ICC FraudNet
COMMERCIAL CRIME SERVICES
est. 2004

GLOBAL REPORT 2021

International Developments and
Perspectives in the field of
Fraud, Financial Crime and Asset Recovery

Acknowledgments

Many individuals and organisations have been of great assistance in the writing, editing and production of the inaugural FraudNet Global Report. The Editor first wishes to thank FraudNet's Members and Strategic Partners who have authored and co-authored articles for inclusion in this publication, as well as their colleagues and staff who have assisted them. FraudNet's unparalleled international reach and subject expertise in fraud and asset recovery are well captured in this Report, and it is testament to the collective energy of the group that such wide-ranging insights were provided for this Report from so many countries, particularly in these unprecedented times.

The Editor secondly wishes to thank Mr Peter Lowe, Executive Secretary of FraudNet for his support from the inception of this project right through to publication. His operational assistance, and acute understanding of the expertise and resources available within FraudNet has been greatly valued during the collation of papers. Further thanks are owed to Mr Michele Caratsch and Mr Babajide Ogundipe for their help throughout the strategic stages, and work in convening and being part of, along with Mr Peter Lowe, a very supportive Editorial Board. The Editor wishes to thank all members of the Editorial Board – Mr Bobby Banson, Mr Shaun Reardon-John, Mr Rodrigo Callejas, Mr Waseem Azzam, Mr Christopher Redmond and Mr John Greenfield – for their time, guidance and energy for this project. Gratitude is also extended to Mr Bruce Horowitz, whose support as an Assistant Editor has been significantly valued during the review and editorial stages, and also Mr Andrew Witts for his guidance.

Finally, the Editorial Board wishes to thank all Members, Strategic Partners and Staff of FraudNet for their continued support and collaboration in making this Report possible.

Contents

Foreword

This, the first FraudNet Global Report emerged from discussions of members at our Beirut meeting in October 2019. Following the decision to elect us as co-Executive Directors, members may have thought that we had to be kept busy. One of the things that emerged were thoughts about the need to develop a more academic element to the network. Given that the focus of our members is more practical in nature, aimed at providing results for clients, this was a move in a slightly different direction. Consideration was given to participating in programmes with educational institutions, and this thinking resulted in a meeting in January 2020 with Professor Barry Rider OBE, the Founder of the annual Cambridge International Symposium on Economic Crime and sometime Fellow, Dean and Tutor of Jesus College, Cambridge, amongst his many accomplishments. At the time, the existence of a new disease reported to have originated in Wuhan, China, was known, but nobody at that meeting had any notion of what was to come.

Professor Rider introduced us to Dr Dominic Thomas-James, who agreed to be the Editor of a journal that would feature articles on developments related to our practice areas from our members and Strategic Partners, as well as from leading academics engaged in research relating to economic crime, risk, financial regulation and compliance, and who were authors of key academic texts in the field.

The explosion of the new disease into something that left no part of the world untouched was not foreseen. Had it not occurred, this Report would nevertheless have been produced. The pandemic prevented FraudNet members, Strategic Partners and invited guests from meeting in Nairobi and Miami in 2020. Had we been able to hold these meetings, doubtless some of the material contained here would have been shared there. Whilst the Report did not come about as a result of the pandemic, what we are experiencing most certainly influenced some of its contents. The certification of vaccines, which started in December 2020, holds out hope that the fears, restrictions and risks related to travel will have dissipated by the time the 2022 Report is published.

We thank all the contributors, not just for providing such valuable material, but for doing so in good time and thereby relieving the Editor of chasing them holding a big stick. This augurs well for future editions.

Case Study of the Coincheck Cryptocurrency Hack: a Major Japanese Cryptocurrency Exchange Lost "NEM" Worth USD 530 million due to Cyber-Attack

Hiroyuki Kanae & Hidetaka Miyake

Abstract

In this article Hiroyuki Kanae and Hidetaka Miyake discuss, by reference to a case study, a significant cyber-attack in Japan. The case discussed in this article is the biggest cyber-attack of a cryptocurrency exchange to date and new challenges and developments are observed in Japan to address various issues raised in the case. This article touches upon some of the new challenges and developments in the areas of asset recovery, criminal enforcement, regulatory actions and class action. Although enormous efforts have been made by government agencies and other stakeholders, no criminal enforcement or regulatory or class action has been brought against the cyber-attackers thus far and no asset has been recovered from them. In the meantime, the Japanese authorities strengthened the regulations on cryptocurrency exchange business in response to this incident. This case illustrates the importance of criminal enforcement and asset recovery for growth of a new market of cryptocurrency business.

Case Summary

Coincheck, Inc. ("Coincheck"), one of Japan's leading cryptocurrency exchange service providers, suffered a cyber-attack on 26 January 2018. During this attack, a cryptocurrency called "NEM" which was held by Coincheck was illegally transferred outside the company by the attackers. As a result, Coincheck's customer assets suddenly disappeared. Anonymous hackers appeared to have spread malware and penetrated Coincheck's internal network via employees' infected personal computers. The value of stolen "NEM" was 54.7 billion yen at that time. This case is the biggest cyber-attack of a cryptocurrency exchange to date, surpassing the US$460 million attack on Mt. Gox in 2014. It is generally acknowledged that this huge loss of customer assets was caused not by a problem with the NEM cryptocurrency itself, but rather by Coincheck's weak security system. Coincheck's major security weakness was that it did not manage customer assets in an off-line "Cold Wallet". As a result, about 260,000 customers' NEM wallets were hit by the cyber-attack, which

forced the Japanese government and financial regulators to fundamentally strengthen their regulations on cryptocurrency exchanges and related security protocols.

Asset Recovery

It was an extremely difficult proposition to track down and recover the stolen cryptocurrency. In February 2018, a website suddenly appeared in a group of anonymous sites that require special software to access called the "Dark Web". This site offered to exchange bitcoin and other cryptocurrencies for NEM at a discount relative to the normal market price. This website is believed by experts to have been set up by the hackers involved in the attack on Coincheck. Accordingly, many people made purchases from that website, and it is likely that almost all of stolen NEM was exchanged for other currencies by March 2018.

In the meantime, Coincheck announced on 27 January 2018 that it intended to compensate its customers for their stolen NEM. As a result, Coincheck eventually paid a total of 46 billion yen on 12 March 2018 to its customers who held NEM as of 26 January 2018, taking into account the decline in NEM's market value over that period.

Criminal Enforcement

The Tokyo Metropolitan Police Department (the 'TMPD') set up a special investigation team of around one hundred highly experienced cybercrime specialists within the Cyber Crimes Division to investigate the Coincheck case. These criminal investigators have been trying to charge the hackers involved in the attack on Coincheck with the violation of the Unauthorized Computer Access Law. However, thus far no criminal charges have been brought against the attackers by the public prosecutor.

In April 2020, as a result of the investigation by the above-mentioned Cyber Crimes Division of the TMPD, the public prosecutor of the Tokyo District Public Prosecutors Office brought criminal charges against two Japanese suspects for accepting criminal proceeds, as prohibited under the Act of Punishment of Organized Crimes, Control of Crime Proceeds and Other Matters (the 'Organized Crime Punishment Act'). According to the indictment from the public prosecutor and other information, the two suspects are alleged to have purchased large quantities of NEM between February and March 2018 at low prices through an automated trading program that made many high-speed transactions in a short period of time. The accused allegedly knew that the NEM that they were purchasing was stolen from Coincheck. The two suspects also allegedly exchanged the stolen NEM for another cryptocurrency and, as a result, made a profit of billions of yen. One of the two suspects has pleaded not guilty and the criminal trials of both accused are still ongoing.

Over the course of the investigation into the Coincheck case, criminal investigators used a new tool to freeze the assets of one of the above-mentioned criminal suspects. In response to the TMPD's request, the Tokyo District Court issued, on 30 March 2020, a protective order for confiscation against a company managed by one of those criminal suspects. This order was issued prior to the public prosecutor's indictment under the Organized Crime Punishment Act. This was the first time a pretrial protective order for confiscation under the Organized Crime Punishment Act was issued in Japan. Any property obtained through criminal acts or obtained as remuneration for

criminal acts may be subject to confiscation and, if a protective order for confiscation is issued, criminal suspects will be prevented from disposing of such property even before the public prosecutor's indictment and the commencement of a criminal trial.

Regulatory Actions

Due to the fact that the legal status of Bitcoin and other cryptocurrencies were unclear under Japanese law, and that there were no clear regulations on cryptocurrency exchange service providers, the Japan Financial Services Agency (the 'JFSA') introduced the amended Payment Services Act, which came into force in April 2017. The amended Payment Services Act introduced a new registration requirement for "cryptocurrency exchange service providers". However, as a transitional measure, service providers that had been operating before the enactment of the amended Payment Services Act were categorized as "deemed cryptocurrency exchange service providers". These deemed providers were allowed to continue their business subject to the new regulations if they applied for registration. At the time of the incident on 26 January 2018, Coincheck was still undergoing the process of completing their registration. Therefore, the company was still a deemed cryptocurrency exchange service provider.

In response to the incident, financial regulators immediately issued a business improvement order against Coincheck on 29 January 2018. In addition, the JFSA commenced an on-site inspection of Coincheck on 2 February 2018. On 8 March 2018, another business improvement order was issued against Coincheck, calling for the fundamental restructuring of its management system and strategy, as well as other measures to ensure proper business operations. In addition, the JFSA also issued administrative orders on 2 February 2018 against other service providers to submit reports on their risk management systems.

As of 12 September 2018, the financial regulators issued business suspension orders and business improvement orders against ten deemed cryptocurrency exchange service providers, as well as seven registered cryptocurrency exchange service providers. As a result, more than a dozen deemed cryptocurrency exchange service providers withdrew their applications for registration. The Coincheck case had a significant negative impact on the cryptocurrency exchange market in Japan, which was otherwise expected to grow under the new regulations. Eventually, Coincheck became a wholly owned subsidiary of Monex Group, a major online financial institution, in April 2018 and subsequently completed its registration as a cryptocurrency exchange service provider in January 2019.

The JFSA further amended the Payment Services Act and other legislation to strengthen regulations surrounding cryptocurrency. These new amended regulations came into force in May 2020 and (among other measures) changed the legal term from "virtual currency/cryptocurrency" to "crypto asset".

Class action

Between 26 and 27 February 2018, Coincheck customers filed a series of lawsuits seeking the return of their cryptocurrency assets. As of the 27 of February 2018, a total of 144 Coincheck customers had filed lawsuits. Since then, the number of plaintiffs has gradually increased, and it is

estimated (case records are not disclosed to outside non-interested parties in Japan) that nearly 200 plaintiffs have filed lawsuits.

These civil suits have sought damages for (i) the difference between the Coincheck's discretionary compensation and the price of NEM at the time of the cyber-attack, and (ii) the amount that the price of cryptocurrencies deposited by customers in Coincheck had declined by during the suspension of trading of the assets (including 11 virtual currencies other than NEM). Losses to customers were caused by the decline in the value of NEM and many other virtual currencies because Coincheck suspended trading of all virtual currencies for a period of time after the NEM cyber-attack. The main issue in the case is whether the difference between the NEM price at the time of the attack and the amount that Coincheck voluntarily compensated can be awarded as damages.

In these lawsuits, the plaintiffs (Coincheck's customers) sought, from the Toyko District Court, a document production order on a report submitted to the FSA by the defendant (Coincheck). The plaintiffs intend to use this report to prove that the defendant was negligent while in custody of the plaintiffs' virtual currencies. In response, on November 11 2019, the Tokyo District Court issued a ruling to "dismiss the petition". This meant that no order was issued against Coincheck to produce reports and other documents filed with the JFSA and the Kanto Local Finance Bureau.

In its decision, although the Court accepted the plaintiff's arguments that (1) Coincheck is the holder of the documents (i.e. the reports, etc. submitted to the JFSA, etc.), (2) the subject documents had been identified by the plaintiffs, and (3) there is a need to examine the evidence, the Court concluded that the contents of the reports, etc. would "undermine the relationship of trust between the supervisory authorities and Coincheck, thereby impeding the fair and smooth operation of public services" if they were to be made public. Accordingly, the Court did not order Coincheck to produce the reports, etc. submitted to the JFSA, etc. pursuant to Article 220, item (iv), (b) of the Code of Civil Procedure.

On November 15, 2019, the plaintiffs' counsel filed an immediate appeal (i.e. procedures for filing an objection) against the Tokyo District Court's decision. As a result, the Tokyo High Court will determine whether or not to order the production of documents. Unlike in the United States and elsewhere, there is no system for discovery in Japanese civil suits. Therefore, it is extremely difficult for the plaintiffs to present evidence in court and, accordingly, prove the defendant's negligence. Since more than two years have passed since the filing of these lawsuits, it is expected that the outcome of these civil suits will be unfavorable for the plaintiffs.

Conclusion

In conclusion, after almost three years of asset recovery efforts against the cyber-attackers involving Coincheck, one of the major cryptocurrency exchange service providers, they have faced numerous obstacles due to the difficulty of identification of such attackers and cross-border impediments. Further, although more than one hundred cybercrime specialists of the TMPD have investigated the incident and the cyber-attackers, law enforcement authorities could not identify the attackers and recover the stolen cryptocurrencies. While the JFSA issued a number of rules and guidelines for the strict enforcement on the security requirements on the cryptocurrency exchange service providers, once the cyber-attackers hacked the network sysem and conveyed the cryptoassets into other locations, it is almost impossible to trace and recover such assets from the attackers. Therefore, for

now the cryptocurrency exchange service providers should make every exertion on the strict security measures and the training of their employees to avoid any loopholes for cyber-attackers.

About the Authors

Hiroyuki Kanae has more than 30 years' experience in the cross-border litigation. He has served as a corporate auditor of a premier international logistic company since 2012 and advises the management with the corporate governance and legal matters surrounding the international business. He focuses on commercial litigation matters, including domestic and cross-border litigations involving major Japanese and foreign companies. He has been advising on the global asset recovery projects involving Japanese clients in USA, Asia Pacific and Europe. He has represented trustees in bankruptcy proceedings in Japan, in pursuing successful asset recovery in the United States.

Hidetaka Miyake is one of the leading lawyers in the fields of government investigations and crisis management in Japan. By leveraging his background as a former public prosecutor, a former senior investigator at the Securities and Exchange Surveillance Commission and a former forensic senior manager of a Big Four accounting firm, he focuses on handling internal or independent investigations for listed companies to address complex accounting frauds. He also handles crisis management for financial institutions and criminal defense for non-Japanese clients. Since joining Anderson Mori & Tomotsune in 2017, he has been involved in accounting fraud investigations for more than 12 Japanese listed companies.

Hiroyuki Kanae
Anderson Mori & Tomotsune
T. +81-3-6775-1011
E. hiroyuki.kanae@amt-law.com

Hidetaka Miyake
Anderson Mori & Tomotsune
T. +81-3-6775-1121
E.hidetaka.miyake@amt-law.com

ANDERSON MŌRI & TOMOTSUNE

ICC FraudNet Strategic Partners

ICC Commercial Crime Services

Cinnabar Wharf
26 Wapping High Street
London
E1W 1NG
United Kingdom

Phone: +44 (0) 20 7423 6960
Fax: +44 (0) 20 7423 6961
Email: fraudnet@icc-css.org
Web: www.icc-css.org/home/fraudnet

FraudNet was founded in 2004 and operates under the auspices of ICC Commercial Crime Services – the anti-crime arm of the International Chambers of Commerce (ICC), the Paris based world business organization with offices in more than 90 countries.