator
Jan Peeters
Stibbe, *Brussels*

Deputy Programme Coordinator
Sara Marchetta
Chiomenti - Italy, *Milan*

Committee Coordinator
Eriko Hayashi
ERI Law Office, *Osaka*

Deputy Committee Coordinator
Gmeleen Tomboc
Credit Suisse, *Singapore*

Membership Committee Chair
Melva Valdez
Bello Valdez Caluya and Fernandez, *Manila*

Membership Committee Vice-Chair
Sebastian Kuehl
Huth Dietrich Hahn Partnerschaftsgesellschaft, *Hamburg*

Publications Committee Chair
James Jung
College of Law, *Sydney*

Publications Committee Vice-Chair
Olivia Kung
Wellington Legal, *Hong Kong*

Chief Technology Officer
Riccardo Cajola
Cajola & Associati, *Milan*

Deputy Chief Technology Officer
Robert Quon
Dentons Canada LLP, *Vancouver*

Membership Leaders

Jurisdictional Council Members

Australia: Michael Butler
Finlaysons, *Adelaide*

Canada: Sean A. Muggah
Borden Ladner Gervais LLP, *Vancouver*

China: Jiang Junlu
Beijing Puran Law Firm, *Beijing*

France: Frédéric Dal Vecchio
FDV Avocat, *Neuilly-Sur-Seine*

Germany: Thomas Zwissler
Zirngibl Rechtsanwälte Partnerschaft mbB, *Munich*

Hong Kong: Myles Seto
Deacons, *Hong Kong*

India: Shweta Bharti
Hammurabi & Solomon Partners, *New Delhi*

Indonesia: Kurniawan Tanzil
SHIFT Counsellors at Law, *Jakarta*

Japan: Kenichi Masuda
Anderson Mori & Tomotsune, *Tokyo*

Korea: Jihn U Rhi
Rhi & Partners, *Seoul*

Malaysia: Tunku Farik
Azim, Tunku Farik & Wong, *Kuala Lumpur*

New Zealand: Michael Shanahan
Tompkins Wake, *Auckland*

Pakistan: Mohammad Abdur Rahman
Vellani & Vellani, *Karachi*

Philippines: Emerico De Guzman
ACCRALAW, *Manila*

Singapore: Chong Yee Leong
Allen & Gledhill LLP, *Singapore*

Switzerland: Urs Zenhäusern
Baker & McKenzie Zurich, *Zurich*

Taiwan: Chun-Yih Cheng
Formosa Transnational Attorneys at Law, *Taipei*

Thailand: June Vipamaneerut
Tilleke & Gibbins International Ltd., *Bangkok*

UK: Alex Gunning
One Essex Court, *London*

USA: Jeffrey Snyder
Crowell & Moring LLP, *Washington, DC*

Vietnam: Net Le
LNT & Partners, *Ho Chi Minh City*

At-Large Council Members

China: Xinyue (Henry) Shi
JunHe LLP, *Beijing*

Europe: Gerhard Wegen
Gleiss Lutz, *Stuttgart*

India: Manjula Chawla
Phoenix Legal, *New Delhi*

Latin America: Rafael Vergara
Carey y Cia, *Santiago*

Osaka: Kazuhiro Kobayashi
Oh-Ebashi LPC & Partners, *Osaka*

USA: Wilson Chu
McDermott Will & Emery, *Dallas, TX*

Regional Coordinators

Australasia & Southwestern Pacific Islands: Ben Smith
MinterEllison, *Sydney*

East Asia: Song Dihuang
Hui Zhong Law Firm, *Beijing*

Hawaii & Northern Pacific Islands: Steven Howard
Fiskars, *Tokyo*

Middle East: Mohammed R Alsuwaidi
Al Suwaidi & Co, *Dubai*

SE Asia: Sylvette Tankiang
Villaraza & Angangco, *Manila*

IPBA Committee Chairs/ Co-Chairs & Vice-Chairs

Anti-Corruption & Rule of Law
Lim Koon Huan, Skrine, *Kuala Lumpur* – Co-Chair
Susan Munro, K&L Gates, *Hong Kong* – Co-Chair
Anne Durez, Total SA, *Paris*
Siva Kumar Kanagabasai, Skrine, *Kuala Lumpur*

APEC
Wang Zhengzhi, Beijing Globe-Law Law Firm, *Beijing* – Chair
Raymond Goh, China Tourism Group Corporation Limited, *Hong Kong*
Zunu Lee, Yoon & Yang, *Seoul*
Ryo Matsumoto, Oh-Ebashi LPC & Partners, *Osaka*

Aviation and Aerospace
Jean-Claude Beaujour, Harlay Avocats, *Paris* – Chair
Gabriel R. Kuznietz, Demarest Advogados, *São Paulo*
Lai Wai Fong, Shearn Delamore & Co., *Kuala Lumpur*

Banking, Finance and Securities
Yuri Suzuki, Atsumi & Sakai, *Tokyo* – Co-Chair
Catrina Luchsinger Gaehwiler, MML Legal, *Zurich* – Co-Chair
Don Waters, McMillan LLP, *Toronto*
Vivek Kathpalia, Nishith Desai, *Singapore*
Stéphane Karolczuk, Arendt & Medernach S.A., *Hong Kong*
Vinay Ahuja, DFDL, *Bangkok*

Competition Law
Atsushi Yamada, Anderson Mori & Tomotsune, *Tokyo* – Co-Chair
Manas Kumar Chaudhuri, Khaitan & Co LLP, *New Delhi* – Co-Chair
Eva W. Cole, Winston & Strawn LLP, *New York, NY*
Andrew Matthews, Matthews Law, *Auckland*
Anthony F. Baldanza, Fasken, *Ontario*

Corporate Counsel
Christopher To, GILT Chambers, *Hong Kong* – Chair
Lakshmi Nadarajah, Christopher & Lee Ong, *Kuala Lumpur*

Cross-Border Investment
Charandeep Kaur, Trilegal, *New Delhi* – Co-Chair
Jan Bogaert, Stibbe, *Brussels* – Co-Chair
Kenichi Sekiguchi, Mori Hamada & Matsumoto, *Tokyo*
Eric Marcks, Southgate, *Tokyo*
Santiago Gatica, Freshfields Bruckhaus Deringer US LLP, New York, *NY*
André Brunschweiler, Lalive, *Zurich*
Haiyan (Sara) Zhang, Y & T Law Firm, *Suzhou*
Areej Hamadah, Legal Challenges Group, *Kuwait City*
Chester Toh, Rajah & Tann, *Singapore*
Heida Donegan, Dentons Kensington Swan, *Auckland*
Youn Nam Lee, Bae Kim & Lee, *Seoul*

Dispute Resolution and Arbitration
Sae Youn Kim, Kim & Chang, *Seoul* – Co-Chair
Koh Swee Yen, WongPartnership LLP, *Singapore* – Co-Chair
Mariel Dimsey, HKIAC, *Hong Kong*
Fei Ning, Hui Zhong Law Firm , *Beijing*
Marion Smith KC, 39 Essex Chambers, *London*
Thomas G Allen, Kilpatrick Townsend & Stockton LLP, *Washington, DC*
Kshama Loya, Nishith Desai Associates, *Mumbai*
Yutaro Kawabata, Nishimura & Asahi, *Tokyo*
Dorothee Ruckteschler, Independent Arbitrator & Lawyer, *Stuttgart*
Angela Lin, Lee and Li, *Taipei*
J Felix de Luis, Legal 21 Abogados, *Madrid*
Mark Mangan, Dechert, *Singapore*

DRAC Investment Arbitration Sub-Committee
Kshama Loya, Nishith Desai, *Mumbai*, Co-Chair
Lars Markert, Nishimura & Asahi, *Tokyo*, Co-Chair

Employment and Immigration Law
Carolyn Knox, Ogletree Deakins Nash Smoak & Stewart, P.C., *San Francisco, CA* – Chair
Björn Otto, CMS Hasche Sigle, *Cologne*
Christine Chen, Winkler Partners, *Taipei*

Veena Gopalakrishnan, Trilegal, *Bengaluru*
John Wilson, John Wilson Partners, *Colombo*

Energy and Natural Resources
Wang Jihong, Zhong Lun, *Beijing* – Chair
Manoj Kumar, Hammurabi & Solomon Partners, *New Delhi*
Karl Pires, Shearman & Sterling, *Tokyo*
Alberto Cardemil, Carey y Cia. Ltda., *Santiago*

Environmental Law
Rosa Isabel Peña Sastre, Lex Administrativa Abogacía, *Barcelona* – Chair
Jian (Scott) Li, Jin Mao Partners, *Shanghai*

Insolvency
Hiroe Toyoshima, Nakamoto & Partners, *Osaka* – Chair
Vivek Daswaney, V Law Partners, *Mumbai*
Ajay Bhargava, Khaitan & Co., *New Delhi*
David Ward, Miller Thomson LLP, *Ontario*

Insurance
Kemsley Brennan, MinterEllison, *Sydney* – Chair
Steven Wong, Azim, Tunku Farik & Wong, *Kuala Lumpur*
Takahiko Yamada, Anderson Mori & Tomotsune, *Tokyo*
Ying Shuang Wang, Rajah & Tann Singapore LLP, *Singapore*

Intellectual Property
Lidong Pan, Reiz Law Firm, *Guangzhou* – Chair
Jose Eduardo T. Genilo, ACCRA Law, *Manila*
Christopher Kao, Pillsbury Winthrop Shaw Pittman LLP, *San Francisco, CA*

International Construction Projects
Matthew Christensen, Kim & Chang, *Seoul* – Co-Chair
Alfred Wu, Norton Rose Fulbright, *Hong Kong* – Co-Chair
Karen Gough, 39 Essex, *London*
Mirella Lechna, Wardyński i Wspólnicy sp.k., *Warsaw*
Miranda Liu, Stellex Law Firm, *Taipei*
Peter Chow, King & Spalding (Singapore) LLP, *Singapore*

International Trade
Augusto Vechio, Beccar Varela, *Buenos Aires* – Chair
Seetharaman Sampath, Sarvada Legal, *New Delhi*
Ngosong Fonkem, Page Fura, P.C., *Chicago, IL*
Kala Anandarajah, Rajah & Tann, *Singapore*

Legal Development & Training
Raphael Tay, Law Partnership, *Kuala Lumpur* – Chair
Keanu Ou, Jin Mao Partners , *Shanghai*
Jonathan Lai, Watanabe Ing LLP, *Honolulu, HI*
Rosie Thuy Huong, Nguyen Van Hau & Associates, *Ho Chi Minh City*
Martin Polaine, Brooke Chambers, *London*

Legal Practice
James Miller, Reynolds Porter Chamberlain LLP (RPC), *London* – Chair
Abraham Vergis, Providence Law Asia LLC, *Singapore*

Maritime Law
Yosuke Tanaka, Tanaka & Partners, LPC, *Tokyo* – Chair
Cheng Xiangyong, Wang Jing & Co., *Beijing & Shenzen*

Next Generation
Valentino Lucini, Wang Jing & Co. Law Firm China, *Guangzhou* – Co-Chair
Julie Raneda, Schellenberg Wittmer Pte Ltd/Attorneys at Law, *Singapore* – Co-Chair
Ferran Foix Miralles, Gómez-Acebo & Pombo, *London*
Patricia Cristina Tan Ngochua, Romulo Mabanta Buenaventura Sayoc & De Los Angeles, *Manila*
Santiago Fontana, Ferrere, *Montevideo*

Scholarship
Mahesh Rai, Rose, Drew & Napier, *Singapore*– Chair
Sophia S.C. (Chea Chyng) Lin, Primordial Law Firm, *Taipei*
Kazuya Yamashita, Higashimachi, LPC, *Tokyo*
Varya Simpson, V Simpson Law, *Berkeley, CA*

Tax Law
Jay Shim, Lee & Ko, *Seoul* – Chair
Tracy Xiang, Y&T Lawyers, *Suzhou*
Charles C. Hwang, Crowell & Moring LLP, *Washington, DC*
Thomas Meister, Walder Wyss Ltd., *Zurich*
Ronald Parks, SMPP Legal Myanmar Co., Ltd., *Yangon*

Technology, Media & Telecommunications
JJ Disini, Disini & Disini Law Office, Manila – Co-Chair
Doil Son, Yulchon LLC, *Seoul* – Co-Chair
Masaya Hirano, TMI Associates, *Tokyo*
Lai Ling Tong, Raja, Darryl & Loh, *Kuala Lumpur*
Miriam Pereira, Oh-Ebashi LPC & Partners, *Tokyo*

Women Business Lawyers
Winnie Tam SC, Des Voeux Chambers, *Hong Kong* – Chair
Diep Hoang , DILINH Legal, *Ho Chi Minh City*
Goh Seow Hui, Bird & Bird, *Singapore*
Zhang Yun Yan, Jincheng Tongda & Neal, *Shanghai*
Frédérique David, Harlay Avocats, *Paris*
Yoko Maeda, City-Yuwa Partners, *Tokyo*

Past Presidents

Jack Li (Immediate Past President 2020-2022)
Jin Mao Partners, *Shanghai*

Francis Xavier (Past President 2019-2020)
Rajah & Tann LLP, *Singapore*

Perry Pe (2018-2019)
Romulo, Mabanta, Buenaventura, Sayoc & De Los Angeles, *Manila*

Denis McNamara (2017-2018)
Independent Consultant, *Auckland*

Dhinesh Bhaskaran (2016-2017)
Shearn Delamore & Co., *Kuala Lumpur*

Huen Wong (2015-2016)
Huen Wong & Co, *Hong Kong*

William A. Scott (2014-2015)
CI Investments Inc., *Toronto, ON*

Young-Moo Shin (2013-2014)
S&L Partners, *Seoul*

Lalit Bhasin (2012-2013)
Bhasin & Co., Advocates, *New Delhi*

Shiro Kuniya (2011-2012)
Oh-Ebashi LPC & Partners, *Osaka*

Suet-Fern Lee (2010-2011)
Morgan Lewis Stamford LLC, *Singapore*

Rafael A. Morales (2009-2010)
Morales & Justiniano, *Manila*

Gerold W. Libby (2008-2009)
Zuber Lawler & Del Duca LLP, *Los Angeles, CA*

Zongze Gao (2007-2008)
King & Wood Law Firm, *Beijing*

James McH. FitzSimons (2006-2007)
Bird & Bird, *Sydney*

Felix O. Soebagjo (2005-2006)
Soebagjo, Jatim, Djarot, *Jakarta*

Sang-Kyu Rhi (2004-2005)
Rhi & Partners, *Seoul*

Ravinder Nath (2003-2004)
Rajinder Narain & Co, *New Delhi*

Vivien Chan (2002-2003)
Vivien Chan & Co, *Hong Kong*

Nobuo Miyake (2001-2002)
MASS Partners Law Firm, *Tokyo*

John W. Craig (2000-2001)
(retired) *Toronto, ON*

Dej-Udom Krairit (1999-2000)
Dej-Udom & Associates Ltd, *Bangkok*

Susan Glazebrook (1998-1999)
Supreme Court of New Zealand, *Wellington*

Cecil Abraham (1997-1998)
Cecil Abraham & Partners, *Kuala Lumpur*

Teodoro D. Regala (1996-1997)
(deceased) *Manila*

Carl E. Anduri, Jr. (1995-1996)
Lex Mundi, *Lafayette, CA*

Pathmanaban Selvadurai (1994-1995)
Tan Rajah & Cheah, *Singapore*

Ming-Sheng Lin (1993-1994)
(deceased), *Taipei*

Richard James Marshall (1992-1993)
Glencore International AG

Kunio Hamada (1991-1992)
Hibiya Park Law Offices, *Tokyo*

Past Secretaries-General

Michael Burian (2019-2021)
Gleiss Lutz, *Stuttgart*

Caroline Berube (2017-2019)
HJM Asia Law & Co LLC, *Guangzhou*

Miyuki Ishiguro (2015-2017)
Nagashima Ohno & Tsunematsu, *Tokyo*

Yap Wai Ming (2013-2015)
Morgan Lewis Stamford LLC, *Singapore*

Alan S. Fujimoto (2011-2013)
Goodsill Anderson Quinn & Stifel, *Tokyo*

Gerald A. Sumida (2009-2011)
Carlsmith Ball LLP, *Honolulu, HI*

Arthur Loke (2007-2009)
Virtus Law LLP, *Singapore*

Koichiro Nakamoto (2005-2007)
Anderson Mori & Tomotsune, *Tokyo*

Philip N. Pillai (2001-2005)
Shook Lin & Bok, *Singapore*

Harumichi Uchida (1999-2001)
TMI Associates, *Tokyo*

Takashi Ejiri (1995-1999)
Natori Law Office, *Tokyo*

Nobuo Miyake (1991-1995)
MASS Partners Law Firm, *Tokyo*

The President's Message

Richard Briggs
President

Dear Colleagues, Members and Friends,

As we head into the final month of the first quarter of 2023, the organising committee of the IPBA Annual Meeting and Conference in Dubai is working harder than ever to bring you a memorable event for the first fully international annual conference since Singapore 2019. We all look forward to welcoming you to the JW Marriott Marquis Hotel Dubai for four days of receptions, committee sessions, dinners and networking opportunities. The theme of the Conference is "One World: Law & the Environment Beyond Covid", with sessions addressing the issues faced as the world emerges from the pandemic with a different perspective and new tools to address the challenges before us.

This conference will mark the end of my first term as IPBA President. As you may recall, the association took the unprecedented step of extending the term of my predecessor, Jack Li, and subsequently my term as well. The IPBA has had to take unusual measures to adapt to the disruptions caused by not being able to travel internationally, postponing and rearranging our Annual Conferences since 2020. Kudos to Jack for holding a very successful Annual Conference in Shanghai in 2021, although most of our members could not attend in person. The accepted practice of holding a Conference in Japan in a year ending with a "1" could not be followed and instead will now be held in spectacular fashion in 2024.

In Dubai, the IPBA leadership will meet with leaders of several other international and local bar associations to reaffirm our friendship or to establish new ties. In recent years we have been approached by an increasing number of entities with a solicitation to collaborate, which demonstrates that the IPBA is a premier global association with a high name value. The Officers are careful to make sure that the terms of any official agreements have mutual benefits that can be upheld by both parties, and we do have protocols regarding the types of associations with which we sign such agreements. Nonetheless, we welcome open discussion with other entities.

It has been an honour to serve as IPBA President the past year and I look forward to reconnecting with you all in Dubai.

Yours sincerely,

Richard Briggs
President

The Secretary-General's Message

Yong-Jae Chang
Secretary-General

Dear IPBA Members,

For the past two years, it has been a great honour for me to serve as Secretary-General of this wonderful and extraordinary, yet resilient, organisation. I could not have fulfilled this important role without the support of many friends at IPBA. I would like to thank all of the past and current Presidents, Vice-Presidents, Officers, Membership Leaders and Committee Chairs and Co-Chairs who worked very hard together to deal with so many unprecedented issues during the pandemic.

I still vividly remember the first-ever IPBA Virtual Conference which was held from 15 to 19 June 2021 and how the 30th Annual Meeting and Conference could not be fully celebrated by everyone. At last, it was great to meet many of the IPBA Officers and other Council members during our Mid-Year Council Meetings and the East Asia Forum in Seoul from 24 September to 26 September 2022. Many of our members put in much time and effort throughout the global pandemic and I am very confident that the IPBA will continue to go from strength to strength with its ability to handle both onsite and online conferences and seminars as necessary. As the new year has started, we are now looking ahead to successfully embark on our journey beyond the 30th anniversary.

This will be the first time our annual conference will be held in the Middle East and our IPBA members will finally be able to meet in person since the pandemic. I am very much looking forward to seeing many IPBA members and friends in Dubai. It will be held from 7 to 10 March 2023 with the theme of 'One World: Law & the Environment Beyond Covid'. The Host Committee in Dubai has been under great pressure due to prior postponement but, under the great leadership IPBA President Richard Briggs, they continued to strive to make this conference a great event (which everyone will remember for a long time) by having interesting and relevant topics (such as ESG, climate change, diversity and inclusion) as well as unique and enjoyable social functions.

Further, all IPBA members will benefit from the Process Improvement Project which will consolidate all of the IPBA's historic data, membership records and conference registration and payments into one simplified (and connected) system for more convenient use and better access by our IPBA members. It has been a rather long process for us to reach this milestone and I must thank my predecessor, Michael Burian, who originally commenced this project, and my successor, Jose Cochingyan, who will continue to support and improve this ongoing project. Also, my sincere gratitude to Randa (Rhonda) and Yukiko for their immeasurable support and their willingness to test and implement this new technology for the IPBA Secretariat.

Now, as my term is drawing to a close, I would like to also express my gratitude for your great friendship and cooperation and, in particular, those who helped to organise (and reschedule) past events during challenging times. I wish everyone health and happiness and look forward to seeing all of you in Dubai in March!

Yong-Jae Chang
Secretary-General

Message to the Reader

Dear Reader,

Welcome to the March issue of the IPBA Journal. The topic we have chosen for this month's issue of the Journal is 'Cross-Border Fraud, Law and Investigations'.

Cross-border fraud refers to a scam or fraud in which a criminal in one country uses deception to steal money or valuables from a victim in another country. As the world is more digitally connected than ever before, fraudsters take advantage of this online transformation to target weaknesses in online systems, networks, and infrastructure—which results in a large economic and social impact on governments, businesses and individuals worldwide.

Investigating cross-border fraud is often complicated because the criminal is in a different country from the victim. Lawyers dealing with cross-border fraud play a crucial role in identifying, preventing, and prosecuting fraudulent activities that occur across international borders. This may include investigation and identifying fraudulent activities and advising clients on compliance with international laws—including obtaining effective and time-critical legal remedies to secure and recover assets, including freezing injunctions, disclosure orders and other ancillary relief for the identification and protection of assets.

As for the articles relevant to the theme of this issue of the Journal, we would like to express our thanks to all the authors who have contributed to it. This issue inludes seven articles, with topics ranging from the UAE preventative measures in combating cross-border fraud, asset tracing and recovery and legal analysis of cross-border fraud in Chinese securities regulation, and a detailed discussion of cross-border fraud laws and issues from different jurisdictions, including the Netherlands, Russia, Vietnam and Poland.

The Publications Committee is currently engaged in a review of the publication and copyright guidelines. We aim to initiate a discussion on a new set of copyright guidelines by the IPBA Officers and Council for consideration during the next Council meeting. Discussions regarding the new layout and theme (or possibly themes) for the next Journal are also underway.

We hope that all readers enjoy what is yet another issue of the Journal replete with many interesting and informative articles from contributors covering a wide geographical span. Our Publications Committee Vice-Chair, Olivia, and I would like to thank all those who have contributed and we encourage all members of the IPBA to continue submitting articles for consideration for publication in future issues of the IPBA Journal.

Yours sincerely,

James Jung
Chair, Publications Committee

IPBA Upcoming Events		
Event	**Location**	**Date**
IPBA Annual Meeting and Conferences		
32nd Annual Meeting and Conference	Tokyo, Japan	1st Quarter 2024
33rd Annual Meeting and Conference	Chicago, IL, USA	1st Quarter 2025
IPBA Mid-Year Council Meeting and Regional Conference		
IPBA Council Meetings (Council Members only)	Jakarta, Indonesia	16-17 September 2023
Regional Conference (topic TBA)	Jakarta, Indonesia	18 September 2023
IPBA Local and Regional Events		
IPBA Arbitration Day	Singapore	30 August 2023
More details can be found on our web site: https://ipba.org The above schedule is subject to change.		

Preventive Measures Implemented by the United Arab Emirates to Combat Cross-Border Fraud

This article aims to examine the legal and procedural frameworks in place in the UAE to combat cross-border fraud, highlighting the country's efforts and the lessons that can be learned from these experiences. Based on the analysis, recommendations for further legislative reforms that could enhance the effectiveness of the UAE's system for combating cross-border fraud will be offered.

The Growing Threat of Cross-Border Fraud

As technology continues to advance, cross-border fraud has become an increasingly prevalent and dangerous threat to the global economy and financial systems. Fraudsters are constantly finding new ways to deceive and manipulate individuals, organisations and governments across international borders with the goal of financial gain.

While the United Nations has provided a general definition of fraud as 'any illegal or criminal deception aimed at achieving financial or personal gain', a clear definition of 'cross-border fraud' has yet to be established. International cooperation and legal frameworks are becoming increasingly important in preventing and combating financial crime.

The International Association of Financial Crime Investigators ('IAFCI') and The Association of Certified Fraud Examiners ('ACFE') have both provided specific definitions of cross-border fraud as 'An illegal act exemplified by deception, concealment or breach of

trust, which is committed across international borders for financial gain' and 'An intentional act to deceive or manipulate another individual, organisation, or government within a different country or territory for the purpose of unlawful financial or personal gain', respectively. These definitions emphasise the intentional nature and the element of deception involved. In the United Arab Emirates ('UAE'), the legislation has not provided a specific definition of cross-border fraud, but it is addressed in both the Federal Penal Code and the Law on Combating Rumors and Cybercrimes.

Cross-border fraud can take various forms, ranging from sophisticated cyberattacks to simple low-tech scams. One prevalent form of this type of fraud is phishing, where scammers send emails that appear to be legitimate, often from banks or government institutions. These emails contain a link or attachment that when clicked installs harmful software or directs to a fake website where the recipient is asked to enter sensitive information. This may lead to identity theft, where criminals use personal information such as names, dates of birth and passport numbers to open bank accounts, apply for loans or credit cards, make fraudulent purchases and more in the names of victims. To combat cross-border fraud, countries must collaborate and coordinate their efforts. This includes working to defeat related crimes such as money laundering.

The UAE has ratified several international agreements and conventions to address cross-border fraud, including the United Nations Agreement to Combat Corruption in 2006 and the United Nations Convention against Transnational Organized Crime in 2006. The UAE also signed regional treaties such as the Arab Convention Against Corruption and the Gulf Cooperation Council Convention on Combating Fraud and Financial Crimes, both aiming to prevent and combat financial crimes, including cross-border fraud.

The UAE's Proactive Strategy for Combating Cross-Border Fraud

Background

The UAE has become a hub for international trade and commerce, making it susceptible to fraudulent activities targeting victims beyond its borders. To effectively address cross-border fraud, the UAE has implemented a comprehensive set of regulatory and legal measures aimed at preventing fraudulent activities and prosecuting those responsible.

Overall, the UAE's approach to fighting cross-border fraud involves a combination of legal and regulatory measures, international cooperation and robust enforcement efforts. The efforts have helped create a secure and transparent financial environment in the Emirates, benefitting both individuals and companies operating within the state. This article focuses on the legislative and practical measures adopted by the UAE to combat cross-border fraud.

The UAE has implemented a comprehensive legal framework to combat cross-border fraud, including specialised courts, bilateral and international agreements, and various laws such as Federal Law No (7) of 2014 on Anti-Terrorism Crimes, Federal Law No 20 of 2018 on Criminalization of Money Laundering, Decree Federal-Law No (34) of 2021 on Combating Rumours and Cybercrimes, Federal Law No 1 of 2006 on E-transactions and Commerce, Law No (9) of 2022 on Regulating Provision of Digital Services in the Emirate of Dubai and Decree-Law (46) of 2021 on Electronic Transactions and Trust Services. These measures aim to protect society from electronic crimes committed through internet networks and technologies.

However, it is difficult to distinguish cross-border fraud from other crimes that target countries, as cross-border fraud often has parallel criminal objectives that target countries themselves. For instance, in 2019 the Federal Supreme Court in Abu Dhabi convicted two individuals of providing financial support to Jabhat Al-Nusra, an Al-Qaeda affiliated group in Syria, by transferring over AED2.2 million (approximately US$600,000) through e-transfers.

As reported on the website of the Federal Authority for Identity and Citizenship on 8 March 2013, the General Department of Criminal Investigations Management of the Dubai Police arrested an electronic fraud gang composed of African and Asian nationals who specialised in hacking programs to obtain the information of companies and steal their money, both inside and outside the state. The police seized commercial papers and forged cheques worth AED6 billion (US$1.63 billion) from the gang.

The 2011 'Norton' report on internet security revealed that cybercrime costs the UAE economy approximately AED2.25 billion (US$610 million) annually. The report also highlighted that at least two UAE residents fall victim

to cybercrime every minute through viruses, phishing emails and phishing attacks aimed at acquiring confidential and banking information.

The UAE has a legislative policy that monitors gaps and deficiencies to effectively combat cross-border crimes, specifically fraud. The legislator continuously issues new laws related to new forms of trade and financial transactions, including Law No (4) of 2022 on Regulating Virtual Assets in the Emirate of Dubai, which aims to establish an integrated legal framework to protect investors, set guaranteed international standards for the governance of virtual assets and promote responsible commercial growth. The Securities and Commodities Authority also takes steps to protect investors in the state by notifying them to be careful in relation to fund-raising activities based on investing in digital/encrypted assets that may be unregulated or operated outside the state. Additionally, the Authority formed a work team to facilitate the implementation of financial technology initiatives and to allocate an email to receive questions and answer inquiries related to financial technology.

The UAE has been actively engaging in international cooperation with legal systems that share similar goals and advancing technologies to combat cross-border fraud.

The state's efforts to combat cross-border fraud crimes are not limited to direct intervention. Legislative and procedural interventions were put in place to cover many shortcomings that prevent having a more effective procedural system. For instance, the enactment of Federal Law No 14 of 2020 on Protection of Witnesses and the like activated the role of community participation in uncovering crimes, which closed the gap of the absence of an effective procedural system that provides protection for witnesses and victims, especially in the case of organised criminal groups. Although international conventions such as the United Nations Convention against Organized Crime and the annexed protocols require this type of protection, the UAE was late with this international approach, but later redressed this issue.

In its efforts to combat cross-border fraud, the UAE actively seeks to cooperate with other countries and stay up to date on the latest legal developments and technologies. The UAE participated in various conferences and conventions organised by the United Nations and the International Bar Association, bringing together legal professionals, law enforcement agencies and other stakeholders to develop strategies to combat cross-border fraud.

The UAE has been actively engaging in international cooperation with legal systems that share similar goals and advancing technologies to combat cross-border fraud. This has been achieved through various conferences and conventions, such as the United Nations Global Conference on Combating Counterfeiting and Piracy held in Dubai in 2008, which discussed the latest trends in the field of counterfeiting and piracy and developed strategies to address these issues. Another important annual conference was held in Dubai in 2011 by the International Bar Association discussing 'Cross-Border Fraud: Legal Trends and Challenges', which focused on the latest legal trends and challenges related to cross-border fraud and its investigation.

One of the most significant forms of cooperation adopted by the UAE to prevent cross-border fraud crimes is the signing of mutual legal assistance treaties ('MLATs') with other countries. The first mutual legal assistance agreement was signed between the UAE and the Republic of France in 1995, followed by many mutual agreements with countries in Europe, Asia and the Americas and neighbouring countries in the Middle East and North Africa, such as the Kingdom of Saudi Arabia, Bahrain and Egypt. In 2018, the UAE signed a memorandum of understanding with the United Kingdom to enhance cooperation in the field of financial intelligence and combating money laundering and terrorist financing. This aimed to establish a common framework for exchanging information and expertise, conducting joint investigations and coordinating efforts to prevent and disrupt financial crimes. The UAE also expanded its cooperation with countries in Asia, such as the Republic of China in 2020 and the Republic of India in 2021, to enhance cooperation in combating economic crimes and cybercrime, exchanging information and best practices, joint training and capabilities building.

The UAE's preventive approach also included intelligence agreements and joint international

operations with many countries. In 2019, in collaboration with the United States of America and other countries, it participated in a process aimed at removing an international network of fraudsters who were involved in a scheme to steal millions of dollars from companies and individuals through fake online auctions. The operation resulted in the arrest of more than 280 individuals worldwide.

In addition to mutual legal assistance agreements, the UAE has also established formal and informal networks for exchanging information and conducting joint investigations with other countries. For example, the UAE is a member of the Egmont Group, an international network of financial intelligence units that share information to combat money laundering and financing of terrorism. The country is also a signatory to various United Nations conventions aimed at combating fraud and other forms of organised crime, including the United Nations Convention against Corruption and the United Nations Convention against Transnational Organized Crime.

Furthermore, the UAE has established specialised bodies and working teams to investigate and prosecute cross-border fraud cases. These include: the Financial Intelligence Unit at the Central Bank of the UAE ('FIU'), which collects, analyses and disseminates financial information related to money laundering and terrorist financing; and the Cybercrime Department of the Dubai Police which investigates cybercrime, including cross-border fraud that occurs through electronic means.

The UAE courts have played a pivotal role in preventing cross-border fraud by issuing judicial rulings that create a deterrent effect. Examples of such rulings include the sentencing of a British national to 10 years in prison for defrauding investors of approximately AED75 million (US$20.4 million) through a fraudulent cryptocurrency scheme and the sentencing of two individuals to 10 years in prison for their involvement in a fraud scheme that cost a company AED30 million (US$8.1 million).

The Role of Governmental Financial Institutions in Dealing With Cross-Border Fraud

To fully understand how financial institutions in the UAE combat cross-border fraud, it is necessary to discuss the role of the UAE Central Bank in safeguarding the economy under the direction of the country's leadership.

The UAE Central Bank has established various Anti-Money Laundering and Terrorist Financing ('AML/CFT') regulations that apply to all financial institutions operating within the UAE. These regulations require financial institutions to develop policies, procedures and systems to prevent money laundering and terrorist financing activities, conduct customer due diligence, monitor transactions and report suspicious activities to the relevant authorities. Financial institutions must comply with guidelines for customer identification and verification information ('KYC') and disclose beneficial ownership of accounts and transactions, as specified in the Central Bank Circular No 24 of 2017.

The Central Bank also mandates regulations on combating the financing of terrorism and electronic funds transfer ('EFT') which describes the methods and procedures for monitoring and reporting suspicious electronic transfer transactions, and customer due diligence ('CDD') which outlines procedures for assessing high-risk customers and transactions in accordance with the guidelines of Circular No 42 of 2018.

Furthermore, the Central Bank ensures compliance with the sanctions systems through its sanctions compliance regulations, requiring financial institutions to implement measures to prevent individuals and entities subject to penalties from accessing funds. The Central Bank's responsibilities extend to enforcing penalties imposed by foreign entities on perpetrators of cross-border fraud crimes.

The Central Bank has increased penalties for financial institutions that do not follow its decisions, including fines, suspension or cancellation of licences and criminal prosecution. in 2019, the Central Bank imposed penalties on several banks for non-compliance with AML/CFT regulations, ranging from fines to licence suspension, due to failure to implement customer due diligence measures, maintain updated records and report suspicious activities. The Central Bank's actions show its commitment to preventing cross-border fraud and enforcing regulations.

As a result, the UAE's efforts to combat cross-border fraud have been recognised internationally, and the state was placed on the 'grey list' by the Financial Action Task Force ('FATF') for its commitment to implementing effective measures against AML/CFT.

Regulating Electronic Fund Transfer ('EFT') in the UAE

Given the UAE's global economic environment, EFT has become a widely used payment method by companies and individuals to transfer funds electronically with the goal of ensuring secure and safe transactions. Considering this, the UAE government has issued several regulations that govern the operations of ETFs and outlines the responsibilities of the parties involved in these transactions.

It is important to note the prevalence of fraud crimes associated with EFTs, as well as the target of these crimes, which has caused the UAE to focus on organising this type of transaction. One such example of EFT fraud occurred in 2016 when hackers breached the computer systems of the Central Bank of Bangladesh and transferred US$81 million from its account at the Federal Reserve Bank in New York to accounts in the Philippines and Sri Lanka using fraudulent SWIFT messages to initiate transfers and conceal their tracks. The perpetrators chose the Philippines as a major centre for money laundering activities, especially within the casino industry which is not subject to the same anti-money laundering regulations as banks.

The UAE courts have played a pivotal role in preventing cross-border fraud by issuing judicial rulings that create a deterrent effect.

The incident was one of the largest electronic thefts in history and raised concerns regarding the vulnerability of the global financial system to cyberattacks. It also highlighted the requirement for stronger cybersecurity measures and international cooperation to combat cross-border fraud. While the UAE was not directly involved in the incident, its financial system was used for money laundering activities related to stolen funds as the perpetrators used the stolen funds to purchase luxury goods and real estate in the UAE and other countries.

To strengthen cybersecurity and prevent cross-border fraud involving EFT, the UAE authorities implemented several measures after the 2016 incident. These measures included due diligence and monitoring requirements for financial institutions, stricter regulatory oversight and increased cooperation and information sharing with foreign law enforcement agencies and regulators.

As part of its role in stabilising the country's economic system, the UAE Central Bank was assigned the task of organising electronic transfer operations and has set many requirements for licensed payment service providers. The regulations stipulate that only regulated and authorised entities can provide wire transfer services, mitigating the risk of fraudulent transactions and ensuring transparency and accountability in the payment process.

In addition, payment service providers must implement security measures, such as encryption, to protect transfer transactions as well as other security protocols to prevent unauthorised access to payment systems and data breaches. They are also required to apply AML/CTF measures to prevent financial crimes and ensure the transaction is processed accurately and securely. Payment service providers must keep accurate records of electronic transfer transactions and report any suspicious transactions to the authorities.

The regulations also clarify the dispute settlement process, enabling parties to resolve any disputes arising during the payment process. Payment service providers are obliged to report any suspicious transactions to the authorities and maintain accurate records of electronic transfer transactions.

The Central Bank of the UAE performs routine inspections on payment service providers to ensure their adherence to guidelines and regulations, thereby enforcing compliance. Violators of wire transfer regulations may face penalties or legal action from the bank.

Furthermore, the UAE also has multiple regulatory bodies and law enforcement agencies who collaborate to identity and scrutinise fraudulent activities. Examples of such entities include the Dubai Financial Services Authority ('DFSA'), Abu Dhabi Global Market ('ADGM') and the Federal Public Prosecution.

The Vital Role of Lawyers in Assisting Clients to Detect Cross-Border Fraud Under UAE Law

In order to protect clients from suspicious or harmful activities, lawyers play a crucial role that is particularly

important when it comes to identifying cross-border fraud in the UAE. Due to the constantly evolving nature of fraud schemes, it is essential that lawyers stay up-to-date with laws and regulations surrounding cross-border fraud and related offences to be able to assist clients effectively. This often requires specialised attention, including exercising due diligence when dealing with potential business partners, vendors or clients by researching their history, reputation and financial position, conducting background checks on key individuals involved, reviewing financial transactions and contracts, and drafting contractual clauses that address potential fraudulent activities.

In the event of fraud, lawyers are obliged to report any suspicious activity to the appropriate authorities and provide legal representation to victims in legal proceedings aimed at recovering damages. This may involve taking legal action against perpetrators or representing the client in investigations conducted by regulatory authorities.

Given the complexities of cross-border fraud, particularly when a perpetrator is located outside the borders of the UAE, filing a judicial claim can be a complicated and challenging process. Nonetheless, there are practical legal steps that can be taken when pursuing a cross-border fraud case in accordance with UAE law.

The initial step in pursuing a cross-border fraud case under UAE law is to gather evidence, such as financial documents, emails, contracts and other relevant information that meet the legal requirements. The second step is to determine the appropriate jurisdiction by analysing contracts, agreements and laws and contacting relevant authorities in the UAE, such as the FIU or the Cybercrime Department of the Dubai Police, to assist in the investigation and coordinate with international partners in locating suspected fraudsters. It is important to note that the authority to which a complaint is submitted depends on the nature of the fraud, such as the Central Bank, DFSA or ADGM.

After obtaining a favourable judgment, the lawyer must legally seek to implement the ruling, which may require navigating procedural laws and researching legal and procedural conflicts between different countries. Cooperation between law firms in different countries is essential to understand and interpret foreign laws, avoid the establishment of incorrect judicial claims and expedite the time required for clients to obtain their rights from perpetrators. This cooperation also facilitates obtaining judicial orders in foreign states to prevent perpetrators from continuing fraudulent activities and pursuing civil and criminal prosecution, ensuring protection of the procedural system against invalidity.

INTERPOL should play a more significant role in strengthening global cooperation to confront cross-border fraud.

Challenges to Enhancing Cooperation in Combating Cross-Border Fraud

Cross-border fraud presents significant challenges that require extensive international cooperation to combat them effectively. Despite efforts to establish legal frameworks and mechanisms for cooperation, several obstacles impede the ability of countries, including the UAE, to cooperate more effectively in this area.

One of the main obstacles is conflicting legal frameworks and cultural differences, as different countries have varying laws that can lead to conflicts and challenges when pursuing cross-border fraud cases. For example, the United States has a strong legal framework for prosecuting cross-border fraud cases such as the Foreign Corrupt Practices Act ('FCPA'), while other countries may have weaker or less comprehensive legal frameworks.

Additionally, different legal cultures may have different attitudes towards fraud, affecting the willingness of countries to cooperate with each other. Another important obstacle to international cooperation in this field is the issue of sovereignty. Each state and judicial system has its own sovereignty, which places restrictions on the extent of their ability to enforce foreign judgments and laws in their territory or enforce their laws and provisions outside their territory. This creates difficulty in recovering funds or property which have been subject to fraud and also prosecuting perpetrators of cross-border fraud, particularly in the absence of a mutual legal assistance treaty between the two countries.

Further challenges to effective international cooperation in combatting cross-border fraud is the poor exchange of information and communication between law enforcement agencies in different jurisdictions which can result in a lack of coordination in following up cross-border cases and exchanging important information, such as intelligence on suspects, ongoing investigations and other crucial details. Recovering assets located in a different country from the one where the judgment was issued can be particularly difficult, as can navigating different legal systems and processes which may be necessary to achieve this. Close cooperation is vital in such situations.

Lack of resources may also pose a significant obstacle in international cooperation. Investigating and prosecuting cross-border fraud cases can be expensive and time-consuming. Many countries may lack the necessary resources or expertise to handle investigations of this complexity or to pursue cases through the international legal system. This should not be overlooked as a major challenge to combatting cross-border fraud effectively.

Proposed Recommendations to Enhance the State's Response to Cross-Border Crimes

Despite the challenges discussed, there is still much that can be done to improve the effectiveness of combatting cross-border fraud, including improving investigations and trials, and enforcing these rulings outside the jurisdiction. To address these challenges, the UAE can strengthen its legal and regulatory frameworks, increase the capacity and resources of its law enforcement agencies and regulators and enhance its cooperation with other countries and international organisations.

Improving public awareness and education about the risks of cross-border fraud can also be beneficial, as well as highlighting the importance of reporting suspicious activities to competent authorities and agencies through public awareness campaigns and training programs for financial institutions and other organisations at risk. Mandatory training programs can also be implemented for specialists and those associated with the legal field to periodically review developments related to this type of crime and technical acts and follow the latest jurisprudence and legal developments issued by comparative legal jurisdictions. In addition, expanding the 'Digital Citizen' program to improve community members' ability to use electronic services can be helpful.

At the global level, a specific legal framework can be developed to regulate the use of cryptocurrencies to prevent their use in cross-border fraud and legal protection can be strengthened for whistleblowers. Enhanced cooperation and coordination between international partners, including participation in international conferences and workshops focused on combating cross-border fraud, can also be useful.

INTERPOL should play a more significant role in strengthening global cooperation to confront cross-border fraud. It should urge member states to adopt a consistent legal framework for prosecuting those responsible for such crimes, based on guidelines issued by international organisations such as the United Nations and the World Bank. Additionally, INTERPOL should propose the creation of a robust international mechanism for exchanging information, utilising modern technology to ensure quick and secure communication among law enforcement agencies. This would simplify the mutual legal assistance process and enhance the accuracy and efficiency of information exchanged.

Abdulla Ziad Galadari
Senior Partner, Galadari Advocates & Legal Consultants, Dubai

Abdulla is a key influencer across the UAE, supporting a diverse range of businesses and senior dignitaries to navigate the legal framework of the country. He is the strategic leader behind the firm's progressive approach, introducing global lawyers, sharing key insights with the market, and developing and executing a technology-driven strategy which will continue to drive innovation within the legal profession.

He actively supports the young Emirati leaders of tomorrow through internship programmes and training contracts for new graduates enabling over 30 Emirati lawyers to obtain a federal lawyer's license, growing the UAE's inhouse professional capabilities.

The author would like to thank Abdalmeged Alsweedy and Gheith Cherkeh for their assistance with this article.

Asset Tracing and Recovery—How Tools in the Caribbean Can Help Trace and Recover Assets in Asia

Asset tracing and recovery ('ATR') is a crucial area for those who find themselves caught up in fraud and investigatory situations. When it comes to the tools available for ATR, the Caribbean jurisdictions of the Cayman Islands, British Virgin Islands ('BVI') and Bermuda offer a powerful arsenal for dealing with complex and often cross-border scenarios, including where parties are seeking to trace and recover assets in Asia.

Introduction

The sphere of ATR, particularly the extent of tools available around the world, is rightly attracting more attention in cross-border fraud and investigations. This includes projects at the international level, such as UNCITRAL's ongoing efforts (for which the author acts as an expert), as well as attention being given in national legislatures around the world. This makes perfect sense as ATR is often a pass/fail requirement; if you cannot trace, secure and recover meaningful assets, it is irrelevant what legal remedies may on paper otherwise be open to the victim.

In the Caribbean legal jurisdictions, owing to the strong influence of the English legal system, a number of the quintessential tools that can be used for ATR in common law jurisdictions are also available and widely used under the legal systems of the Cayman Islands, BVI and Bermuda. This article will explore these various tools in the Caribbean, take stock of their current development and demonstrate how they are used, including in cross-border situations.

As will be illustrated in the cases that are discussed, the Courts of the Caribbean jurisdictions are familiar with and have substantial experience in dealing with cross-border cases, so where clients from Asia require assistance, there are a variety of powerful options standing ready.

The Foundations

When it comes to ATR, there are a number of classic tools, including Norwich Pharmacal, Bankers Trust and Mareva orders. These are available under all of the Caribbean jurisdictions of the Cayman Islands, BVI and Bermuda—although there may be differences in detail in how these orders are required to be applied for and function, they are broadly the same as in many common law jurisdictions.

One additional feature of the Caribbean jurisdictions is that in the latter stages of asset recovery, if there is any need for restructuring or liquidation, these jurisdictions are also well versed in the use of receivers and liquidators, both to protect value and enhance recovery efforts.

In the following sections of the article, we will discuss the basic foundational elements of the tools that can be used for ATR and explore some interesting new cases, many involving Asian elements, that showcase how these tools have been deployed in practice in fraud, asset tracing and recovery cases.

Norwich Pharmacal Orders

Overview

Norwich Pharmacal orders are a well-known and powerful disclosure tool that have a long history of being used in asset tracing situations to obtain information from third parties. Called Norwich Pharmacal orders following the case of Norwich Pharmacal Co v Customs and Excise Commissioners [1974] AC 133, they are typically sought against those who have become 'mixed up' in the wrongdoing committed by another person or entity, because this can often be an effective way of seeking out information about the missing assets.

The requirements for a Norwich Pharmacal order tend to be quite stringent, commensurate with the power of the remedy. In essence, a party applying for the order must be able to show: (1) a good arguable case of wrongdoing; (2) the respondent involved in the wrongdoing is more than a mere witness; (3) the target of the order is likely to have the documents that are being sought; and (4) the order being sought is necessary and proportionate in the interests of justice.

For the Caribbean jurisdictions, what we often see is that Norwich Pharmacal orders are sought against professional providers of registered office services ('ROs'), as they often hold information about companies by way of their 'know your customer' and anti-money laundering requirements. These ROs will also likely have information about a company's shareholders or beneficial owners, which can also be useful in cases of asset tracing. Following amendments to the relevant legislation at the beginning of this year in the BVI, there is also now the prospect of obtaining detailed accounting records from ROs there; a tantalising and powerful treasure trove of information for ATR.

Related to a Norwich Pharmacal order is a gagging order, which is often sought in conjunction.

Related to a Norwich Pharmacal order is a gagging order, which is often sought in conjunction. Gagging orders prevent the person against whom the order has been granted from disclosing the fact that it has been ordered to disclose information. The purpose of this is to avoid tipping off, or the risk of the wrongdoer finding out and therefore destroying evidence or dissipating assets.

Viewed from the lens of Asian clients, a Norwich Pharmacal order can be particularly useful because such an order can also be used across jurisdictions, for example, by the Court of the Cayman Islands granting a Norwich Pharmacal order in support of foreign proceedings, such as proceedings in Hong Kong.

Essar Global Fund Ltd et al v Arcelormittal USA LLC

The area of Norwich Pharmacal orders has undergone insightful and multi-faceted development in the case law. A good illustration is from the Cayman Courts. In the case of Essar Global Fund Ltd et al v Arcelormittal USA LLC (Civil) Appeal No 15 of 2019, the Cayman Court characterised Norwich Pharmacal orders' jurisdiction as 'broad, flexible and developing' and said that the Courts should adopt a 'common sense non-technical approach' when dealing with such applications.

In that case, the dispute concerned a jurisdictional dispute between ArcelorMittal USA LLC ('AMUSA') and parties related to Essar Global Fund Limited ('EGFL') and Essar Capital Limited (collectively with EGFL, the Essar Parties). AMUSA applied for a Norwich Pharmacal order to seek disclosure of information and documents by the Essar Parties, the purpose of which was to assist with the enforcement of an ICC Arbitral Award obtained against Essar Steel Limited, a Mauritian-incorporated subsidiary of EGFL. The Essar Parties objected to the Norwich Pharmacal order on, *inter alia*, grounds that the relief could not be granted for the purpose of enabling AMUSA to use the information or disclosure to pursue foreign proceedings.

The argument of the Essar Parties was that the relevant provision for international evidence assistance ('Evidence Order') already conferred statutory jurisdiction on the Cayman Islands Grand Court to respond to requests from foreign courts for oral and documentary evidence to be used in foreign proceedings which are pending or contemplated, and therefore this should be the exclusive route for obtaining information or documents for the purposes of foreign proceedings.

The case proceeded to the Caribbean Islands Court of Appeal ('CICA'), which drew an interesting distinction between the Norwich Pharmacal jurisdiction and the grant of relief under the Evidence Order. It held that the former was for the purpose of providing information about wrongdoing and the latter was to impose an obligation for the provision of evidence. In particular, the CICA explained that: (1) the courts of the Cayman Islands have no inherent jurisdiction to order evidence to be provided for the purpose of foreign proceedings; and (2) where provision in the statute was made for the production of evidence, there will be an implied exclusion of any overlapping jurisdiction that might otherwise exist.

Overall, however, the CICA continued with the flexible approach of the Grand Court. It stated that 'so long as care is taken to confine the Norwich Pharmacal jurisdiction to its proper scope, there can in principle be

no overlap between that jurisdiction and the statutory regime relating to evidence in foreign proceedings, and accordingly no reason to regard the former as excluded by the latter'. The CICA explained that it did not see 'why legislation dealing with the giving of evidence in foreign proceedings should be treated as impliedly excluding jurisdiction to order the provision of information necessary to enable foreign proceedings to come into existence at all—such as, in Norwich Pharmacal itself, information about the identity of the wrongdoer'.

What the CICA decision shows is that in the area of Norwich Pharmacal orders, the law of the Cayman Islands has diverged somewhat from that in England and Wales and instead has aligned itself more closely with recent decisions in other offshore jurisdictions. In March 2021, the Essar Parties applied for leave to appeal the CICA's decision to the Judicial Committee of the Privy Council ('JCPC'), but the CICA refused to grant leave, on the basis that the Essar Parties did not have an appeal as of right and that the matters raised in the appeal did not raise questions of great general or public importance. The JCPC also dismissed the Essar Parties' challenge to the CICA decision by finding that the appeal did not raise an arguable point of law and the CICA was right for the reasons it gave.

In all of the Caribbean jurisdictions, the approach with regards to Norwich Pharmacal orders in aid of foreign proceedings has generally been flexible, but in the BVI in particular, the Eastern Caribbean Supreme Court (Virgin Islands) (Amendment) Act confirmed the BVI Court's jurisdiction to make disclosure orders (for example, Norwich Pharmacal/Bankers Trust orders) in support of actual or contemplated foreign proceedings, even where a letter of request might also be available to the applicant as an alternative. This confirms that the BVI Court will not be bound by the English decision in Ramilos Trading Limited v Buyanovsky [2016] EWHC 3175 (Comm). Although several decisions of the BVI Court had already confirmed that it would not follow Ramilos Trading, this legislative amendment adds further certainty in this important area, and therefore in some respects provides even more clarity than the BVI's fellow Caribbean jurisdictions, such as the Cayman Islands.

Bankers Trust Orders

Overview

An application for a Bankers Trust order is similar to seeking a Norwich Pharmacal order and the basic requirements are the same, except that there will also be an added requirement of demonstrating that there is good reason to believe that the target is holding property that was misappropriated by fraud or breach of trust and which the applicant also had a proprietary claim to. The target is usually confidential documents held by a bank to support a proprietary claim, and in this scenario they are of considerable value to a victim to further its ATR efforts.

Singularis v Daiwa Capital Markets Europe

To supplement the picture regarding the involvement of banks, recent case law also provides an interesting perspective into the scenario of where money has been misappropriated by those with control over a victim's bank accounts. In such cases, a claim may potentially arise against the victim's banks who effected any relevant transfers of money.

A bank owes a duty of reasonable skill and care to its customers when executing a customer's order (commonly known as the Quincecare duty). A bank will have liability if it executed an order knowing it to be dishonest or was wilfully blind or reckless in failing to make sufficient enquires about the appropriateness of the order. In the case of Singularis v Daiwa Capital Markets Europe [2019] UKSC 50, which involved a claim brought by the Cayman Islands court-appointed liquidators of one of the companies in the Saad group, against the London subsidiary of the Japanese investment bank and broker Daiwa, the UK Supreme Court examined this duty. In that case, Daiwa had been instructed to execute transfers by the main protagonist, Maan Al Sanea, from Singularis' account to other entities.

The appointed liquidators investigated and decided to bring claims against Daiwa for breach of the Quincecare duty of care, arguing that, in that case, Daiwa should not have effected the transfers. Despite the fact that Daiwa had mounted an illegality defence, the Supreme Court nevertheless found that a negligence claim against Daiwa should be allowed. Part of the Supreme Court's reasoning was that otherwise this would undermine the public interest aspect that requires banks to play an active role in preventing financial crime. Further, as a matter of causation, the Supreme Court found that the fraudulent instruction from Al Sanea to Daiwa gave rise to Daiwa's duty of care, Daiwa breached this duty, and there was in fact causation that was made out.

What this case illustrates is that banks involved in handling wrongly obtained assets could also potentially be responsible for a much broader range of activity. Where cases involve Caribbean elements, such as in this case where the claim was brought by Cayman Islands court appointed liquidators, they will not shy away from using the full range of tools in their possession to seek accountability and responsibility when assets are lost.

Mareva Injunction

Overview

Mareva or freezing orders are some of the most frequently sought orders, both for proceedings in the Caribbean jurisdictions and in aid of foreign proceedings. As well as the standard freezing orders against the respondent, freezing orders may also be available against third parties in certain circumstances, if it can be demonstrated that there is a good arguable case that the third party holds assets belonging to the respondent. In the Cayman Islands, for example, such freezing orders can be granted against third parties in the Cayman Islands, or against third parties (whether or not based in the Cayman Islands) which have assets in the jurisdictions.

Mareva or freezing orders are some of the most frequently sought orders, both for proceedings in the Caribbean jurisdictions and in aid of foreign proceedings.

Broad Idea International Limited v Convoy Collateral Limited

In terms of recent case developments regarding freezing injunctions, perhaps one of the most notable developments has been the Black Swan saga in the British Virgin Islands. In its May 2020 decision in Broad Idea International Limited v Convoy Collateral Limited No 2 (BVICMAP 2019/0026), the Eastern Caribbean Court of Appeal held (overturning Black Swan jurisdiction, named after the case in which Justice Bannister applied the dissenting judgment of Lord Nicholls in Mercedes Benz AG v Leiduck [1996] 1 AC 284 and ruled that the BVI Court was not bound by the majority decision in that case) that the BVI Court was bound by the majority decision in Mercedes Benz. Consequently, it found that there was no common law jurisdiction to grant a free-standing freezing injunction against a respondent which was not a party to substantive proceedings in the BVI.

This decision appeared to pose a significant obstacle to those seeking freezing injunctions to preserve assets and prevent dissipation. Interestingly, the Eastern Caribbean Court of Appeal decision hinged itself on a decision from the House of Lords that stemmed from a much earlier period of judicial development, when issues of jurisdiction and global commercial interests were comparatively less developed.

The Court of Appeal realised that the first instance court's decision would not be beneficial for the BVI looking to strengthen its position as an international financial hub. Hence, in deciding the case, the Court of Appeal suggested that there should be consideration of intervention by legislation to address the situation. Legislation did in fact follow swiftly, with the Eastern Caribbean Supreme Court (Virgin Islands) (Amendment) Act taking effect in January 2021. The newly inserted section 24A of the Eastern Caribbean Supreme Court (Virgin Islands) Act provides statutory jurisdiction to grant interim relief where proceedings have been or are about to be commenced in a foreign jurisdiction, and allows the court to grant any relief which may be granted in relation to matters within the BVI Court's jurisdiction (including freezing injunctions and receivership appointments). It also expressly gives the Court power to grant relief against non-cause of action (or 'Chabra') defendants.

Subsequent to that, as a cherry on top, in October 2021, the Privy Council handed down its much anticipated judgment in Broad Idea International Ltd (Respondent) v Convoy Collateral Ltd (Appellant) (British Virgin Islands) Convoy Collateral Ltd (Appellant) v Cho Kwai Chee (also known as Cho Kwai Chee Roy) (Respondent) (British Virgin Islands) [2021] UKPC 24. By a 4:3 majority, the Privy Council held that: (1) Black Swan jurisdiction should be upheld. It decided that the original (obiter) judgment by Bannister J in 2010 had been a vital tool in aid of judgment and award enforcement in the BVI, permitting freezing injunctions against BVI respondents to foreign proceedings in aid of potential future enforcement; and (2) on the rules and law as it then was, the Court did not have jurisdiction to grant service out of a claim seeking only a freezing injunction.

The analysis by the Privy Council highlighted the tension between two lines of authority: one from the decision

of the House of Lords in The Siskina [1979] AC 210, which suggested that a freezing injunction could be granted only where substantive proceedings were extant in the same jurisdiction; the other was from the decision of Bannister J in *Black Swan*, which suggested that a freezing order could be granted in aid of foreign proceedings.

The Board unanimously dismissed the appellant's appeals, although there was a 4:3 divide on one aspect. The majority judgment given by Lord Leggatt (with whom Lord Briggs, Lord Sale and Lord Hamblen agreed) concluded that where a court has a personal jurisdiction over a party, the court has power and in fact can exercise that power to grant a freezing injunction against that party to assist enforcement through the court's process of a prospective or existing foreign judgment. The majority reasoned that Bannister J in Black Swan had been correct and that its decision should not have been overturned. However, it held that the Eastern Caribbean Court of Appeal had been right to set aside the freezing injunction granted against Broad Idea on the facts of the case and was also right to conclude that the BVI court had no personal jurisdiction over Dr Cho, since there was no power in the Eastern Caribbean Civil Procedure Rules that gave permission to serve out of the jurisdiction proceedings which seek only an interim freezing injunction.

The minority (Sir Geoffrey Vos, Lord Reed and Lord Hodge) felt that they should not decide whether there is a power for the court to grant a freezing injunction against a defendant in aid of foreign proceedings when no substantive claim was made in proceedings before the domestic court. However, overall the Privy Council decision endorsed the decision of Bannister J in the Black Swan, rather than the reasoning of Lord Diplock in The Siskina.

A further important principle to derive from this decision is that a freezing injunction operates to support enforcement of judgments and not (exclusively) to support the bringing of substantive claims within the jurisdiction. This explains expansions in the jurisdiction such as the granting of post-judgment freezing injunctions and so-called Chabra injunctions (following TSB Private Bank International SA v Chabra).

The Road Ahead

What we can see from an analysis of recent case law in the Caribbean jurisdictions is that these jurisdictions have taken the classic tools of ATR and have strengthened and clarified their usage through detailed judicial development and refinement. Further, in many cases, particularly in the BVI, these jurisdictions have also taken to statute to enshrine the flexibility and availability of these tools by way of legislation, as a further way to bolster their effectiveness.

This is particularly useful for cross-border ATR, such as where there are foreign proceedings in an Asian jurisdiction or the parties are located elsewhere than in the Cayman Islands, BVI or Bermuda. It is worth remembering that often an applicant trying to trace and recover its assets will seek from the offshore Courts more than one type of order, such that these orders can be used in combination with each other, to obtain the maximum effect and assist in other jurisdictions.

As the cases examined in this article have demonstrated, parties do increasingly fully utilise these ATR tools, and it is clear that one of the key strengths of these Caribbean jurisdictions of the Cayman Islands, BVI and Bermuda is that they are often pragmatic and realistic in their approach, meaning that they will develop case law in a way that remains friendly to those seeking to use these. Decisions such as the Privy Council decision of Broad Idea v Convoy show that the Courts have further galvanised these jurisdictions as the upholders of legal remedies being flexible, reactive and widely available.

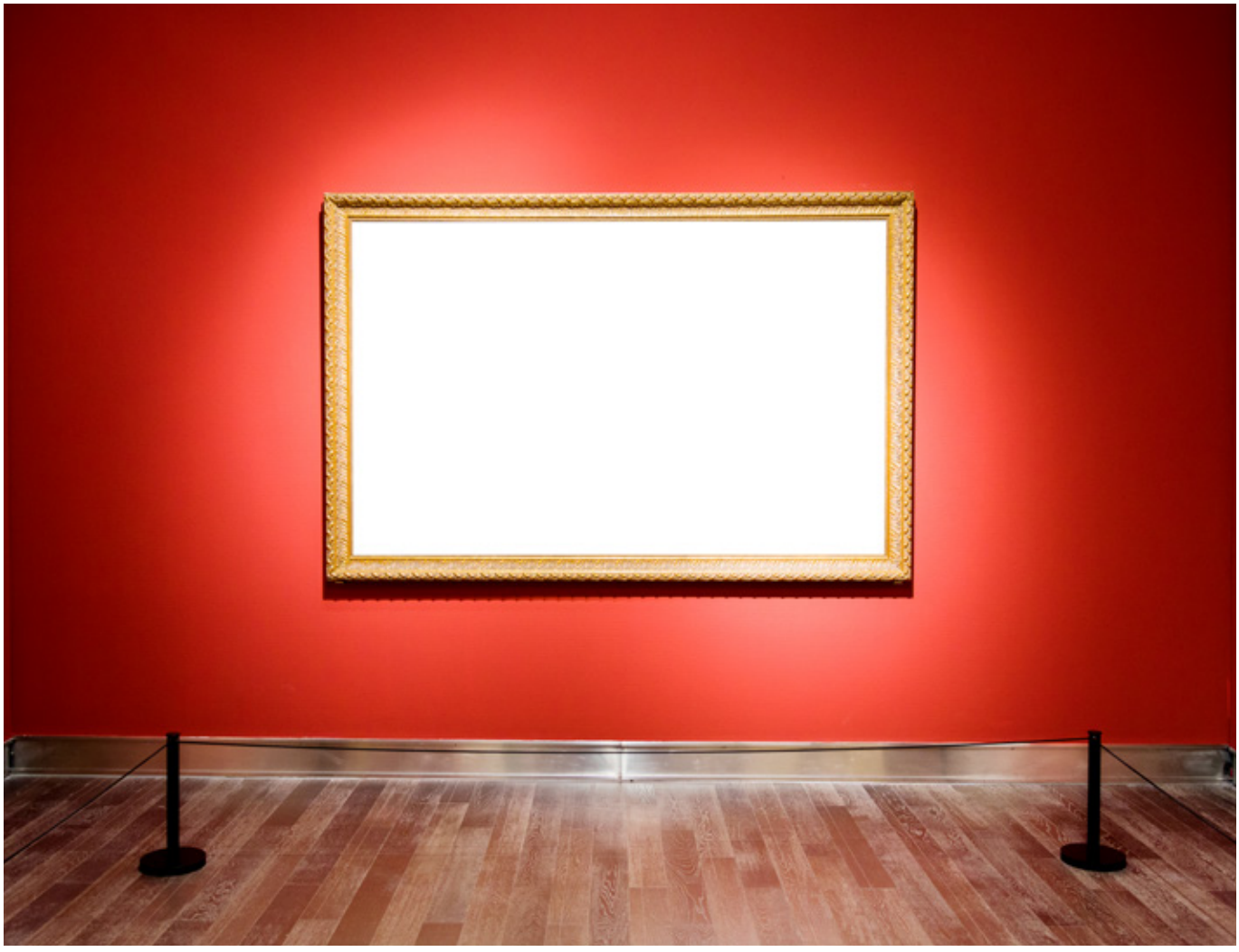
We expect that this trend will continue into the future and that we will see further interesting developments in this area of law, which will no doubt benefit those who look to use these tools and remedies in complex situations of ATR. Long gone are the days when discovering the assets had moved was the unwelcome end of a case; it is now the beginning of the ATR phase and there is a powerful toolkit available offshore.

Jeremy Lightfoot
Partner, Carey Olsen Hong Kong LLP, Hong Kong

Jeremy leads offshore law firm Carey Olsen's litigation practice in Hong Kong. His practice is focused on high value and complex commercial and corporate litigation, insolvency and restructuring matters under the laws of Bermuda, the BVI and the Cayman Islands.

Cross-Border Fraud in Art: Lessons From a Dutch Perspective

Cybercrime is pervasive across all industries; however, the art world has repeatedly become a victim of this type of fraud. As an industry that comprises businesses ranging in scale and size, often lacking robust security measures yet transacting large sums of money, the art world has become a prime target for fraudsters.



Introduction

'Art crime' is a phrase that will likely prompt thoughts of the film *The Thomas Crown Affair*, recent acts of vandalism, or perhaps even tales of fakes and forgeries. While these examples can and do illustrate the intersection between art and law, cybercrime may also claim a place on that list.

One only needs to consider the rapid changes in ways of working over the past few years to appreciate how and why cybercrime is at an all-time high. This article will seek to examine the main cross-border fraud and cybercrime-related laws and regulations that apply in the Netherlands. Frequent reference will be made to a recent high-profile case involving the Netherlands, the United Kingdom and Hong Kong, in order to contextualise the often intangible nature of this type of crime. Despite the case being heard in the United Kingdom, it will provide a platform for exploring the Netherlands' legislation relevant to a crime of this nature.

Rijksmuseum Twenthe v Simon C Dickinson Ltd

A 2018 deal between a Dutch museum and a London art dealer sets the scene for an exploration of cross-border fraud, specifically, cybercrime within the art world. At the time, the Rijksmuseum Twenthe in Enschede, the Netherlands (the 'Museum'), was engaged in lengthy negotiations with London art Dealer Simon C Dickinson (the 'Dealer') to purchase a painting by John Constable. The painting, *A View of Hampstead Heath: Child's Hill, Harrow in the Distance* (1824), was to be sold for a sum of GB£2.4 million. During negotiations, emails between the two parties were intercepted by cybercriminals, in other words, hackers. The hackers specifically intercepted communications between the two parties containing bank details, replacing them so that when the Museum paid the purchase price of almost GB£2.5 million, the Dealer received nothing. On successfully intercepting communications, the hackers had posed as the Dealer, substituting the legitimate payment details provided to the Museum for those of a fraudulent Hong Kong-based bank account. This technique used by the hackers to intercept correspondence between the parties and substitute the correct back details for fraudulent ones is known as phishing.

It remains unclear whether the hackers infiltrated the Museum's or the Dealer's system, with each side claiming that the other had been hacked, and it is worth noting that a subsequent police investigation into the Hong Kong-based account failed to identify the hackers responsible for the fraud. Once the Museum became aware that it had unwittingly paid the purchase price for the painting into a Hong Kong-based bank account, it issued a claim against the Dealer. The Museum brought the claim against Dickinson in the High Court of England and Wales (Commercial Court) (note that future references to this case will be made as Rijksmuseum Twenthe v Dickinson).

A legal battle between the parties ensued, with the basis of the Museum's claim being that the Dealer had been negligent in protecting communications between the parties from interception. It must be acknowledged that while the Dealer did in fact owe a duty of care to the Museum, conversely, the Museum also owed a duty of care to the Dealer. As noted above, and expectedly so, each party blamed the other for the transgression. Despite a lack of evidence as to which system was infiltrated, each system was found to have flaws. Judge Pelling dismissed the Museum's claim for negligence, holding that the Museum owed its own duty of care to maintain reasonable cybersecurity and was equally responsible for determining the destination of the funds. The Museum was granted the right to amend its claim and went on to pursue an alternative claim for damages, discussed below.

Key Terminology

At this point, expanding on some of the key terminology used within cybercrime may be useful. Cross-border fraud refers quite generally to any scam or fraud in which a criminal in one country uses deception to steal money or valuables from a victim in another country, which may be considered cross-border fraud. The transnational nature, combined with the victimisation of others resulting in loss of value, are critical elements of this crime. Historically, cross-border fraud would likely have been perpetrated through mail, phone, fax or ads in newspapers and magazines. However, with the advent of the internet and email, social media and online banking, it has become easier for fraudsters to carry out their criminal activity on a global scale.

Cybercrime is the use of a computer to carry out criminal activity. The varying types of cybercrime is an extensive list and can include anything from email and internet fraud, ransomware attacks, system interference, theft of financial data, infringing copyright to selling illegal items online. Though the term 'hacking'

is widely understood, it lacks a universally accepted definition. It generally refers to unauthorised access to a computer network system or individual computer for personal gain, be that theft, destruction of files or unlawful review of data. While not always a malicious activity, it is the lack of consent and personal gain involved that lends hacking its status as a crime.

Lastly, phishing, the technique carried out by the hackers in Rijksmuseum Twenthe v Dickinson, is a type of cybersecurity attack where cybercriminals send messages pretending to be a trusted person or entity, often used to trick victims into revealing sensitive information or installing malware.

What are the Main Cross-Border Fraud/ Cybercrime-Related Laws and Regulations that Apply in the Netherlands?

Any discussion around the legislative framework for combating cross-border fraud or cybercrime in the Netherlands must first make reference to The Council of Europe's Cybercrime Convention (the 'Cybercrime Convention');[1] a landmark effort to harmonise national criminal law in the area of cybercrime. Although the Cybercrime Convention provides extensive substantive, procedural and mutual assistance provisions, it naturally allows for reservations and variations when it comes to implementation by the various member states.[2] This has the ability to result in cross-jurisdictional inconsistencies, and as such, the laws and regulations in place might therefore be more accurately described as a 'patchwork' system consisting of national implementation of various international legal instruments. Regardless, it is the starting point for developing an understanding of Dutch cybercrime legislation.

In the Netherlands, criminal law is codified in the Dutch Criminal Code or Wetboek van Strafrecht ('DCC') and the Dutch Code of Criminal Procedure or Wetboek van Strafvordering ('DCCP'), with the majority of cybercrimes provided for in the Second Book DCC.[3] Various offences will be detailed below, each carrying a maximum penalty. The DCC does not provide for minimum penalties and the right to exercise prosecutorial discretion is an important feature of Dutch criminal law. This can mean that, on occasion, some acts that may fall within the broad criminal provisions of the DCC may not be deemed worthy of criminal prosecution. An example of this may be the changing of a single bit of data on a computer without authorisation, an offence that is provided for under article 250a of the DCC, but one that would not ordinarily be prosecuted.

The most important cybercrime laws in the Netherlands are the Computer Crime Act (Wet computercriminaliteit) 1993 and the Computer Crime II Act (Wet computercriminaliteit II) of 2006. These are the laws that have adapted the DCC and the DCCP. The Cybercrime Convention was accepted concurrently with the Computer Crime II Act, coming into force in the Netherlands on 1 March 2007. With the full extent of cybercrime-related offences able to be located in the DCC, we have opted to focus this discussion primarily on hacking and data interference, given their relevance to issues contained in Rijksmuseum Twenthe v Dickinson.

In addition to the terminology defined above, the definition of both 'data' and 'computer' are essential to the application of the articles addressed below. The DCC defines data as 'any representation of facts, concepts, or instructions, in an agreed-upon way, which is suitable for transfer, interpretation or processing by persons or automated works'[4] and defines computer as 'a construction designed to store, process, and transfer data by electronic means'.[5]

Hacking is the intentional and unlawful entry into a computer or a part thereof and is penalised under article 138a DCC. Hacking carries a maximum penalty of one year imprisonment for 'simple' hacking, and four years imprisonment if the hacker copies data after entry. Data interference is penalised under article 350a DCC. Considered to be the intentional or unlawful deleting, damaging or changing of data it carries a maximum penalty of two years imprisonment. It is this offence that may invoke prosecutorial discretion as mentioned above, with minor cases unlikely to be prosecuted. However, if the interference was committed through hacking and resulted in serious damage, the maximum penalty is four years imprisonment.

At this juncture it is appropriate to return to the facts of Rijksmuseum Twenthe v Dickinson. The cybercriminals responsible for the misdirection of funds from the Museum to the Hong Kong bank account intentionally and unlawfully entered into a computer and, despite

contention over which 'side' had been hacked, if this were to be considered under the DCC, the offence of hacking would have been committed under article 138a of the DCC. However, the offence in this case goes further than this, as the hackers proceeded to interfere with data by substituting legitimate payment details for those of the fraudulent Hong Kong-based bank account, an offence constituting interference with data under article 350a of the DCC. Given the purchase price of the painting and the impact of the hacking and subsequent interference on the parties to the case (that is, serious damage), and in accordance with the extended penalty available under article 350a of the DCC, in the Netherlands the hackers could be punishable by up to four years imprisonment.

The DCC does not provide for minimum penalties and the right to exercise prosecutorial discretion is an important feature of Dutch criminal law.

It is interesting to consider the development of the law surrounding hacking over time within the Netherlands. In 1993, hacking was punishable only in the event that a security measure was breached. This was cause for debate in the lead up to The Computer Crime Act, with the key question being what level of security should be required. It was found that a minimal level of protection was adequate. However, in 2006 this requirement for a minimum level of security was done away with. The justification for this was the Cybercrime Convention, which allowed countries to implement a requirement of infringing security measures, but not one for other types of deviance, a stolen password for example. It follows that, even if the Museum's security systems were found to be lacking, the cybercriminals would still be punishable under article 138a of the DCC.

In addition to the Cybercrime Convention, a number of other instruments exist to facilitate harmony across Europe and beyond when it comes to specific aspects of cybercrime. These include EU Framework Decisions and EC Directives and it is generally considered that the Netherlands has effectively implemented such instruments. However, the challenge with cross-border fraud is the very cross-jurisdictional nature of it. The discrepancies in implementation across jurisdictions has a direct impact on the intended harmonisation, as well as subsequent uncertainty on national standards when mutual legal assistance is being sought.

Who is Ultimately Held Responsible for Cross-Border Fraud Involving a Diverted Payment?

As in Rijksmuseum Twenthe v Dickinson, cross-border fraud often involves a contract where one party is required to pay another, with the issue arising when a cybercriminal (by any variety of means) manipulates the buyer into paying the criminal instead of the seller. Under these circumstances, a number of options are available to the parties. Sometimes, they may have commercial insurance in place, or alternatively, they may pursue legal action. A disagreement typically arises between the two parties as to who is at fault and who will suffer the loss. For example, in Rijksmuseum Twenthe v Dickinson, is it the Museum that should be required to make payment to the Dealer twice or should the Dealer have to forgo payment for the sale of the painting? The question that will usually arise next is whether it matters that one of the parties was hacked. Typically, as was the case in Rijksmuseum Twenthe v Dickinson, each party will claim that the other was responsible for the fraud due to inadequate cybersecurity. However, this is difficult to prove and, under the DCC, largely irrelevant.

In 2020, the director of the Museum stated that 'investigations have shown that our email systems had no vulnerabilities, that they were up-to-date and in order. We ultimately took the dealer to court to make it clear that this painting was bought and paid for'.[6] As stated earlier, the Dealer also maintained that its security systems were in order and the Museum's initial claim for negligence was dismissed. The Museum went on to claim that negotiators for the Dealer had been included on several of the hacked email chains and should have alerted the Museum to the fraud. The Museum argued that upon discovery of the fraudulent email activity and failing to notify the Museum, the Dealer was implicitly representing that the email correspondence was genuine. However, the Museum was unable to prove knowledge on the Dealer's behalf and the argument failed.

At the time of payment from the Museum to the fraudulent bank account, the Museum was in possession of the painting. According to the director of the Museum, this was not unusual, in large part due

to fundraising reasons. As a result, the Dealer, who was attempting to take possession of the painting that they had not received payment for, was prevented from trying to resell it. At present, the painting remains on display in the Museum and the Dutch government has subsequently provided the Museum with a €2.5 million subsidy to enable it to settle the dispute and acquire the painting which, as stated, is already on display at the Museum.

How Can Lawyers Help Clients to Identify, Stop and Bring Effective Enforcement Actions Against Cross-Border Fraudsters?

According to the 2022 Hiscox Online Art Trade Report, 71 per cent of art buyers said that cybercrime was a worry to them in the online art market, up from 63 per cent in 2020.[7] Maureen Bray, executive director of the Art Dealers Association of America ('ADAA'), reinforced these concerns, noting that 'cybersecurity is a pressing concern for galleries, collectors, and artists alike'. Despite the very real concern among the art world, it is unrealistic for legal professionals to assume all clients within the sector will be willing to invest the resources required to mitigate potential threats. However, it remains necessary to educate clients about technologies available to them and encourage the implementation of measures such as two-factor authentication, vetting of suspicious emails and protecting login credentials. In the event that no such factors are employed by clients for any number of reasons (for example, time or cost), it is highly encouraged that, much like it is standard practice within the legal profession, confirmation of account numbers is carried out either over the phone or face-to-face prior to payment. This relatively simple, expedient and cost-free step could have circumvented the issue between the Museum and the Dealer in Rijksmuseum Twenthe v Dickinson; protecting the Museum from having its funds stolen and the Dealer from facing legal action.

It is not uncommon for actors within the art world to conduct large-sum business transactions and the likelihood of such transactions taking place remotely is ever increasing. Rijksmuseum Twenthe v Dickinson is not a standalone case. In 2017, a similar fraud forced Laura Bartlett Gallery to close, and in 2022, Italian gallery T293 was targeted by hackers, who manipulated a purchaser into transacting US$30,000 into their bank account instead of the gallery's. The art world has traditionally been a community built on trust, with a predisposition for handshake deals at art fairs and limited involvement from lawyers or financial advisers and the like. This idealistic approach to conducting business within the art world is no longer workable. When carrying out business, particularly online, galleries, museums, dealers, collectors and artists alike must remain vigilant for fraudsters seeking to deceive and while Rijksmuseum Twenthe v Dickinson presents a valuable warning for the art world specifically, it is one that should be heeded by all.

Notes

[1] The Council of Europe's Convention on Cybercrime was opened for signature on 23 November 2001. The Convention is the first international treaty designed to address several categories of crimes committed via the Internet and other computer networks.
[2] The Council of Europe has 46 members, including all 25 members of the European Union and seeks to promote and protect human rights and the rule of law throughout Europe.
[3] In Dutch criminal law, substantive law distinguishes between crimes (Second Book DCC), to which almost all cybercrimes belong, and misdemeanors (Third Book DCC).
[4] Article 80 quinquies DCC.
[5] Article 80 sexies DCC.
[6] Arnoud Odding, director of the Rijksmuseum Twenthe, became interested in the painting in question at TEFAF in Maastricht, 2018.
[7] The Hiscox Online Art Trade Report addresses trends in online sales of art, and focuses on the US and European markets.

Laurens Kasteleijn
Managing Director, Art Law Services, Amsterdam

Laurens founded Art Law Services in Hong Kong over a decade ago, expanding to Amsterdam in early 2020. As a former art gallery director and corporate M&A lawyer, Laurens advises and represents the whole array of participants in the international art world, with a particular focus on legal issues related to fine art and other creative industries.

The author would like to thank Lucy Grenfell for her assistance with this article.

Legal Analysis of Cross-Border Fraud: From the Perspective of Chinese Securities Regulations

With the rapid development of the internet, cross-border securities fraud has become more frequent, and many investors have suffered losses. This paper analyses the current situation of securities cross-border fraud in China, the laws and regulations therein, and other aspects, combined with cases in order to give readers an understanding of the Chinese legal system in this regard, and to enable readers to know how to avoid such fraud.

The Current Situation in China Regarding Cross-Border Securities Fraud

Due to the development of economic globalisation and the progress of network technology, the trend of internationalisation of financial markets has a significant impact on the supervision of the world's financial markets. Financial transactions and the accompanying illegal acts have transnational attributes or foreign-related factors, which bring certain challenges to traditional financial supervision.

On 30 December 2022, the China Securities Regulatory Commission ('CSRC') issued a document saying that in recent years, FUTU and UP Fintech Holding Limited had not been approved to carry out cross-border securities business for domestic investors in accordance with relevant laws and regulations such as the Securities Law and the Regulations on the Supervision and Administration of Securities Companies. Its behaviour has constituted an illegal operation of securities business. On 11 November 2021, the CSRC conducted regulatory interviews with senior executives of FUTU and UP Fintech Holding Limited, clarifying their regulatory attitude and requiring them to regulate cross-border securities business for domestic investors in accordance with the law.

The attitude of the CSRC towards the discovery of cross-border securities fraud is firm. One is to ban incremental illegal business activities according to law. It is prohibited to solicit domestic investors, develop new domestic customers and open new accounts. Second, properly handle the stock business: in order to maintain the stability of the market, domestic investors in stock are allowed to continue trading through the original foreign institutions, but foreign institutions are prohibited from accepting incremental funds in violation of China's foreign exchange regulations into the accounts of such investors. Any entity shall engage in cross-border securities business for domestic investors in China in accordance with the law and regulations.

Legal Regulation of Cross-Border Securities Fraud

Article 2 of China's first Securities Law in 1999 stipulates that 'this Law shall apply to the issuance and trading of stocks, corporate bonds and other securities recognized by the State Council according to law within the territory of China' and the effectiveness of China's Securities Law is strictly limited to the territory of China. However, Article 2 of the Securities Law of the People's Republic of China, which came into effect on 1 March 2020, stipulates that the issuance and trading of securities outside the territory of the People's Republic of China, which disrupts the market order within the territory of the People's Republic of China and damages the legitimate rights and interests of domestic investors, shall be dealt with in accordance with the relevant provisions of this Law and shall be investigated for legal liability. In accordance with the provisions of the above-mentioned Securities Law, the securities regulatory authorities and judicial authorities in China can exercise jurisdiction over them.

Article 219 of the Securities Law stipulates: 'Where a violation of the provisions of this Law constitutes a crime, criminal liability shall be investigated in accordance with the law'. The PRC securities regulatory authorities have the right to exercise administrative jurisdiction over fraudulent acts that disrupt the market order in the People's Republic of China or damage the legitimate rights and interests of Chinese nationals or investors in the People's Republic of China and the PRC judicial authorities also have the right to impose criminal liability on suspected entities and specific individuals in accordance with the law.

For the first time, the new Securities Law in 2020 established the 'effect principle' of the extraterritorial effect of Chinese securities law, stipulating in Article 2 that 'the issuance and trading of securities outside the People's Republic of China, which disrupts the market order within the People's Republic of China and damages the legitimate rights and interests of domestic investors, shall be dealt with and investigated for legal liability in accordance with the relevant provisions of this Law'.

It can be seen that China has made a useful attempt on the extraterritorial jurisdiction of the Securities Law and adopted the 'effect principle' to initially construct the extraterritorial jurisdiction system of the Securities Law. China's 'effect principle' also reflects the balance between the protection of public interests and the protection of private interests in the securities law as a 'public law' attribute, that is, the 'effect' of overseas acts on China is either the public interest that affects the 'order of China's market' or the private interest that 'damages the domestic investors'. Of course, the protection of investors is more a reflection of the public purpose of the implementation of securities law than the protection of all relevant private interests by securities law.

Article 95 of the Regulations on the Supervision and Administration of Securities Companies (Revised in 2014) specifies that where an overseas securities business institution operates securities business or establishes a representative office in China, it shall be approved by the securities regulatory authority under the State Council. On this basis, the Securities Brokerage Business Management Measures recently issued by the Securities Regulatory Commission (implemented on 28 February 2023) have further refined and supplemented the supervision of cross-border securities business. According to Article 46 of the Measures for the Administration of Securities Brokerage Business, if an overseas securities operating institution violates Article 95 of the Regulations on the Supervision and Administration of Securities Companies and directly or through its affiliated institutions or cooperative institutions carries out marketing and account opening activities of overseas securities trading services in China, it shall be punished in accordance with Article 202 of the Securities Law. The above provisions provide a law enforcement basis for the CSRC to crack down on the illegal cross-border brokerage business of overseas securities business institutions.

Practical Countermeasures and Case Analysis for Cross-Border Securities Fraud

Article 2 of the Provisions of the Supreme People's Court on the Jurisdiction of Cases of Beijing Financial Court and Article 2 of the Provisions of the Supreme People's Court on the Jurisdiction of Cases of Shanghai Financial Court stipulate that the two financial courts in Beijing and Shanghai shall have jurisdiction over domestic companies listed outside China and overseas companies that damage the legitimate rights and interests of domestic investors. The Articles also stipulate that the two financial courts shall have jurisdiction over financial disputes in which the providers of other overseas financial products and financial services damage the legitimate rights and interests of domestic investors. The court of jurisdiction for cross-border securities fraud has made clear provisions.

The CSRC and the Hong Kong Securities and Futures Commission (SFC) approved the Shanghai-Hong Kong Stock Connect in 2014 and the Shenzhen-Hong Kong Stock Connect in 2016. On 19 December 2022, the CSRC and SFC issued a joint announcement that, in order to further deepen the interconnection mechanism between the mainland and Hong Kong stock markets and promote the common development of the two capital markets, the CSRC and SFC agreed in principle to further expand the scope of stock interconnection between the two exchanges. Therefore, domestic investors can invest in the Hong Kong securities market through Hong Kong Stock Connect and trade specific stocks listed on the Hong Kong Stock Exchange. Investing in overseas securities through legal channels is the right way for investors to avoid fraud.

The strengthening of the education and guidance of investors on cross-border securities fraud is another measure. For instance, they should not trust foreign securities transactions easily. Also, domestic investors

Publications Committee Guidelines for Publication of Articles in the IPBA Journal

We are pleased to accept articles on interesting legal topics and new legal developments that are happening in your jurisdiction. From time to time, issues of the Journal will be themed. Please send: (1) your article to both **James Jung** at jjung@collaw.edu.au and **Olivia Kung** at olivia.kung@wellingtonlegal.com.hk; (2) a lead paragraph of approximately 50 or 60 words, giving a brief introduction to, or an overview of the article's main theme; (3) a photo with the following specifications (File Format: JPG or TIFF, Resolution: 300dpi and Dimensions: 4cm(w) x 5cm(h)); and (4) your biography of approximately 30 to 50 words.

The requirements for publication of an article in the *IPBA Journal* are as follows:

1. The article has not been previously published in any journal or publication;
2. The article is of good quality both in terms of technical input and topical interest for IPBA members;
3. The article is not written to publicise the expertise, specialization, or network offices of the writer or the firm at which the writer is based;
4. The article is concise (2500 to 3000 words) and, in any event, does not exceed 3000 words;
5. The article must be written in English (with British English spelling), and the author must ensure that it meets international business standards;
6. The article is written by an IPBA member. Co-authors must also be IPBA members; and
7. Contributors must agree to and abide by the copyright guidelines of the IPBA. These include, but are not limited to
   a. An author may provide a link on the website of his/her firm or his/her personal website/ social media page to the page of the Journal on which the first page of his/her article appears; and
   b. An author may not post on any site an entire PDF of the Journal in which the article authored by him/her appears.

participate in overseas securities market transactions through the platform website or mobile client of domestic internet companies, because there is no corresponding legal protection and as securities investment accounts and funds are overseas, once disputes occur, investors' rights and interests will not be effectively protected. Some overseas securities business institutions cooperate with domestic internet companies to provide trading channels and services for domestic investors to invest in overseas securities markets through the platform websites or mobile clients of domestic internet companies. Domestic trading venues and other institutions should strengthen all-round guidance to investors, give early warning of relevant events and combine this with investor education.

Recently, there have been cases of suspected cross-border fraud. In 2022, some so-called intermediaries held press conferences, promotion meetings, forums and other activities in Hainan, Guangxi and other places, declaring that the Mozambique International Stock Exchange has set up a representative office in China and obtained authorisation from overseas securities companies to sponsor companies to list on overseas exchanges such as the Mozambique International Stock Exchange. Such so-called intermediaries may issue a Letter of Recommendation and Letter of Acceptance for the listing. There were also some companies that issued press releases, WeChat articles or held offline meetings, claiming that they have been approved by the Mozambique International Stock Exchange and will be listed on the main board. The scheme was that major shareholders would transfer the original shares for financing or claim to give them back to customers. Customers who bought products could get points that could be converted into original shares. Once the company is listed, they would get high returns. According to the relevant provisions of Chinese national laws and regulations, it is illegal to issue or transfer shares to the domestic public without legal registration and the relevant companies and their major shareholders are suspected of illegal issuance of shares by publicly issuing or transferring original shares in China. The above-mentioned intermediaries, which use overseas listing as a gimmick to promote and induce the public to buy original shares, are suspected of illegally operating securities business or fraudulent activities. The CSRC also warned the companies concerned and their major shareholders that they would bear legal responsibility for selling original shares to the domestic public and that the domestic representative offices of the Mozambique International Stock Exchange should not trust illegal intermediaries without the filing of the CSRC. At the same time, it reminds investors to stay away from illegal issuance or transfer of 'original shares' in order to avoid property losses and to report to the public security organs in time once they are found to have been deceived.

Conclusion

China has perfect laws and regulations on cross-border securities fraud, and investors should remain vigilant and not be confused by seductive propaganda. When encountering possible cross-border fraud, they should consult and report it to the regulatory authorities in a timely manner. When they are subject to cross-border securities fraud, they should take up the weapon of laws and actively safeguard their rights and interests.

Jack Li (Li Zhiqiang)
Founding Partner, Jin Mao Partners, Shanghai

Jack Li is the Founding Partner of Jin Mao Partners and was the 30th President of the Inter-Pacific Bar Association. He has served as a legal consultant for more than 300 Chinese and foreign enterprises for restructuring and mergers and acquisitions, financing, IPO and for the Office Building project of the Shanghai Government. Jack was the 8th Shanghai Top Ten Outstanding Youth in 2001 and has been the chief editor for more than 30 legal books.

Scott Li (Li Jian)
Lawyer, JMKD Lingang Law Office, Shanghai

Scott Li has handled a number of major litigation and arbitration cases, many of which were disputes over the repurchase of pledged shares of listed companies. His professional works were published in the first batch of Class A academic journals in China such as the 8th issue of Financial Market Research in 2018.

James Yang (Yang Zian)
Partner, Jin Mao Partners, Shanghai

James Yang has comprehensive experience in legal practice including IPO, bond issuance, commercial disputes and company consultation. James also assists in translation and analysis of various foreign law rules, transaction documents and articles.

International Fraud in Current Russian Realities

Globalisation and digitalisation make business processes easier and a provide level playing field for everyone, especially for emerging nations. At the same time, these trends create new opportunities for criminals, who employ technological developments in their favour. Russia is one of the countries to have faced the growth of international fraud and crimes using new technologies which have created a number of problems for the Russian authorities.

In recent years, cross-border crime has increased worldwide. The contributing factors are well known and include development of digital technologies and the convenience of cross-border communication. Thus, in many cases, cross-border fraud means cyberfraud or fraud committed by means of digital communications.

This tendency is well demonstrated by the exponential increase in spending on cyber security, which is expected to comprise up to US$10.5 billion in 2025. Russian authorities registered an upsurge of cybercrime up to 80 per cent in 2022 as compared to 2021. The majority of these crimes were committed from abroad.

A substantial part of cross-border crimes is accounted for by fraud offences. In the Russian legal system, 'fraud' is defined as the stealing of other people's property or acquisition of the right to other people's property by deception or breach of trust.

This tendency is relevant both for actions committed on Russian soil against foreigners and for crimes committed from abroad. However, modern technologies (for instance, VPN connections) often make it impossible to pinpoint the exact location of a fraudster. Therefore, some crimes that appear to be cross-border may actually be committed by local citizens adept at using modern technologies.

For instance, a substantial number of frauds were committed by making calls from fake phone numbers (so called 'substitutive phone numbers'). A caller may cause any phone number to appear on a victim's phone screen (for example, a phone number of a bank or any other organisation). The purpose of this is to persuade a victim that the call is being made by a representative of their bank or even a police officer who is trying to prevent the stealing of the victim's assets. The aim of the fraudster is to receive personal information of the victim, including the CVV code of their credit card.

The number of such incidents motivated some Russian banks to create an antifraud system that operates in several CIS countries. Banks often encounter malicious and phishing mailings directed not only to depositors, but also to bank employees. It was reported that the system has helped to save billions of rubles from being stolen.

Such attacks and calls may be performed by individuals regardless of their location. In 2021 in Russia, more than

500,000 crimes were registered and committed with the use of information and telecommunication technologies or in the field of computer information.[1]

The employment of modern technologies in cross-border crimes makes it necessary for a lawyer to engage digital specialists for facilitating the process of gathering evidence of the deed. It becomes a general rule for law firms to carry out internal investigations of incidents jointly with IT specialists. This practice demonstrates high efficiency. For instance, in a series of internal investigations conducted regarding an alleged fraud, our team were able to obtain electronic correspondence with foreign entities that became a crucial piece of evidence.

Another important aspect of work that may be subcontracted to IT specialists is searching for digital traces of an offender. The personality of a cross-border culprit is intentionally hidden. Therefore, open sources of intelligence may discover a variety of vicarious evidence sufficient to establish the identity of the criminal. For instance, methods of intelligence helped our team to determine the name and location of a person involved in the theft of cryptocurrency from a foreign company. This information was necessary for preparing a criminal complaint.

The important role of digital evidence is recognised also by the state authorities which actively employ such specialists in investigations starting from the initial stages. For example, getting copies of all digital devices became a standard for every economic criminal case. They yield an abundance of information, even that which was deleted by the user.

Also frequent in Russia are cases where the assets of Russian companies are alienated on the basis of falsified evidence provided to Russian courts. This can be done by way of a corporate takeover of the company or establishment of a debt in the Russian courts. Despite the fact that the official court databases are mostly open to the public, in many cases the fraudsters exploit the efficiency of the Russian court procedure and the huge workload of Russian judges, obtaining judgments in the Russian courts in the absence of the defendant in two to three months and subsequently foreclosing on the assets of the company. The Russian courts are trying to fight such types of fraud. Recently the Supreme Court of the Russian Federation requested the lower courts to bring the state authorities (customs authorities, tax authorities, prosecutor's office) into suspicious cases. However, the number of such crimes didn't reduce. What is even more problematic is that such crimes are now conducted in many cases by big cross-border groups which use the falsified documents from other countries which are quite difficult to check in Russian courts.

The criminal law in Russia doesn't distinguish cross-border crime as a separate legal construction. It authorises investigative bodies to initiate a criminal case against foreign nationals and stateless persons who do not reside permanently in the Russian Federation and who have committed crimes outside the boundaries of the Russian Federation, where the crimes infringe upon the interests of the Russian Federation or a citizen of the Russian Federation. The Russian authorities should also investigate cases provided for by international agreements of the Russian Federation or other documents of an international nature containing obligations which are recognised by the Russian Federation in the sphere of the relations regulated by the Criminal Code and unless the foreign citizens and stateless persons not residing permanently in the Russian Federation have been convicted in a foreign state and are brought to criminal liability in the territory of the Russian Federation.

However, lawyers must take into account the specific features of cross-border crimes. With regard to fraud and other white-collar crimes, it is the duty of the lawyer to gather a pool of evidence sufficient for initiation of a criminal case.

The active role of consultants in searching for evidence derives from the features of the Russian criminal procedure. It consists of several separate stages, including a pre-investigative check, preliminary investigation and trial (that is, examining the merits of the case).

Each of the stages may be terminated without bringing the alleged offender to criminal liability. For instance, the criminal complaint by itself doesn't automatically lead to initiation of a criminal case in Russia as the pre-investigative check may be terminated with the investigator's decree to refuse to initiate the criminal case, which is a quite frequent outcome. The available statistics of the Ministry of Internal Affairs demonstrate that several years ago it was considering more than 11

million criminal applications per year, but only 1.7 million criminal cases were initiated.

The vast majority of criminal applications in Russia related to economic crimes do not result in prosecution. A lot of decisions not to initiate a criminal case were based on the grounds of there being a lack of the elements of the offence. However, the real ground for such refusals was absence of evidence presented in a form recognisable by state authorities. For instance, the investigator often isn't able to distinguish whether the disputable matter is of a civil or criminal nature. This problem is common for cross-border crimes in which the alienation of assets may be related to violation of a foreign law. In one such case, the offender provided his client (a foreign corporation) with false information, stating that the Russian legislation contained a provision that prohibited foreigners from owning immovable property. To circumvent this prohibition, the lawyer offered to register all the property rights in his name. According to his words, his status as a 'registered agent' deprived him of the right to alienate the assets. After receiving all the property rights, he swiftly sold the property. However, from the point of view of an outside observer, his actions could look like being of a civil nature. The attorney made all the misleading statements orally, during private conversations with his client. Therefore, there is no material evidence that could convince an investigator that a deception was committed.

It is even more relevant to cross-border crimes where the lack of easily obtainable evidence is a common obstacle for urgent initiation of a criminal case in Russia. Fraudsters are well informed about such difficulties and employ foreign accomplices as a self-protection measure. For example, illegal appropriation of title to assets is often done under a power of attorney by a person not aware of the illegal nature of their actions. The instigator of the crime issues such fake power of attorney abroad. Staying abroad prevents them from being caught and complicates the process of verification of the power of attorney.

Another factor that hinders efficient prosecution is the formalistic approach to the provided evidence adopted by investigative authorities. The law defines a list of admissible evidence which includes the evidence given by a suspect and an accused; the evidence of a victim and a witness; the conclusions and testimony of an expert; the conclusion and testimony of a specialist; demonstrative proof; records of the investigative and judicial actions; and other documents.

However, in practice an affidavit of a victim (witness) is not considered as evidence. It can be attached to the case file; however, the alleged victim (witness) is required to visit an investigator to be interrogated in person. The Russian authorities are not eager to accept interrogation using online technologies. In many cases it is quite difficult to organise such a personal visit of the victim or their representatives to Russia. This problem was especially crucial during COVID-19 restrictions on travelling in Russia and abroad.

A similar approach is usually taken in respect of digital evidence gathered and presented to the investigator by a third party or in respect of the copies of criminal case materials received from foreign jurisdictions.

For example, unknown entities presented to the court powers of attorney authorising them to represent the interests of a plaintiff residing in a Western European country. It followed from the circumstances of the case that the plaintiff's suit was initiated maliciously as an attempt to appropriate the victim's assets via a court judgment taken on the grounds of falsified evidence. During interrogation carried out by the foreign police, the plaintiff testified that the suit had been initiated groundlessly at the demand of his acquaintance. He also confessed that the powers of attorney were issued to an unknown person appointed by this acquaintance. Copies of those case files were transferred into Russia by foreign advocates. However, the investigator refused to initiate a criminal case based on the protocols of the interrogations composed by his foreign colleagues.

The legislation entitles an investigator to seek international cooperation in obtaining evidence from abroad. The process of this procedural action is complicated by strict regulation and bureaucratic delays. If it is necessary to carry out an interrogation, examination, seizure, search, court examination or other procedural actions stipulated by the Russian Criminal Procedure Code in the territory of a foreign state, the court, the public prosecutor, investigator, the head of an investigatory body or inquirer shall direct a request for performing these actions to the competent bodies or officials of the foreign state in conformity with an international treaty with the Russian Federation or with an international agreement or based upon the principle

of reciprocity. It is very important that a request cannot be filed at the stage of a pre-investigative check, which makes it impossible for an investigator to obtain evidence from abroad until the criminal proceedings are initiated.

Another actual problem stems from the dualism of the legal profession in Russia. The law does not prohibit a person lacking any legal qualification from rendering legal services (excluding criminal defence and some other specific forms of legal assistance). This ambiguity creates a favourable environment for committing fraud against foreign clients who are not aware of it. For instance, a foreign entity hired a private lawyer to recover a debt from a seller of goods through court procedures. The lawyer had been reporting to his client via email about his successful work and provided the copies of civil court judgments. For more than a year he had been receiving fees from the foreign entity. The fact of deception was discovered only when the entity hired another law firm for initiating the enforcement proceedings. It became clear that the lawyer had never filed a civil suit in the court, but had simply forged all the documents that were presented to the client.

Fraudsters actively use foreign entities' lack of information about national realities and their inability to verify the provided information. The following case can serve as an illustration. For example, a company from South Korea made several attempts to conclude a supply contract with major petroleum companies in Russia. All the offers were ignored or rejected by the producers. Before long, a representative of a third company contacted the foreign firm and stated that he was acting as an intermediary of one of the major companies. He declared that he was able to supply the required materials. After signing the contract, the representative of the intermediary company requested US$10,000 to be transferred to him for freighting a ship. The required sum was duly transferred to him. However, the navigation monitoring system showed that the ship moved to Europe instead of its planned destination in Eastern Asia. For an explanation, the intermediary company representative said that the ship had broken down and was headed to a dock for repairs and for that he required an additional US$10,000 for freighting another ship because, according to the contract with the shipping company, the previous payment would be returned in two months. After receiving the second payment, the so-called representative of the intermediary company stopped all communication with the foreign company.

Another common type of fraud is committed by local management against a foreign corporation. The roots of such crime are similar to that previously discussed: an inability to check all of the information provided by employees. The following case may serve as an illustration. A Chinese corporation had a subsidiary in Russia which was headed by a foreign manager as CEO. All other managerial positions (including CFO, COO, commercial director) were held by locals. Several years ago, one of the local managers informed the CEO that in order to continue receiving contracts from large Russian firms, they had to invent some sort of financial incentive for their managers. As direct payments from the foreign company's account could be regarded as corruption, the manager suggested creating an independent company which would receive payments for its services, cash them out and then use them as a source for paying illicit financial incentives. The new company would be able to render such services by unofficially subcontracting all the services to the employees of the foreign company. In other words, the foreign company paid fees to the firm, while all the services were rendered by its own staff using its own equipment. Even all the accounting was kept by the financial department of the foreign company. Eventually, this situation raised the suspicions of the compliance officer at the head office and he initiated an internal investigation. It helped to discover that the whole plan was devised by one of the local managers only to enrich himself through this scheme. In actual fact, absolutely no payments were made to the managers of large Russian firms; all accumulated money was simply stolen.

Therefore, the misrepresentation of information is often a common *modus operandi* of cross-border frauds. Several times in the course of internal investigations our white collar crime team was able to discover situations where the signs of embezzlement were concealed by shading factual details of business activity from the head office. For example, local management often overstated the real pricing of repairs or communal services. This let them conclude hugely overpriced contracts with affiliate contractors and share the excess monies. For example, a compliance department's attention was drawn to the activity of a local manager responsible for picking contractors for maintenance

and repairs of the premises of the company who hadn't taken sick leave or a vacation for five years. Analysis of the contracts which he supervised showed that each of them had been overpriced three- to five-fold. The contractual performer of the works and services acted as an intermediary, while works and services were performed by a sub-contractor. But the sub-contractor's fee was several times lower and all the excess income was appropriated by the intermediate contractor. It must be noted that, as in many other cases, our team discovered that local executives who weren't actually involved in this fraud did their best to hide this incriminating information from the head office, as they perceived it as a sign of their incompetence. This approach is one of the most conducive factors that facilitates the committal of cross-border crimes by local management against foreign head offices.

So, in summary, our experience demonstrates that the following factors simplify the commission of cross-border crimes:

- impossibility to verify the information provided by a contractor from abroad;
- a complicated procedure for gathering evidence from foreign jurisdictions;
- the application of cyber technologies;
- an excessive trust in local management;
- shortcomings of internal regulation in a company;
- a conflict of interest that prevents local executives from 'washing dirty linen in public'.

When providing legal services for foreign clients, our team usually advises them to follow some simple rules in order not to be deceived:

1. To avoid working with individual legal consultants abroad, because the law doesn't provide sufficient protection against abuse from their side. Only trusted and well-known firms should be hired for representation abroad.
2. To engage independent consultants for carrying out internal investigations separately from the local staff who may not be interested in uncovering the truth.
3. To avoid letting local managers pick subcontractors without a transparent procedure.
4. To implement internal policies in local offices in accordance with Russian labour legislation (which requires translation of the internal policies into Russian and notifying every employee against signature).
5. In case any assets are present in the local market, to monitor official court databases in order not to miss a maliciously taken legal action based on a forged power of attorney.
6. To implement antifraud digital technologies aimed at prevention of hacking and phishing mailing attacks.
7. To carry out training for personnel conducted by criminal law specialists experienced in internal investigation of fraudulent incidents in this particular jurisdiction.
8. To think in advance what evidence would you be able to present to the state authorities in the case a prospective counterpart commits an offence.
9. To analyse in advance whether it would be expedient to spend time and money on an attempt to initiate criminal proceedings that most likely would be waived according to local practice.

Notes

[1] http://crimestat.ru/analytics, 2021 report on the state of crime in Russia.

Maxim Alekseyev
Senior Partner, Head of Asia-Pacific Desk, ALRUD Law firm, Moscow

Maxim is the Co-founder, joint Senior Partner and Head of the Asia-Pacific Desk at ALRUD Law Firm. Maxim specialises in advising clients on international trading matters, regulatory and economic developments, domestic and international tax planning, strategic M&A, risk management, good governance, contentious investigations and dispute resolution.

Cross-Border Fraud— Law and Investigations in Vietnam

As global trade increases rapidly, in addition to the flows of legal trading moving globally, illegal business activities of transnational criminals are globalised, increasingly expanding their areas and taking advantage of markets. In addition, the internet has increased developments in technology and social media has made communication across countries much easier, which in turn also facilitates a much larger scale for fraudsters targeting millions of potential victims globally.

Introduction

Cross-border crimes are rapidly increasing, especially drug trafficking and highly profitable crimes such as firearms trafficking, human trafficking, money laundering, international economic crime and high-tech crime. In addition, many other illegal trade activities are also appearing and increasing, such as trade in rare animals, artworks, stolen antiquities and international crime related to credit cards. The flows of people, money and goods moving from one country to another in the context of globalisation and international economic integration are favourable conditions for criminals to expand their activities such as: smuggling, trafficking of women and children, and sending people abroad to reside and work illegally.

Transnational criminal organisations fully exploit international deregulation, border controls and the promotion of freedom to expand their reach in many countries around the world; colluding with each other more often and more closely, to take advantage of the strengths, limit the weaknesses of each organisation, divide criminal activities and reduce the risk of detection.

Cross-Border Crime Situation in Vietnam

In the past years, the cross-border crime situation related to Vietnam has also tended to increase gradually in terms of both the number of cases, their nature and severity, and especially the activities of cross-border organised criminal groups. Highlighted are:

1. *Crime of trafficking Vietnamese women and children abroad*. This type of crime is increasingly complicated and tends to increase with many new and more sophisticated tricks, such as fake marriages, taking advantage of visa exemptions and using fake passports to smuggle people into the country. Vietnamese women and children go abroad to work in prostitution, are sold as foreign wives, exploited as labour, etc., concentrated in a few countries and territories such as Russia, China, Hong Kong, Korea, Taiwan, Cambodia, Malaysia and Singapore.

2. *Crime of sending people abroad illegally*. Scam activities to bring Vietnamese people abroad to reside and work illegally has also tended to increase and involves mainly sending Vietnamese people to Eastern Europe, Western Europe, Northeast Asia (Japan and South Korea), and Australia as well as countries and territories in the region such as Malaysia, Thailand and Taiwan.

3. *Drug crimes*. In recent years, the international and foreign-related factors of drug crimes in Vietnam

have become clearer. Specialised forces in Vietnam and other countries discovered that many drug offenders were overseas Vietnamese and foreigners entering Vietnam to trade and transport drugs. At the same time, through international cooperation, the functional forces of Vietnam coordinated with the functional forces of other countries to detect and arrest many cases of drug transport from Vietnam to other countries (such as Australia, Canada, New Zealand and USA) and transporting drugs from abroad into Vietnam (from China, Laos and Cambodia, for example). However, the situation of drug trafficking and transportation from abroad into Vietnam and vice versa is still very complicated, especially over land border and sea and air routes.

4. *Crime of producing and trading in counterfeit money, counterfeit goods, commercial fraud, smuggling, economic fraud, import and export tax evasion in free trade economic zones and e-commerce*. The production, transportation and consumption of counterfeit money (including Vietnamese and foreign currency) is complicated and has increased. The source of fake Vietnamese money is mainly brought into the country from the border area. The offence is established in the way that domestic people often buy counterfeit money in border areas, mainly sourced from foreigners, then bring it inland for consumption. In addition, there are some foreigners who use fake cheques and credit cards to enter Vietnam to withdraw money. Smuggling and commercial fraud are complicated. The main offencers are transporting goods, especially consumer goods from other countries into Vietnam for consumption, and transporting precious and rare petroleum and forest products from Vietnam to foreign countries taking advantage of the 'loopholes' in the law, limitations in management and control to evade taxes.

5. *Crime of fraud, appropriation of property*. Foreign criminals take advantage of 'loopholes' in Vietnam's regulations on economic management, set up 'ghost' companies and fraudulently appropriate property. Recently,

some foreigners have operated in the form of limited liability companies, then appropriated money and fled back to their home or third countries.

6. *High-tech crime*. This type of crime in Vietnam has thrived in recent years with dozens of cases related to taking advantage of stolen credit cards from foreigners via the internet (ATM Cash-out). It is complex with extremely sophisticated technological elements and includes attacks on the websites of businesses, financial institutions, theft of confidential information, hackers, theft of money through banks by means of a device and theft of telecommunications fees.

7. *Crimes committed by overseas Vietnamese who then fled back to Vietnam*. In recent years, in some countries, many Vietnamese criminal gangs have appeared, with activities such as smuggling (drugs and weapons for example), cheating, abduction extortion, murder, robbery, money laundering and trafficking in women and children. Through international cooperation, Vietnamese authorities have discovered and arrested many people belonging to overseas Vietnamese criminal gangs that collude with domestic criminals conducting such smuggling activities, illegal money transfers, kidnapping, debt collection and forming smuggling and human trafficking lines. Most overseas Vietnamese criminal gangs have colluded with criminal gangs in Vietnam and other countries to conduct cross-border criminal activities.

8. *Crimes committed by foreigners in Vietnam*. Currently, there are nearly 400,000 foreigners living in Vietnam (of which Chinese, Taiwanese and Korean nationals account for about 40 per cent). Many foreigners enter Vietnam to carry out new criminal activities such as credit card fraud, fraud through the implementation of economic contracts via the Internet, high-tech crimes, etc.

Vietnam's Current Relevant Regulatory Framework

Vietnamese law has domesticated most of the content recognised in ASEAN conventions on cross-border crimes. Basically, as required by the ASEAN Convention against Trafficking in Persons, Especially Women and Children ('ACTIP'). Vietnam has criminalised acts such as human trafficking, corruption, legalisation of property acquired by crime and acts of obstructing judicial activities.

Similarly, in accordance with the provisions of ACCT, Vietnam has also criminalised the crime of terrorism, terrorist financing, money laundering and other acts related to this crime. In addition, several other cross-border crimes such as drug crimes, high-tech crimes and weapons trafficking are also criminalised under Vietnam's criminal law.

In the spirit of preventing and combating cross-border crimes in the region, besides the promulgation of legal regulations, Vietnam has constantly launched programs and action plans to effectively implement crime prevention and control. Although the country has paid much attention to building the legal system related to cross-border crime prevention and control, there are still many shortcomings, lack of synchronisation and lack of a system, requiring further research to supplement and amend the current regulations to suit international law in general and ASEAN law, in particular:

1. *Specialised legal documents on the prevention and combat of some typical regional cross-border crimes such as terrorism financing, high-tech crimes, and piracy crimes have not been developed yet*. The act of financing terrorism is an act as dangerous as the criminal acts of terrorism. However, Vietnam does not have any separate law regulating this issue; it is only mentioned in a few laws by the Ministry of Finance, the criminal law; Law on Anti-Terrorism; Law on Anti-Money Laundering, etc. Moreover, piracy is also a dangerous crime. Criminal acts are also quite common in the region and high-tech crimes are becoming more and more complicated. However, Vietnam's law only provides regulations on the punishment for this type of crime, but there are no other regulations on detecting, warning, or coordinating to prevent and handle such crimes in a specific way. In addition, the provisions of Vietnamese law on cross-border crimes have not yet fully codified the provisions of the legal documents of ASEAN, such as the Law on Prevention and Control of Terrorism 2013 which does not have provisions on 'refugee status' or 'rehabilitation program for offenders'. Meanwhile, these are regulations that ACCT requires countries to take appropriate measures to enforce.

2. *Some regulations of Vietnamese law are not compatible with international and regional laws on national crime prevention and control.* Regarding the provisions of the crime of trafficking in persons, ACTIP also covers the trafficking of a child or person who is unable to care for or protect themselves because of a physical or mental disability or condition considered to be particularly vulnerable. Therefore, when committing a crime against these individuals, it is considered as one of the aggravating circumstances to impose a heavier penalty than a normal crime. However, at present, Vietnamese law only stipulates children to be considered as particularly vulnerable people; there is no other provision for aggravating circumstances for crimes involving victims who are incapable of taking care of or protecting themselves because of a disability or physical or mental condition. For example: Article 151 of Criminal Code 2015 regarding the trafficking of a person under 16 years old. In addition, the ACTIP defines 'a child as any person under the age of 18', while Vietnamese law defines 'a child as a person under the age of 16'. That is why Vietnam's Criminal Code 2015 stipulates that the crime of trafficking in people from 16 to under 18 years old is a common human trafficking crime without having to trade in children as prescribed in the ACTIP. This shows that the Criminal Code of Vietnam has the policy to deal with the crime of trafficking in persons from 16 to under 18 years old in Article 150 which is not compatible with international treaties of which Vietnam is a member.

   In addition, according to the provisions of the ACTIP, 'Trafficking in persons is the recruitment, transportation, transfer, harbouring or receipt of persons for the purpose of ...'. Thus, the acts specified in the ACTIP that constitute the crime of human trafficking, such as the act of transferring, receiving, recruiting, transporting and harbouring are independent from each other. When any of these acts are committed for the purposes of the Convention, it constitutes a crime of trafficking persons. However, the Vietnam Criminal Code 2015 has a completely different stipulation, that is, recruiting, transporting, harbouring other people to perform acts, transferring or receiving people to deliver or receive money and property or other material benefits; the transfer or receipt of a person for sexual exploitation, forced labour, organ removal or other inhumane purposes, constitute a crime of human trafficking.

   The ACTIP requires its members to adopt legislative and other measures as appropriate so that those who commit crimes are subject to more severe penalties than would otherwise be the case for ordinary crimes in one of the following aggravating circumstances:

   - When the crime causes serious injury or death to the victim or another person, including when the person dies by committing suicide.
   - When the crime involves a victim who is a particularly vulnerable person such as a child or who is unable to take care of or protect themselves because of a disability or physical or mental condition.
   - Crimes expose victims to life-threatening diseases, including HIV/AIDS.
   - Committing crimes with multiple victims.
   - When the crime is committed as part of an organised crime group's activities.
   - When the offender has been convicted of the same or similar crime.
   - When the offender is a public servant who abuses his position or power to commit a crime.

   However, in both Articles 150 and 151 of the Criminal Code 2015, the aggravating penalty frame has not been applied to the circumstances required by the Convention, for example, circumstances when the offender is a public official or circumstances of causing victims infected with dangerous diseases such as HIV/AIDS. In addition, Article 150 and Article 151 provide inconsistent aggravating circumstances, for example, Article 51 contains the circumstance of 'abusing position and rights', but Article 150 does not so stipulate. Therefore, this issue should be considered and a relevant adjustment to the prevailing Criminal Code should be made on the basis of the ACTIP.

   In addition, the ACTIP provides that its members consider, through legislative or other appropriate measures, permitting victims of trafficking to remain in their territories, either temporarily or permanently,

on a case-by-case basis. Up to now, Vietnamese law has only provided assistance in arranging temporary accommodation for victims. The lack of specific provisions on assisting trafficked persons to remain in its territory permanently can make it difficult for victims in certain circumstances. For example, trafficked children are children who have been kidnapped and sold since birth. It is difficult to determine their hometown and origin, so it is difficult to return them to their homeland.

Furthermore, the ACTIP provides that its members consider not imposing penalties or administrative liability on a trafficked person for his or her unlawful conduct if such illegal acts are the direct consequences of human trafficking. This is also an important issue to ensure the legitimate rights and interests of victims, but this issue has not been recognised by Vietnamese law so far. After being trafficked, victims are mostly dependent on criminals, easily exploited by them and required to perform illegal acts. For example, trafficked persons should not be punished for immigration fraud, working illegally or working in the sex industry. This consideration and recognition of these rights is necessary for the specific situations of trafficked children and others with special protection needs. If the provision of criminal and administrative liability for such acts would be unfair to victims, it would also make them hesitate to report crimes by traffickers or cooperate in giving testimony and evidence related to the crime.

3. *The international legal basis*. Although Vietnam has made efforts to sign and join international treaties related to crime prevention and control, within ASEAN there is no such agreement on extradition. In the area of extradition agreements, bilateral agreements on this issue are still modest, especially since there is no basis for cooperation with some ASEAN countries with large numbers of Vietnamese working and living there. Moreover, there are documents that have been signed for a long time and need to be amended and supplemented accordingly. It is worth noting that Vietnam currently affirms not to apply many multilateral international treaties to which Vietnam is a member (such as the United Nations Convention against Corruption and the United Nations Convention against Transnational Organized Crime) as a direct legal basis for extradition activities but must apply those provisions in accordance with the basic principles of the national legal system and on the principle of reciprocity. This will significantly limit the possibility of cooperation in arresting and transferring criminals between Vietnam and the member countries of the conventions, including ASEAN countries.

4. *Coordination between Vietnam's central agency and ASEAN agencies*. Practice shows that the coordination relationship between Vietnam's central agency on the implementation of cooperation in crime prevention and control (extradition, mutual legal assistance in criminal matters and the transfer of persons sentenced to imprisonment) and the corresponding agencies of ASEAN countries is not close and effective. There is still a lack of information on contact points, making information exchange and cooperation requirements difficult. Some countries request that the request for cooperation be transferred through diplomatic channels, which takes a long time.

The Role of Lawyers in Helping Clients Identify Behaviour and Implement Effective Enforcement Actions Against Cross-Border Fraud

Introduction

In the practice of law in Vietnam, the participation of lawyers in the investigation and handling of cross-border fraud crimes is still limited and not conclusive. During this stage, the role of the investigating agency and mutual legal assistance between the state agencies of the concerned countries plays a significant part.

However, the role of lawyers cannot be denied in the preparation and negotiation stage for several cross-border trading transactions such as the purchase and sale of goods, transactions of shares and capital contributions between enterprises ('M&A transactions'). As cross-border trading transactions or M&A transactions are always risky, even companies that regularly conduct M&A activities, with a large and elite team of M&A developers, cannot be completely sure to anticipate all possible risks encountered. The complexity and risks of M&A transactions require companies to consult with experienced lawyers.

In these transactions, lawyers will be involved in legal due diligence to determine the legal status of the seller or

buyer and reviewing the activities of the seller/buyer to determine the suitability of the conditions and standards as prescribed by law. In addition, there will also be the participation of an audit firm or experts with specialised functions to conduct due diligence and investigation of issues related to finance, accounting, commerce, information technology, intellectual property, etc. From there, it is possible to detect current or potential risks to provide important insights and necessary warnings about signs of fraud and dishonesty for clients to consider.

Legal Due Diligence

Lawyers will review in general and give expert legal opinions on the implementation of M&A transactions. In other words, lawyers will:

1. Play the role of strategic consultants and may also be involved in negotiations as requested and proposed by clients in the first stage. Specifically, the lawyer will analyse the potential of clients based on tangible and intangible aspects such as vision, strategy, brand, exclusive products, human resources and ability to be listed on the stock exchange. Accordingly, it will help clients to exactly identify their capacity and position in conducting M&A transactions appropriately and effectively.

2. Help clients determine the accuracy of the information. There will be a lot of information that should be carefully considered while conducting M&A transactions or cross-border trading transactions, because when any information about both the buyer and the seller appears, it can affect the success of the M&A transactions or cross-border trading transactions. Therefore, the lawyer will be able to assess the accuracy and reliability of the information given to help clients make the right decisions and take the right steps in accordance with the actual situation.

3. Analyse and forecast potential risks. Risk forecasting will determine the success of M&A transactions or cross-border trading transactions. Especially in M&A transactions, risks can still occur after the transaction is completed. Some of the risks considered by lawyers may be the prediction of non-depreciable assets, doubtful debts or cash flows from the sale of fixed assets that are not commodities. In addition, the risk related to personnel instability is also an aspect related to M&A transactions that should be raised as after the M&A transaction is made, key officials are no longer interested in the company, which will affect the sustainable development of enterprises.

4. Support on drafting necessary meeting minutes, memoranda of understanding, sale and purchase contracts, internal governing documents related to the change of capital structure and number of members or shareholders.

Although Vietnam has made efforts to sign and join international treaties related to crime prevention and control, within ASEAN there is no such agreement on extradition.

Financial Due Diligence

Lawyers will cooperate with financial professionals to verify the financial information provided, evaluate the underlying business activities of the target business as well as check the compliance with accounting standards. Accordingly, lawyers will coordinate in the assessment of income, assets, liabilities, cash flow, loans as well as the internal control system of the target business based on the following documents: financial statements, accounting balance sheets, agreements, profit/loss records, taxation applications, reports on business results and activities, etc.

Other Due Diligence

Lawyers will be in cooperation with professionals to verify the environment in which the buyer/seller is operating, such as assessing clients, competitors, business sectors, prospects and risks as well as evaluating the assumptions used in developing the business plan. The assessment is often based on the SWOT analysis model: Strengths, Weaknesses, Opportunities and Threats.

Regarding tax due diligence, lawyers may coordinate in assessment of relevant taxes, compliance records, tax status, tax planning, tax incentives and tax risks. Regarding IT due diligence, lawyers may coordinate in assessment of accounting software, enterprise-wide management system, internal servers, software and network systems. Regarding intellectual property due diligence, lawyers may coordinate on the assessment of property titles by certificate of ownership, use rights, certificate of copyrights, patents, industrial designs and trade secrets.

Suggestions for Improvement

From the experience of some countries and the implementation of the ASEAN community's law on the prevention and combat of cross-border crimes in Vietnam, there are some recommendations for Vietnam which can be summarised and highlighted as follows:

1. *Developing specialised legal documents on several specific cross-border crimes and mutual criminal justice assistance*. It is necessary to develop specialised legal documents to clearly define the measurement for crime prevention and control in a general way, such as the Law on Prevention and Control of Terrorism 2013; Law on Prevention and Combat of Human Trafficking 2011 and the Law on Drug Prevention and Control 2008. Only these specialised laws can internalise all provisions of international conventions on crime prevention and control, such as: crime prevention measures, information communication, mechanism building and victim support. In the context of the current complicated developments in the financing of terrorism, high-tech crimes and piracy, Vietnam should quickly develop specialised legal documents to regulate these types of crimes to create a solid and specific legal basis for the fight against crime.

   There should be separate laws on mutual legal assistance in civil matters, mutual legal assistance in criminal matters, extradition and the transfer of persons serving prison sentences. This will help specify in detail the order, procedures, principles and conditions to implement mutual assistance for each field as above; to better define the competence, responsibilities and coordination relationship between the competent authorities in the process of carrying out activities related to mutual criminal justice assistance, meeting the requirements specified in the ASEAN Agreement on Mutual Legal Assistance in Criminal Justice 2004.

2. *Completing the content of legal provisions on combatting transnational crime prevention to be compatible with ASEAN legal documents*. To improve the effectiveness of transnational crime prevention and control as well as increase the compatibility of Vietnamese law with the ASEAN community's law on the fight against cross-border crimes, Vietnam should actively research and improve its provisions in specialised legal documents for each specific type of crime. For example, regarding the crime of human trafficking, it is necessary to supplement regulations to protect the legitimate rights and interests of victims, specifically:

   a. Add provisions on crimes involving particularly vulnerable victims, including people who are unable to take care of or protect themselves because of a disability or physical or mental condition.

   b. Promulgate provisions to assist trafficked persons to remain in their territory indefinitely in certain specific circumstances.

   c. Add provisions that do not impose penalties or administrative responsibilities on trafficked persons for their illegal acts if such illegal acts are the direct consequences of human trafficking.

   d. For terrorist crimes, the legislative body should consider amending a few regulations to identify terrorist crimes in accordance with international treaties to which Vietnam is a member, such as the group of acts related to aircraft and infringing on civil aviation safety, the group of acts infringing upon the safety of navigation and fixed structures on the continental shelf and the group of acts related to illegal use of dangerous weapons and explosives.

3. *Refining the legal institutions on transnational crime prevention and control*. From the experience of two other countries in the region (Cambodia and the Philippines), Vietnam should build specialised national committees responsible for managing activities to prevent and combat specific types of crime. At the same time, in addition to the Drug Crime Investigation Police Department and the High-Tech Crime Prevention and Control Police Department, it is necessary to set up other specialised police departments such as the Investigation Police Department for preventing and fighting human trafficking and the Police Department for preventing and fighting terrorist crimes.

4. *Strengthening skills and improving the quality of law enforcement officers and civil servants*. To achieve high results in cooperation in the fight against crime,

Vietnam needs to focus on improving the knowledge and skills of officials, civil servants and public employees working in the field of transnational crime prevention and control (such as foreign language skills, computer skills and professional knowledge) in order to exchange information and data quickly and efficiently, especially in the context of ASEAN where the only regional administrative language is English. In addition, it is necessary to promote cooperation activities outside the ASEAN region, strengthen the organisation with conferences, seminars, training courses, multilateral and bilateral forums on the content of international treaties related to cooperation activities and to share, consult on experiences, improve qualifications and the capacity for specialised staff to meet the increasing requirements of international cooperation on the prevention and the control of transnational crime among ASEAN countries.

5. *International treaties and participation in ASEAN forums*. The promotion and strengthening of negotiation, signing, accession and well-organised implementation of international treaties on the prevention and control of ASEAN transnational crimes, especially the General Convention on Extradition and Convention on drug crime prevention, is important. In addition, Vietnam should continue to keep an active and proactive role in maintaining its participation in annual regional forums such as ASEANAPOL (ASEAN Conference of Police Commanders), Ministerial Conference on Combating Transnational Organized Crime (AMMTC), COMMIT (Ministerial Coordination Initiative in the Prevention and Combat of Human Trafficking in the Mekong Sub-region) and ASOD (Annual Meeting of ASEAN Senior Officials on Drug Issues) to further promote coordination in formulating cooperation policies, as a foundation for the implementation and negotiation of international treaties in each specific area.

6. *Cooperation mechanism between ASEAN central agencies.* Vietnam should do its best to push other member states to build an effective cooperation mechanism between the central agencies of ASEAN countries in the implementation of international treaties on crime prevention and control; to notify and regularly update information about the central authority (address, phone number, contact officer, request forms for mutual legal assistance, etc.) of member countries, building common data for mutual legal assistance in criminal matters, the extradition and transfer of sentenced persons to countries in the region, ensuring the elements of speed, accuracy and efficiency.

Conclusion

It is predicted that, in the coming years, cross-border organised crimes will continue to operate in a complex manner, negatively affecting the process of the international economic integration of Vietnam with constantly increasing criminal acts with more sophisticated methods and tricks to achieve political, economic and social purposes, creating challenges for law enforcement agencies of the countries in the region and the world. The problem of fake news and untruthful information also can cause confusion in public opinion, adversely affecting security and order. The sharp increase in e-commerce transactions, payments through the banking system and payment intermediaries has also created conditions for high-tech criminal activities to increase in both number, nature and the level of crime, with many new methods, directly affecting many areas of social life, causing difficulties in prevention.

Overall, Vietnam should actively perfect its laws based on signed international treaties as well as implement plans and measures for cross-border crime prevention and control in the current context of globalisation and international integration.

Bui Cong Thanh (James Bui)
Managing Partner, PLF Law Firm, Ho Chi Minh City

Mr Bui Cong Thanh is the Managing Partner of PLF Law Firm. He is also a member of the Vietnam Business Lawyers Club, Ho Chi Minh City Bar Association and the Vietnam Bar Federation. He specialises in real estate and M&A deals related to enterprises operating in various industries, such as services, retailing, manufacturing, technology and F&B.

Cross-Border Fraud, Law and Investigations in Poland

It seems that, despite such a significant increase in the number of cross-border frauds in Poland, this type of crime rarely becomes the subject of legal consideration, not many law firms in Poland deal with this issue and there are no broader studies of the doctrine in this area. In this article, the author will present the problems personally encountered when dealing with cross-border fraud cases, as well as the basic types of crime dealt with in the course of the author's daily work. This article also refers to the basic legal regulations that apply to proceedings conducted in connection with the commission of fraud, as well as to which type of procedure should be selected to effectively detect the perpetrator of the crime and quickly recover the property lost as a result of the crime.

Cross-border fraud is understood as a crime in which a perpetrator residing in one country uses fraud to steal property belonging to a person residing in another country. Recently, a significant increase in the number of incidents related to cross-border fraud has been recorded, including those related to the use of the internet; cross-border fraud is becoming a more and more frequent crime against property committed in the Polish jurisdiction. Due to the progress of computerisation and digitisation, especially in the banking sector, the development of information technology, the widespread use of the internet, email, particularly in correspondence with contractors, offices or public authorities, there is a noticeable increase in this type of crime, which is a new challenge for Polish lawyers and legislators.

Cross-border fraud dealt with in the Polish jurisdiction most often includes crimes aimed at the unlawful seizure or extortion of funds accumulated in a bank account, particularly via electronic banking. It should also be pointed out that a common type of cross-border fraud is phishing, which, as commonly understood, is a method adopted by fraudsters when the criminal impersonates another person or institution to extort confidential information, induce the victim to conduct certain actions or infect the computer with harmful software. Another form of cross-border fraud is so-called spoofing, which is a type of attack involving criminals impersonating government institutions and agencies, banks, companies or individuals in order to extort data or money. The criminals sometimes also make purchases via the internet. This happens when the consumer orders goods from abroad, pays for them, but the goods never reach him. As a rule, in this case, all attempts to contact the alleged sellers fail; they are elusive. In fact, the fraudster created a fake website to encourage others to buy goods that do not actually exist or to obtain information about buyers' credit cards and bank accounts.

In the process of analysis of this phenomenon, it should be emphasised that, in the Polish legal system, both criminal and civil law are used to combat cross-border fraud. The best way to fight this type of crime is to prosecute the perpetrators on many levels, that is, initiating criminal proceedings and, at the same time, civil proceedings. To effectively recover the stolen property, it is reasonable to conduct both of the above-mentioned proceedings in parallel with the mutual use of the evidence collected in these proceedings. The legitimacy of conducting criminal law-based proceedings is justified primarily by the fact that Polish civil proceedings are lengthy, which relates to, *inter alia*, a long waiting period for setting the dates of hearings or obtaining security, especially when the case involves an element of foreign law. In criminal

proceedings, on the other hand, when charges have already been brought against the individuals involved, it is possible to obtain security quickly and effectively. It is also worth adding that, in civil proceedings, the courts very rarely show evidence initiative, they prefer to rely on evidence from witness testimonies and evidence from documents that will be presented by the parties.

However, the practice shows that a significant proportion of cases are heard faster in a criminal trial. Moreover, some evidence can only be obtained in criminal proceedings, including in particular, evidence that is relevant to money laundering. In addition, the Polish criminal process also enables an efficient obtaining of evidence that is covered by banking, tax or telecommunications secrecy regulations, as well as the efficient questioning of witnesses. As the practice shows, the key evidence in the case, which allows both the detection of the perpetrators, but, above all, the location and seizure of the assets constituting the subject of the crime, is information which is covered by banking secrecy regulations. In a situation where, when committing a crime, the perpetrator uses a bank account established for this purpose, even if he used false personal data or data of another person, as well as when the bank account was opened via the internet, obtaining data covered by banking secrecy will greatly facilitate the detection of the perpetrator of the fraud, and additionally, determining whether the funds constituting the subject of the crime are still in these bank accounts, and in the case of their further transfer, tracing the transfer destination and, in most cases, determining their final storage location. In each of the cases described above, the perpetrator will leave a trace, particularly in the form of an IP address, ATM data or other bank account numbers used for further transfer of illegally obtained funds.

It is worth noting that in criminal proceedings the victim of the crime also has access to the case files and collected evidence, but more importantly, the victim is entitled to use them. Thus, it is possible to use the above-mentioned evidence in other court proceedings, including those pending abroad.

In this regard, it is also important that the institution of reparation plays an important role in criminal proceedings, which also facilitates the recovery of the lost property. If the property constituting the subject of the crime is traced, it may be seized against the damage caused to the property of the victim. Furthermore, as part of a criminal trial, it is possible to seize the property that is with a third party as compensation for damage.

In view of the above, in the field of combating cross-border fraud, the initiation and conduct of criminal proceedings is of key importance in the Polish legal order. The special role of criminal law in the fight against cross-border crime also results from the general social view of the criminal process and the fact that the Polish criminal process is more feared and respected than the civil process. Naturally, the above is not a rule, in some cases it may turn out that civil proceedings will be conducted in a more effective and efficient manner than criminal proceedings, because it also happens that the prosecutor's office might discontinue a case, indicating that the case should be settled by a civil court. Therefore, it is reasonable to conduct criminal proceedings and civil proceedings basically simultaneously.

The experience gained over the years in connection with several cross-border fraud cases allows us to assume that in order to efficiently recover funds lost as a result of fraud, it is reasonable to initiate and conduct criminal proceedings, at least as a starting point. It is also worth adding that the role of the attorney-in-fact is extremely important in this respect, as the further course of the case for the effectiveness of the proceedings depends to a large extent on the manner of operation adopted by him. Pursuing one's rights through criminal proceedings by submitting a notification of the possibility of the commission of a crime seems to be a necessary element. Due to the possibility of destruction or loss of IT data, as well as the still relatively easy transfer of funds, a notification of fraud should be submitted in the shortest possible time from the moment of its disclosure, which will significantly increase the chances of law enforcement authorities to secure complete evidence, identify the perpetrator and, most importantly, block the property of the victim.

It is worth adding in this regard that the crime of fraud is regulated in the Polish legal system by the provisions of criminal law and is included in the group of crimes against property, it has been penalised in Article 286 of the Penal Code. Pursuant to this provision:

> Whoever, in order to obtain a financial benefit, causes another person to unfavorably dispose of his or her own or someone else's property by misleading them or exploiting an error or inability

> to properly understand the undertaken action, shall be subject to the penalty of deprivation of liberty for a term of between 6 months and 8 years. The same penalty is imposed on anyone who demands a financial benefit in exchange for the return of an unlawfully taken thing.

In the jurisprudence of Polish courts, it is indicated that fraud is a crime characterised by a purpose in the form of a desire to obtain a financial advantage by the perpetrator, that is, a targeted crime. The characteristic feature of this offence is that the perpetrator obtains this advantage by deceiving or exploiting the error or inability of the other party to properly understand the actions performed. In this crime, error is a factor leading to the unfavourable disposal of property. Importantly, the literature on the subject emphasises that the fact that the aggrieved party could detect a mistake while exercising due diligence is irrelevant to the liability of the perpetrator of the fraud. Similarly, the credulity of the aggrieved party also does not exclude criminal liability for fraud. It should be emphasised that, for the assessment of the act, it is only important whether there was an unfavourable disposal of property as a result of misrepresentation. In terms of the subjective side of the crime of fraud, it is also worth adding that the perpetrator's action must be intentional and therefore must be aimed at obtaining an unlawful financial advantage. The jurisprudence of Polish courts also emphasises that the characteristic of the crime of fraud is that the disposition of property for the perpetrator is unforced, it is a voluntary action, which means that at the time of disposition the person disposing of the property for the perpetrator is not aware of the unfavourable nature of this regulation.

It should also be pointed out that the Polish Penal Code provides for basic (Article 286 § 1 of the Penal Code), privileged (Article 286 § 3 of the Penal Code) and qualified (Article 286 § 1 of the Penal Code in connection with Article 294 § 1 of the Penal Code or Article 286 § 1 of the Penal Code in conjunction with Article 294 § 2 of the Penal Code) types of fraud. In the event of a 'minor accident', the legislator has provided for a milder criminal liability (Article 286 § 3 of the Penal Code). However, in a situation where the perpetrator commits fraud in relation to property of significant value, that is, in relation to property whose value at the time of committing the prohibited act exceeds PLN200,000 (approximately US$46,500) (Article 286 § 1 of the Penal Code in conjunction with Article 294 § 1 of the Code penalty) or in relation to goods of particular importance for culture, the legislator introduces stricter criminal liability.

In terms of the analysed matter, attention should be paid in particular to the fact that the initiators of the majority of cross-border fraud involving the Polish jurisdiction are not Polish citizens. However, Polish entities are often used by criminals; in this respect they act as a tool used by criminals. The above is due particularly to the fact that both the establishment of a company and the opening of a bank account in Poland are relatively simple and do not require a complicated procedure and can take place in a short time. It is also worth adding that conducting an investigation into cross-border fraud is especially difficult precisely due to the fact that, as a rule, the offender and the victim are in different countries and therefore fall under different jurisdictions. The existence of the Polish jurisdiction in cases of cross-border fraud results in particular from the fact that it often happens that funds obtained as a result of fraud are transferred to bank accounts maintained by Polish banks. This is largely a consequence of the possibility of quick and relatively simple opening of bank accounts in Poland, as mentioned above.

As regards Polish jurisdiction, it is worth pointing out that pursuant to Article 112 point 5 of the Criminal Code, Polish criminal law applies to a Polish citizen and a foreigner in the event of committing a crime from which a financial advantage was obtained, even indirectly, in the territory of the Republic of Poland. Within the scope of the above-mentioned provision, that is Article 112 point 5 of the Penal Code, is included acts from which a financial benefit was actually obtained on the territory of Poland. Financial advantage may be obtained both by the perpetrators and by a third party, a Polish citizen or a foreigner, a natural person, a legal person or an organisational unit without legal personality. In view of the above, in such cases it is completely justified to apply Polish criminal law, initiate proceedings before Polish authorities and submit notifications of a suspected crime to the prosecutor's office in Poland.

Moreover, it should be pointed out that the competence of the Polish prosecutor's office is determined by § 116 para. 1 of the Regulation of the Minister of Justice of 7 April 2016—Regulations of the internal office of common organisational units of the prosecutor's office in connection with Article 31 § 1 of the Code of Criminal Procedure, that is, according to the place in which the

crime was committed. Therefore, there is no doubt that in a situation where, as a result of fraud, money ends up in a bank account maintained by a bank with its registered office in Poland, the local authority competent to conduct the proceedings, precisely because of the place of the effect, will be the prosecutor's office in Poland.

When analysing the matter of cross-border fraud, with particular emphasis on fraud involving bank accounts maintained by Polish banks, it is also worth adding that the jurisprudence of Polish courts often emphasises the role of banks as victims of fraud when money is transferred to an unauthorised person. The essence of the bank account agreement is the bank's commitment towards the account holder to store its funds for a definite or indefinite period, as well as to make monetary settlements in accordance with the account holder's instructions. Importantly, the bank is entitled to use the funds accumulated in the bank account belonging to the holder, while being obliged to return these funds at each request of the holder, unless the contract stipulates otherwise. It should be pointed out that the view that the bank obtains ownership of the deposited money is considered to be a common and well-established view, while the account holder obtains a claim for the return of the deposited funds. Assuming that the bank obtains ownership of the deposited money leads to an unequivocal conclusion that the bank is the person directly injured in the event of an unlawful breach of security and transfer of money to an unauthorised person.

To sum up, in the practice of conducting cases in the field of cross-border fraud, we most often encounter situations where, as a result of committing the crime of fraud, funds are transferred to bank accounts maintained by Polish banks. As attorneys advocating for the victim of the crime, we strive to recover property lost because of fraud as quickly and effectively as possible. Prosecution of cross-border fraudsters is extremely difficult due to the wide range of tools, in particular social media and email, that criminals currently have access to.

It should also be pointed out that it is difficult to identify the perpetrators of cross-border fraud, in particular when it comes to acts committed via electronic banking. Criminals are able to quickly redirect the appropriated funds to other bank accounts or immediately withdraw them in cash. For this purpose, they most often use dummies who provide their personal data, so, as indicated above, the identity of the real perpetrators is extremely difficult to determine.

It is also worth adding that the intensive increase in cross-border fraud has recently been significantly influenced by the COVID-19 pandemic and the related wider use of services provided electronically, as well as the widespread use of remote work by various companies, without appropriate IT security and without appropriate training. The increase in the number of cross-border fraud incidents is also influenced by the fact that banks are still slow to react to suspicious banking operations, in particular when these operations reference a contract or invoice number in the description.

It seems that the legislators in Poland have noticed the above-mentioned problems and have taken action to increase the effectiveness of the fight against cross-border fraud and cybercrime. One of the latest solutions introduced in Poland is the establishment of the Central Bureau for Combating Cybercrime within the police structure, which is responsible for the implementation of tasks in the area of recognising and combating crimes committed using an IT system, ICT system or ICT network, as well as preventing these crimes, as well as detecting and prosecuting the perpetrators of these crimes, and to support, to the extent necessary, organisational units of the Police in recognising, preventing and combating these crimes. The primary objective of this institution is therefore to identify threats and support citizens in preventing and combating cybercrime, including cross-border crime.

It should also be pointed out that while cooperation and legal assistance in combating cross-border fraud within the European Union works without major reservations and does not cause significant problems, when we are dealing with countries outside the European Union, this cooperation is more difficult, hence the urgent need to take appropriate action in this regard.

Jaroslaw Kruk
Founding Partner, KW Kruk & Partners Law Firm LP, Warsaw

Jaroslaw Kruk is highly experienced in the field of damage compensation and embezzled assets recovery, both in Poland and abroad. He is a specialist in implementing compliance programs, advises on cross-border fraud and asset tracing, money laundering and white-collar crime matters. Jaroslaw is a known and highly valued expert in the defence sector and state security, military equipment purchases, offset as well as public, utilities and defence procurement.

IPBA New Members December 2022 to February 2023

We are pleased to introduce our new IPBA members who joined our association from December 2022 to February 2023. Please welcome them to our organisation and kindly introduce yourself at the next IPBA conference.

Austria, Alice Meissner *Meissner & Passin Rechtsanwalts GmbH (MP – Attorneys GmBH)*	**China**, Zhang Meiping *Beijing Dhh Law Firm*
Bangladesh, A H M Belal Chowdhury *FM Consulting International*	**China**, Zhou Yarui *Dentons China LLP Suzhou Office*
Bangladesh, Tasmiah Nuhiya Ahmed *FM Associates*	**China**, Shaokai Chen
Belgium, Charles Buytaert *Janson*	**China**, Yuxing Ye *Zhonglun Law Firm*
Brazil, Cleber Venditti *Mattos Filho Advogados*	**China**, Zhenyong Ye *JunHe LLP*
Brazil, Min Gon Kim *Demarest Advogados*	**China**, Yan Mo *Nagashima Ohno & Tsunematsu Shanghai Office*
Cambodia, Tayseng Ly *HBS LAW*	**China**, Chen Chen *Guangzhou Arbitration Commission*
Chile, Javier Ceron *Cariola Diez Perez Cotapos*	**China**, Ping Yao *Zhong Lun Law Firm*
Chile, Tomas Andres Vidal Kunstmann *Cariola Diez Pérez-Cotapos*	**France**, Loic Colnat *COLNAT*
China, Yiping Chen *Jiangsu Ruilai Law Firm*	**France**, Paul Leconte *EFB*
China, Zhen Liu *Guantao Law Firm Tianjin Office*	**France**, Therese-Anne Amy *ARCADE AVOCAT*
China, Wen Li *Guantao Law Firm Tianjin Office*	**France**, Michinari Matsumoto *McDermott Will & Emery AARPI*
China, Xin Jin *W&H (Xi'an) Law Firm*	**France**, Isabelle Bouvier *Bouvier Avocats*
China, Kaitian Luo *Beijing Puran Law Firm*	**France**, Mitsuki Hirota *FERAL-SCHUHL SAINTE-MARIE WILLEMANT AARPI*
China, Hui Jia DeHeng Law Offices-Beijing	**France**, Richard Willemant *FERAL-SCHUHL SAINTE-MARIE WILLEMANT AARPI*
China, Wei Lin *P.C.Woo & Zhonglun W.D. LLP*	**France**, Zaïna Azzabi
China, Shengwei Du *Jiangxi Qizheng Wode Law Firm*	**France**, Alexandre Vagenheim *Jus Mundi*
China, Yunyun Yan	**France**, Pierre Pirouzan Parvine *Dentons*

France, Nahoko Amemiya	**Japan,** Fumihide Sugimoto *Nagashima Ohno & Tsunematsu*
Germany, Jasper Schedensack *Kadmos GmbH*	**Japan**, Yasuchika Fukuda *Miyake & Partners LPC*
Hong Kong, Mark John Stevens *Deacons*	**Japan**, Shinji Takakura *Kitahama Partners*
Hong Kong, Kathryn Weaver *Seyfarth Shaw LLP*	**Japan**, Jeff Schrepfer *Pillsbury Winthrop Shaw Pittman LLP*
Hong Kong, Teresa Cheng	**Japan**, Maya Ito *Nishimura & Asahi*
India, Sridhar Gorthi *Trilegal*	**Japan**, Axel Kuhlmann *Nagashima Ohno & Tsunematsu*
India, Shubhangi Garg *Shardul Amarchand Mangaldas & Co*	**Japan**, Takashi Ugajin *Ugajin International Law Firm*
India, Jyotsna Jayaram *Trilegal*	**Japan**, Masao Morishita *Nishimura & Asahi*
India, Nayantara Nag *Trilegal*	**Japan**, Ryoichi Kaneko *Anderson Mori & Tomotsune*
India, Anindya Ghosh *INDUSLAW*	**Japan**, Yuzuko Yamao *Creativity & Insight Legal Professional Corporation*
India, Shantanu Tyagi	**Japan**, Kenichi Tanizaki *Atsumi & Sakai*
India, Rajdutt Shekhar Singh *S&A Law Offices LLP*	**Japan**, Daiki Koso *TMI Associates*
India, Smita Singh *S&A Law Offices LLP*	**Japan**, Masato Tanaka *TMI Associates*
India, Humera Niyazi *Kochhar & Co.*	**Korea**, Hee Woong Yoon *Yulchon LLC*
India, Orijit Chatterjee *Fox Mandal & Associates LLP*	**Korea**, Eunjee Kim *Bae Kim and Lee*
India, Kunal Vajani *Fox & Mandal*	**Lithuania**, Laurynas Lukošiūnas *Advokatų Kontora Sorainen Ir Partneriai*
India, Reena Khair *Kochhar & Co.*	**Malaysia**, Ji En Lee *Chambers Lab*
Indonesia, Ichsan Montang *IM AND PARTNERS*	**Malaysia**, Aniz Amirudin *CECIL ABRAHAM & PARTNERS*
Indonesia, Pheo M Hutabarat *Hutabarat Halim Dan Rekan*	**Malaysia**, Kelvin Loh *Rahmat Lim & Partners*
Indonesia, Harris Toengkagie *Makarim & Taira S.*	**Malaysia**, Siong Sie Khong *Jason Teoh & Partners*
Indonesia, Stephanie Kandou *Makarim & Taira S.*	**Pakistan**, Altamash Faisal Arab *Vellani & Vellani*
Italy, Felice Ferrari *Chiomenti*	**Pakistan**, Ayeshah Alam *Vellani & Vellani*
Italy, Paolo Grandi *RP Legal & Tax*	**Pakistan**, Arzandah Bawany *Vellani & Vellani*

Pakistan, Aly Ahmed Bhamani
Vellani & Vellani

Pakistan, Zara Saba Tariq
Vellani & Vellani

Palestine, Rasem Kamal
Kamal & Associates

Philippines, Carl Ericson John Rodavia Dedace
The Lawfirm of Frederick G. Dedace

Poland, Katarzyna Kuzma
Domanski Zakrzewski Palinka Spolka Komand

Russia, Arkadiy Krasnikhin
Egorov, Puginsky, Afanasiev and Partners Law Offices

Russia, Andrey Mashkovtsev
Egorov, Puginsky, Afanasiev and Partners Law Offices

Russia, Evgeny Raschevsky
Law Offices Egorov,Puginsky, Afanasiev and Partners

Russia, Ilya Kuznetsov
Egorov, Puginsky, Afanasiev and Partners Law Offices

Russia, Sergey Kalinin
Egorov, Puginsky, Afanasiev and Partners Law Offices

Russia, Vladimir Talanov
Egorov, Puginsky, Afanasiev and Partners Law Offices

Singapore, Janice Ngeow
Dentons Rodyk & Davidson LLP

Singapore, Gerard Amann
Accenture

Singapore, Teck Wee Tiong
Wongpartnership LLP

Singapore, Patricia Ko
Nagashima Ohno & Tsunematsu Singapore

Singapore, Darius Chan
Breakpoint LLC

Sri Lanka, Shiara Sellamuttu
JOHN WILSON PARTNERS

Sweden, Mattias Larsson
Advokatfirman Fylgia KB

Switzerland, Anna Kozmenko
Schellenberg Wittmer

Taiwan, Joyce W Chen
Lee and Li, Attorneys-at-Law

Thailand, Emi Rowse (Igusa)
Kudun and Partners

Thailand, Mayuree Sapsutthiporn
Kudun and Partners

Thailand, Chaiwat Keratisuthisathorn
Tilleke & Gibbins International Ltd

Thailand, Frederic Favre
Vovan & Associes Co. Ltd

Turkey, Şafak Herdem
Herdem Attorneys At Law

Turkey, Ahmet Yaşar
Yaşar Law Office

United Arab Emirates, Abdulla Ziad Galadari
Galadari Advocates & Legal Consultants

United Arab Emirates, Anne K Hoffmann
Hoffmann Arbitration

United Arab Emirates, Abdus Samad
Afridi & Angell

United Arab Emirates, Saurbh Kothari
Afridi & Angell

United Arab Emirates, Anders Nilsson
Anders

United Arab Emirates, Gordon Blanke
Blanke Arbitration Fzco

United Arab Emirates, Piers Drysdale

United Arab Emirates, Avichal Prasad

United Arab Emirates, Carlyn Lobo
Kochhar & Co. Inc. Legal Consultants (Dubai Branch)

United Arab Emirates, Roshni Chadda
Kochhar & Co. Inc. Legal Consultants (Dubai Branch)

United Arab Emirates, Shweta Varier

United Arab Emirates, Diwakar Agarwal
Stephenson Harwood LLP

United Arab Emirates, Kokila Alagh
Karm Legal Consultants Pvt Ltd

United Arab Emirates, Philip Punwar
Outer Temple Chambers

United Kingdom, Nelson Goh
Pallas

United Kingdom, Adam Robb
39 Essex Chambers

United Kingdom, Hayata Matsunaga
Nagashima Ohno & Tsunematsu

United States, Evan Chuck
Crowell & Moring LLP

United States, Grigory Marinichev
Morgan, Lewis & Bockius LLP

Yemen, Abdulla Luqman
Luqman Legal

Members' Notes

Frédéric Dal Vecchio, France

Dr Frédéric Dal Vecchio, Attorney at law, Jurisdictional Council Member (France), Visiting Scholar at the University of Chulalongkorn (Bangkok) in 2019 and Lecturer at the Royal University of Law and Economics (RULE) in Phnom Penh since 2014, has published in January 2023 a fascicle on French ex officio taxation procedures, including international aspects, for the *JurisClasseur Tax Procedures Encyclopedia* published by LexisNexis.

Hak Jun Lee, New Zealand

Hak Jun Lee has joined Buddle Findlay as a Partner in the firm's Insolvency, Finance and Asia Business team in Auckland. Buddle Findlay is one of the leading commercial and public law firms in New Zealand, with offices in Auckland, Wellington and Christchurch, and a global reach of contacts and experience.

Hak Jun specialises in banking and financial services, real estate and overseas investment. Hak Jun has extensive experience assisting investors on financing, negotiating, structuring and securing regulatory approvals for transactions, as well as advising inbound investors on all regulatory requirements including Overseas Investment Office ('OIO') consent requirements. He also provides advice on a range of property matters including acquisitions and disposals, leasing, developments and subdivisions.

Stephan Wilske, Germany

Stephan Wilske published (together with Richard Happ) in November 2022 the book *ICSID Rules and Regulations 2022—Article-by-Article Commentary*. This first (and so far only) commentary on the ICSID Arbitration Rules 2022 was presented at book launch events in London, Paris, Washington, D.C. (at the ICSID headquarters) and New York.

Engage your stakeholders

Investor communications

Annual reports

Sustainability reports

In-house newsletters

Professional magazines

Copywriting

ninehills media

T: +852 3796 3060

E: enquiries@ninehillsmedia.com

W: www.ninehillsmedia.com

Labuan IBFC
International Business and Financial Centre, Malaysia

LABUAN IBFC
ASIA'S PREMIER INTERNATIONAL FINANCIAL HUB

Labuan International Business and Financial Centre (Labuan IBFC), located off the North West coast of Borneo, offers global investors and businesses the benefits of being in a well-regulated jurisdiction that provides fiscal, legal and currency neutrality, in addition to being an ideal location for cost-efficient substance creation.

Labuan IBFC is a wholesale financial, risk and wealth management intermediation centre that also boasts a wide range of business structures including solutions for fintech or digital businesses. It is also home to the world's first sukuk and is acknowledged as an Islamic financial hub.

Well-supported by a robust, internationally recognised yet business-friendly legal framework, Labuan IBFC operates within comprehensive legal provisions and guidelines, enforced by a single regulator, Labuan Financial Services Authority – a statutory body under the Ministry of Finance, Malaysia.

Labuan, also known as the 'Pearl of Borneo', offers a myriad of business and leisure opportunities. It is also a hub for financial tourism as its excellent location and compact structure offer easy connectivity between the financial district, and nature offerings.

Labuan IBFC Inc. Sdn. Bhd. (817593-D)
Suite 3A-2, Level 2, Block 3A,
Plaza Sentral, Jalan Stesen Sentral,
KL Sentral, 50470 Kuala Lumpur, Malaysia
Tel: +603 2773 8977
Fax: +603 2780 2077
Email: info@LIBFC.com
@LabuanIBFC
Labuan IBFC

www.LABUANIBFC.com