

NHÓM CHÂU Á- THÁI BÌNH DƯƠNG VỀ CHỐNG RỬA TIỀN

BÁO CÁO MÔ HÌNH THƯỜNG NIÊN APG NĂM 2019

**CÁC PHƯƠNG THỨC VÀ XU HƯỚNG RỬA TIỀN VÀ
TÀI TRỢ KHỦNG BỐ**

2019

Tháng 8/2019

BÁO CÁO MÔ HÌNH THƯỜNG NIÊN APG NĂM 2019

Đơn xin phép tái bản toàn bộ hoặc một phần ấn phẩm này phải được gửi đến:

Ban thư ký APG

Locked Bag A3000

Sydney South

New South Wales 1232

AUSTRALIA

Điện thoại: +61 2 9277 0600

Email: mail@apgml.org

Web: www.apgml.org

© Tháng 8/ 2019/Bản quyền

PHẦN GIỚI THIỆU.....	5
1. CÁC HỘI THẢO VÀ DỰ ÁN DO APG TIẾN HÀNH NĂM 2018 - 2019.....	6
1.1 Các dự án mô hình của APG	6
1.2 Hội thảo xây dựng năng lực và mô hình chung giữa APG và EAG năm 2018	6
2. CÁC DỰ ÁN MÔ HÌNH CỦA FATF VÀ CÁC TỔ CHỨC KHU VỰC DẠNG FATF.....	7
2.1 Các dự án mô hình của FATF	7
2.2 CFATF – Lực lượng đặc nhiệm tài chính vùng vịnh Caribe.....	9
2.3 EAG – Nhóm Á Âu về chống rửa tiền và tài trợ khủng bố.....	10
2.4 GIABA – Nhóm hành động liên Chính phủ chống rửa tiền tại Tây Phi	11
2.5 Nhóm Egmont.....	11
3. XU HƯỚNG RỬA TIỀN VÀ TÀI TRỢ KHỦNG BỐ.....	13
3.1 Nghiên cứu hoặc bài viết về các phương thức và xu hướng ML/TF được các thành viên và quan sát viên APG thực hiện.	13
3.2 Sự kết hợp giữa các loại hoạt động ML hoặc TF với các hoạt động phạm tội tiền thân	19
3.3 Xu hướng mới nổi; xu hướng giảm dần; xu hướng tiếp tục.....	23
4. CÁC VỤ VIỆC ĐIỂN HÌNH VỀ ML VÀ TF	30
4.1 Tài trợ khủng bố	30
4.2 Sử dụng ngân hàng hải ngoại, công ty kinh doanh quốc tế và tín thác hải ngoại	32
4.3 Sử dụng tiền ảo	34
4.4 Sử dụng các dịch vụ chuyên nghiệp (luật sư, công chứng viên, kế toán viên)	37
4.5 Rửa tiền trên cơ sở thương mại và chuyển giá.....	39
4.6 Hệ thống chuyển tiền ngầm/Các dịch vụ chuyển tiền khác/Hawala	47
4.7 Sử dụng internet (mã hóa, truy cập qua ID, chuyển tiền quốc tế, etc.)	49
4.8 Sử dụng hệ thống hoặc phương pháp thanh toán mới.....	51
4.9 Rửa tiền thu được từ hoạt động trốn thuế.....	53
4.10 Bất động sản, bao gồm cả vai trò của các công ty Bất động sản.....	57
4.11 Liên quan đến nạn buôn người trái phép.....	58
4.12 Sử dụng người đại diện, lạm dụng tín nhiệm, thành viên trong gia đình hoặc bên thứ ba	59
4.13 Các hoạt động đánh bạc (sòng bạc, đua ngựa, đánh bạc qua mạng ...)	64
4.14 Mingling (Đầu tư kinh doanh) và gian lận đầu tư	67
4.15 Sử dụng công ty/tổ chức bình phong.....	68
4.16 Đổi tiền/ chuyển đổi tiền mặt	73
4.17 Buôn lậu tiền tệ.....	75
4.18 Sử dụng thẻ tín dụng, séc, kỳ phiếu, v.v.....	77
4.19 Cơ cấu (lẩn giấu)	79

4.20 Chuyển tiền điện tử/ sử dụng các tài khoản ngân hàng ở nước ngoài.....	81
4.21. Trao đổi hàng hóa (trao đổi – ví dụ: tái đầu tư vào thuộc phiên bất hợp pháp)	82
4.22 Sử dụng nhận dạng, tài liệu giả mạo	82
4.23 Kim loại quý, đá quý	83
4.24 Mua tài sản có giá trị (sản phẩm nghệ thuật, đồ cổ, ngựa đua...)	84
4.25 Đầu tư vào thị trường vốn, sử dụng môi giới	85
4.26 Các trường hợp được phát hiện trực tiếp từ các báo cáo giao dịch đáng ngờ hoặc giao dịch vượt ngưỡng.....	85
5. ẢNH HƯỞNG CỦA CÁC BIỆN PHÁP ĐỐI KHÁNG VỀ AML/CFT	91
5.1 Tác động của việc cải thiện khuôn khổ pháp luật hoặc quản lý đến việc phát hiện và / hoặc ngăn ngừa các phương thức cụ thể	91
6. CÁC TỪ VIẾT TẮT VÀ THUẬT NGỮ'	95

PHẦN GIỚI THIỆU

Lời tựa

1 Nhóm Châu Á- Thái Bình Dương về chống rửa tiền (APG) là tổ chức chống rửa tiền và chống tài trợ khủng bố trong khu vực Châu Á/ Thái Bình Dương. APG phát hành những báo cáo mô hình khu vực về các phương thức rửa tiền và tài trợ khủng bố (ML/TF) nhằm hỗ trợ các chính phủ và các cơ quan AML/CFT khác hiểu hơn về bản chất của những mối nguy cơ ML/TF hiện hữu và mới nổi; đồng thời đảm bảo những chiến lược hiệu quả nhằm giải quyết những mối đe dọa đó. Những nghiên cứu mô hình giúp cho các thành viên APG thực hiện các chiến lược hiệu quả nhằm điều tra và truy tố những hành vi ML/TF, cũng như đưa ra và thực hiện các biện pháp phòng ngừa hiệu quả. Khi một loạt những hành vi ML/TF được thực hiện giống nhau hoặc sử dụng những phương thức như nhau, chúng thường được phân loại như những mô hình.

2 APG tiến hành nghiên cứu mô hình có hợp tác với Lực lượng đặc nhiệm tài chính (FATF) và các đối tác khác trong mạng lưới chống rửa tiền và chống tài trợ khủng bố. Điều này bao gồm cả những dự án chung và phối hợp sau dự án về những lĩnh vực được ưu tiên trong khu vực và trên thế giới.

3 Việc phát hành Báo cáo Mô hình thường niên của APG được thực hiện theo Kế hoạch chiến lược của APG và Điều khoản tham chiếu về Ủy ban hoạt động của APG và bao gồm những khái quát về phương thức và kỹ thuật ML/TF. Những báo cáo này nhằm mục tiêu hỗ trợ cho các thành viên APG xác định được những hoạt động tài chính đáng ngờ. Những vụ việc và dấu hiệu trong báo cáo này giúp cho các tổ chức tài chính và các tổ chức cũng như ngành nghề phi tài chính chỉ định (sòng bạc, kế toán viên, luật sư, tín thác, các tổ chức cung ứng dịch vụ công ty, các đại lý bất động sản,...) phát hiện và chống ML/TF.

4 Hàng năm, các thành viên và quan sát viên APG cung cấp thông tin về các vụ việc ML/TF, các xu hướng, những nghiên cứu cũng như hoạt động quản lý, hợp tác quốc tế. Những thông tin thu thập được không những chỉ cung cấp cơ sở cho việc tổng hợp các vụ việc mà còn cho sự lựa chọn và thiết kế cho những nghiên cứu sâu hơn về những chủ đề cụ thể đặc biệt. Thông tin cũng hỗ trợ cho công việc của mạng lưới các chuyên gia tham gia vào công tác mô hình của APG.

5 Những vụ việc nêu trong báo cáo này không chỉ là một phần nhỏ của công việc trong khu vực Châu Á- Thái Bình Dương và những khu vực khác nhằm phát hiện và chống ML/TF. Nhiều vụ việc không thể được chia sẻ công khai do bản chất nhạy cảm của chúng hoặc đang trong quá trình điều tra, tố tụng. Báo cáo này bao gồm tập hợp những vụ việc thể hiện các mô hình khác nhau từ các báo cáo của các thành viên và từ các nguồn công khai. Một vài vụ việc được đưa vào báo cáo này đã xảy ra trong những năm trước đó nhưng thông tin tóm tắt được đưa ra trong năm nay.

Các mô hình trong giai đoạn 2018-2019

6. APG thực hiện công tác mô hình của mình thông qua Ủy ban hoạt động APG, hiện do Ấn độ và Niu Zi-lân làm Đồng Chủ tịch.

1. CÁC HỘI THẢO VÀ DỰ ÁN DO APG TIẾN HÀNH NĂM 2018 - 2019

1 Phần này của báo cáo cung cấp cái nhìn tổng quan về các mô hình liên quan đến công việc mà APG thực hiện từ tháng 7/2018 đến tháng 6/2019.

1.1 Các dự án mô hình của APG

Dự án buôn lậu/ chuyển lậu người (Giai đoạn 2)

2 Giai đoạn 1 của Dự án là dự án chung giữa APG với FATF tập trung vào buôn người và đã kết thúc tháng 7/2018 (xem phần sau của báo cáo này: Các dự án mô hình của FATF/ Các dự án mô hình của FATF và các tổ chức dạng FATF)

3 Giai đoạn 2 là dự án khu vực APG được xây dựng trên cơ sở Giai đoạn 1, tập trung vào Buôn người (HT) và chuyển lậu người (PS). Dự án này tập trung vào việc thực hiện hỗ trợ kiểm soát cả HT và PS, bao gồm cả sự phối hợp giữa khu vực công và tư cũng như xã hội dân sự.

4 Một hội thảo khu vực về HT và PS đã được tổ chức tại Bandung, Indonesia từ ngày 8 đến 10/4/2019, tập trung vào việc thực hiện liên kết khu vực công/ tư/ xã hội dân sự nhằm chống nạn HT và PS. Hội thảo do APG và PPATK, AUSTRAC đồng chủ trì và đã có 64 đoàn đại biểu đến từ 12 nước, các tổ chức quốc tế, khu vực tư nhân, các tổ chức phi chính phủ và xã hội dân sự tham dự. Dự án này sẽ kết thúc vào năm 2020.

TF và những khoản thu phạm tội (bao gồm cả tội phạm có tổ chức)

5 Nhóm Á- Âu về chống rửa tiền (EAG) and APG hiện đang tiến hành dự án chung nhằm tập trung vào các kỹ thuật và xu hướng gắn với việc sử dụng các khoản thu tội phạm, bao gồm cả từ tội phạm có tổ chức, nhằm tài trợ cho khủng bố, cho dù đó là các nhân hay tổ chức khủng bố (xem phần sau trong báo cáo này: EAG – Nhóm Á- Âu về chống rửa tiền và chống tài trợ khủng bố)

1.2 Hội thảo xây dựng năng lực và mô hình chung giữa APG và EAG năm 2018

6 Hội thảo mô hình APG hàng năm có sự tham dự của những người có kinh nghiệm thực tiễn trong AML/CFT từ các cơ quan điều tra, truy tố, các đơn vị tình báo tài chính (FIU), các nhà quản lý, các cơ quan hải quan và các cơ quan khác nhằm xem xét những rủi ro và nguy cơ ML/TF hàng đầu của khu vực.

7 Hội thảo mô hình năm 2018 do APG và EAG đồng chủ trì tại Novosibirsk, Liên bang Nga từ ngày 3 đến 5/12/2018 thu hút sự tham gia của khoảng 250 đại biểu đến từ 41 nước APG/EAG (với khoảng 130 đại biểu từ các thành viên APG), 8 tổ chức quốc tế và 21 đại diện từ khu vực tư nhân, các tổ chức phi chính phủ và xã hội dân sự.

8 Hội thảo gồm phiên toàn thể (ngày đầu và ngày cuối) và 3 phiên 2 ngày về: (i) TF và những khoản thu phạm tội (bao gồm cả tội phạm có tổ chức); (ii) rủi ro và các kỹ thuật điều tra gắn với tài sản ảo; và (iii) HT và PS.

2. CÁC DỰ ÁN MÔ HÌNH CỦA FATF VÀ CÁC TỔ CHỨC KHU VỰC DẠNG FATF

9 Phần này của báo cáo cung cấp cái nhìn tổng quan về các báo cáo mô hình đã được FATF và các tổ chức khu vực dạng FATF phát hành từ tháng 7/2018 đến tháng 6/2019.

2.1 Các dự án mô hình của FATF

Những luồng tài chính chu chuyển từ hoạt động buôn người- HT (Giai đoạn 1)

10 Trong những năm qua, số nạn nhân của hoạt động HT và vận chuyển người nhập cư trái phép gia tăng đáng kể. Tháng 8/2018, FATF và APG đã đưa ra một báo cáo nhằm cảnh báo về loại thông tin tài chính có thể xác định hoạt động HT nhằm mục đích lạm dụng tình dục hoặc lao động ép buộc và nhằm cảnh báo về khả năng buôn lậu tạng nhằm kiếm lời. Báo cáo cũng đã nhấn mạnh đến những mối liên kết có thể có giữa HT và TF.

11 Báo cáo đã nhấn mạnh đến tầm quan trọng của việc xây dựng mối tương tác giữa khu vực công, tư, xã hội dân sự và cộng đồng phi lợi nhuận nhằm chia sẻ kinh nghiệm, tăng cường năng lực và hợp tác. Đặc biệt, khu vực tư nhân và các tổ chức tài chính nằm trên tuyến đầu.

12 Những sáng kiến ở cấp nước và khu vực đã cho thấy các biện pháp AML/CFT, và cả những người đã thực hiện chúng, có thể góp phần chặn đứng loại tội phạm này. Tuy nhiên, vẫn chưa đủ sự tập trung một cách có hiệu quả vào việc làm thế nào sử dụng được các thông tin tài chính để phát hiện, chặn phá và lật tẩy những mạng lưới buôn người. Báo cáo này đưa ra những thực tiễn tốt nhất giúp cho các nước phát triển những biện pháp nhằm giải quyết vấn đề ML/TF từ buôn người và đưa ra những dấu hiệu đỏ giúp xác định được những người đang rửa những khoản thu từ các loại tội phạm này.

Tính minh bạch và chủ sở hữu hưởng lợi

13 Trong khi các cỗ máy kinh doanh như các công ty, các quỹ, các liên danh hay các loại hình tổ chức pháp nhân hay thỏa thuận pháp lý hết sức quan trọng hỗ trợ cho các hoạt động kinh doanh và thương mại, thì chúng cũng có thể bị lạm dụng để che giấu quyền sở hữu và kiểm soát những tài sản kiếm được một cách bất hợp pháp. Tháng 7/2018, FATF và Nhóm Egmont đã đưa ra một báo cáo đánh giá về tính dễ bị tổn thương gắn với việc che giấu chủ sở hữu hưởng lợi nhằm hỗ trợ cho những phân tích rủi ro sâu hơn của khu vực công và khu vực tư.

14 Báo cáo sử dụng 100 vụ việc được 34 nước trong mạng lưới AML/CFT toàn cầu cung cấp, kinh nghiệm từ lực lượng thực thi pháp luật và các chuyên gia khác, có sự đóng góp của khu vực tư nhân cũng như nghiên cứu từ các nguồn mở và các báo cáo thông tin tình báo nhằm xác định các phương thức mà tội phạm đã sử dụng nhằm che giấu quyền sở hữu hưởng lợi. Tính dễ bị tổn thương gắn liền với tính sở hữu hưởng lợi được phân tích, được đặc biệt chú trọng đến sự tham gia của các trung gian chuyên nghiệp.

15 Báo cáo nhấn mạnh rằng, sự dễ dàng khi các pháp nhân, chủ yếu là các công ty trách nhiệm hữu hạn (hoặc tương đương) có thể được thành lập đã khiến chúng trở nên đặc biệt dễ bị tổn thương và thực tế được sử dụng để dựng nên những cấu trúc sở hữu hợp pháp phức tạp, thường là các công ty ma. Hơn nữa, các nhà cung cấp dịch vụ công

ty và tín thác thường xuyên giữ vai trò trong việc chuẩn bị dựng nên những cấu trúc này. Việc sử dụng các giám đốc và cổ đông được chỉ định, cả chính thức lẫn không chính thức, đã làm tăng thêm mức độ rủi ro bằng cách tạo ra những rào cản giữa cá nhân haowcj chủ sở hữu với những khoản thu được rửa. Những trung gian chuyên nghiệp thường giữ vai trò trợ giúp tạo ra hoặc vận hành các cấu trúc được sử dụng để che đậy chủ sở hữu hưởng lợi, hoặc theo cách đồng phạm, hoặc không có chủ tâm.

Rửa tiền chuyên nghiệp

16 Những kẻ rửa tiền chuyên nghiệp (PMLs) cung cấp dịch vụ cho tội phạm và các nhóm tội phạm có tổ chức bằng cách rửa các khoản thu từ hoạt động bất hợp pháp của chúng. Tháng 7/2018, FATF đã công bố một báo cáo nghiên cứu về những kỹ thuật và công cụ mà PMLs đã sử dụng nhằm hỗ trợ các nước xác định và vạch mặt chúng. Dựa trên những vụ việc nghiên cứu được đưa ra trong mạng lưới toàn cầu của FATF, báo cáo đã xác định được phạm vi các tổ chức và mạng lưới rửa tiền khác nhau, từ mạng lưới vận chuyển tiền và kiểm soát tiền mặt cho đến mạng lưới đại diện.

17 Báo cáo phát hiện ra rằng PMLs sử dụng nhiều kỹ thuật và công cụ rửa tiền như: rửa tiền trên cơ sở thương mại, cơ chế quản lý tài khoản, hoạt động ngân hàng ngầm và những kênh chuyển tiền thay thế. Để khoắc vẽ hợp pháp lên những hoạt động của mình, những PMLs có thể làm việc với những cá nhân bị mua chuộc, những người này chuyên cung cấp những dịch vụ hợp pháp (tức là, các nhân viên ngân hàng, các luật sư, kế toán viên) bên cạnh hoạt động phạm tội rửa tiền của họ. PMLs thường làm việc với nhiều hơn 1 kẻ phạm tội hoặc 1 nhóm tội phạm. Một vụ truy tố thành công một kẻ PML vì vậy có thể ảnh hưởng tới hoạt động của hàng loạt nhóm khách hàng tội phạm.

18 Một nhóm dự án cũng đã phát triển một dạng báo cáo không công khai khám phá những kỹ thuật và công cụ điều tra độc nhất đã được chứng minh là hiệu quả trong việc phát hiện và triệt phá những PMLs.

Chiến lược trấn áp tài trợ khủng bố (không công khai)

19 Vào tháng 10/2018, FATF đã thông qua một báo cáo không công khai về việc ngăn chặn những luồng tiền TF. Hiểu những dòng chảy tài chính này là quan trọng không chỉ dưới góc độ điều tra mà còn để đảm bảo rằng các cơ quan có thể có những biện pháp cương quyết, phòng ngừa để ngăn chặn được hoạt động khủng bố trước khi vụ tấn công khủng bố xảy ra.

20 Xây dựng với sự đóng góp từ 33 nước thành viên và quan sát viên từ tất cả mạng lưới toàn cầu của FATF, báo cáo nội bộ này cung cấp cho các cơ quan có thẩm quyền một bộ công cụ gồm những công cụ triệt phá và những chiến lược hoàn hảo sẽ giúp cho họ hoàn thiện được công tác chống tài trợ khủng bố trong nước và xác định được những cách thức mới theo đó các cơ quan có thẩm quyền có thể cùng kết hợp một cách có hiệu quả để ngăn chặn hoạt động tài trợ cho khủng bố.

Cập nhật về tài trợ cho ISIL, Al-Qaeda và các nhánh của các tổ chức này (Tháng 10/2017) – Không công bố

21 Tháng 2/2015, FATF công bố một báo cáo đầy đủ về Tài trợ cho Nhà nước hồi giáo tự xưng ở I- rắc (ISIL). Từ đó, FATF đã phát hành điều đặn nhưng không công bố những ấn phẩm cập nhật 3 lần 1 năm, dựa trên những thông tin mà mạng lưới toàn cầu cung cấp. Những bản cập nhật này cũng bao gồm thông tin về Al-Qaeda, ISIL và các

nhánh của Al-Qaeda. Tháng 10/2018 và tháng 6/2019, FATF đã đưa ra tuyên bố về vấn đề tài trợ cho ISIL sau khi tổ chức này bị mất lãnh thổ của mình.

Xác định và đánh giá rủi ro tài trợ khủng bố

22 Xác định, đánh giá và hiểu những rủi ro tài trợ khủng bố là phần quan trọng trong quá trình vạch trần và triệt phá mạng lưới khủng bố. Tháng 7/2019, FATF đã đưa ra hướng dẫn, trong đó cung cấp những thực tiễn tốt nhất và những điều cần tập trung đối với các nước khi xác định và đánh giá rủi ro tài trợ khủng bố của họ, dựa trên kinh nghiệm từ mạng lưới toàn cầu của FATF.

Sự khai thác tài sản ảo theo cách phạm tội nhằm mục đích ML/TF – giải quyết những thách thức trong điều tra và tịch thu (không công bố)

23 Tài sản ảo (VAs) có những đặc tính riêng biệt như một loại tài sản có thể làm nản các cuộc điều tra tài chính, và việc tịch thu liên quan, hạn chế khả năng của các cơ quan chức năng trong việc phát hiện, điều tra và truy tố tội phạm ML/TF, những kẻ sử dụng những công nghệ này. Tháng 6/2019, FATF đã thông qua một hướng dẫn không công bố, cung cấp những thực tiễn tốt nhất cho các cơ quan thực thi pháp luật nhằm hỗ trợ họ trong các cuộc điều tra tài chính có nghi ngờ liên quan đến VAs. Báo cáo này cũng đưa ra những vụ việc và kỹ thuật có thể được sử dụng bởi các cơ quan chức năng nhằm tịch thu được VAs bất hợp pháp.

2.2 CFATF – Lực lượng đặc nhiệm tài chính vùng vịnh Caribe

24 CFATF đã đưa ra một số báo cáo mô hình, gồm: Rửa tiền có sử dụng những nhà cung cấp dịch vụ công ty và tín thác (2010); Buôn người và vận chuyển lậu người (2014); Chơi bạc bất hợp pháp (2016); Sự dịch chuyển của tiền mặt và các công cụ chuyển nhượng (2016) và Sự phổ biến vũ khí hạng nhẹ và đạn dược (2016).

Dự án mô hình của CFATF về Giảm rủi ro bằng cách giảm khả năng tiếp cận dịch vụ (De-risking) (2019)

25 CFATF thực hiện nghiên cứu về De-risking từ tháng 6/2018 đến tháng 4/2019 với mục đích nhấn mạnh tới mức ảnh hưởng ngược chiều mà nó mang lại trong khu vực. Nghiên cứu này được thực hiện theo 2 giai đoạn và có việc kêu gọi các Ngân hàng Trung ương, các tổ chức tài chính và khu vực tư nhân cung cấp số liệu.

26 Phân tích số liệu nhận được qua lời kêu gọi này cho thấy như sau:

27 Theo như 71% các Ngân hàng Trung ương trong khu vực, De-risking chính là nguy cơ đang tăng. Bên cạnh đó, 90% trong số đó lại cho rằng “De-risking” chính là nguy cơ mà nó đang ảnh hưởng và tiếp tục ảnh hưởng tới khả năng tồn tại hoạt động của họ, bên cạnh những yếu tố khác, bằng cách tăng chi phí hoạt động và kéo dài chuỗi thời gian thanh toán.

28 Dựa trên phản hồi nhận được từ tổng 227 tổ chức tài chính, 158 (hoặc là 77%) các tổ chức này chỉ ra rằng hoạt động của họ bị ảnh hưởng không tốt bởi De-risking (chậm dứt/ hạn chế quan hệ ngân hàng đại lý) với nguyên nhân chính là góp phần gây khó khăn cho việc cung cấp dịch vụ cho khách hàng và bị xếp vào loại rủi ro bởi các ngân hàng đại lý. Những nguyên nhân khác gồm: khó tìm được nơi đặt lại ngân hàng đại lý; và tăng chi phí hành chính.

29 Hai nguyên nhân chính khiến cho các tổ chức tài chính chấm dứt/ hạn chế quan hệ ngân hàng đại lý là: biên lợi nhuận thấp/ nhỏ và chi phí tuân thủ. Tuy nhiên, trong nhiều trường hợp, nguyên nhân không được nêu ra. Một vài nguyên nhân khác gồm: có vấn đề với quy trình AML/CFT; không lâu sau đó thì không còn sản phẩm/dịch vụ mà mỗi quan hệ được thiết lập nhằm phục vụ cho nó; rủi ro có thể có từ nước đó; chiến lược giảm thiểu rủi ro về phía ngân hàng đại lý; khẩu vị rủi ro thấp; mỗi quan hệ kinh doanh không thống nhất với chiến lược của ngân hàng đại lý và nỗi lo sợ bị cơ quan quản lý của nước chủ nhà phạt.

30 Trong những trường hợp khi nước nơi ngân hàng đại lý đặt trụ sở được xác định thì một nửa nằm ở Bắc Phi và 1/3 nằm ở Châu Âu. Những ngân hàng khác nằm ở Châu Á, vùng vịnh Ca-ri-bê và Nam Mỹ.

31 Những sản phẩm và dịch vụ bị ảnh hưởng là hoạt động chuyển tiền điện tử, cho vay/ mở L/C, thanh toán bù trừ séc, đánh bạc online hoặc trò chơi điện tử trên mạng, dịch vụ quản lý tiền mặt, xử lý thẻ tín dụng, hoạt động chuyển tiền và dịch vụ ngân hàng trên điện thoại (mobile banking).

32 Một số ngân hàng (55 ngân hàng) có mối quan hệ ngân hàng đại lý bị chấm dứt trong vòng 3 năm qua. Phần lớn những ngân hàng này (80%) mất từ 1 đến 3 mối quan hệ ngân hàng đại lý, trong khi 11% mất từ 7 đến 10 mối quan hệ ngân hàng đại lý.

33 Báo cáo de-risking đã được thông qua như một tài liệu nội bộ trước Hội nghị thường niên của CFATF tháng 5/2019.

2.3 EAG – Nhóm Á Âu về chống rửa tiền và tài trợ khủng bố

Tài trợ khủng bố và các nguồn thu phạm tội (kể cả tội phạm có tổ chức)

34 Những vấn đề liên quan tới công tác chống tài trợ khủng bố là một nội dung trong chương trình nghị sự của EAG trong nhiều năm và được coi là ưu tiên hàng đầu của EAG và các thành viên. Cho tới nay, EAG đã hoàn thành một số dự án mô hình liên quan tới chống tài trợ khủng bố (CFT). Dự án gần đây nhất là dự án chung với APG (vừa mới qua) về mối liên hệ giữa TF và tội phạm có tổ chức. 3 nước dẫn đầu dự án là Bangladesh, Ấn Độ và Liên bang Nga. Các Nghị quyết Hội đồng Bảo an số 2195 và 2322 chính là cơ sở cho dự án.

35 Dự án nhằm mục tiêu:

☐ Hiểu hơn về phạm vi và cách những khoản thu phạm tội (kể cả tội phạm có tổ chức) được sử dụng hoặc có thể được sử dụng thế nào cho mục đích tài trợ khủng bố bởi những kẻ khủng bố đơn lẻ và các tổ chức khủng bố.

☐ Xác định phương pháp luận được sử dụng để thu thập, chuyển dịch và sử dụng các khoản tiền từ nguồn thu phạm tội, kể cả tội phạm có tổ chức, cho mục đích tài trợ khủng bố.

☐ Xác định những thực tiễn tốt nhất để phát hiện, điều tra và phòng ngừa không cho những kẻ khủng bố và các tổ chức khủng bố sử dụng các nguồn thu phạm tội.

36 Thông tin thu thập được trong 2 giai đoạn, một là gửi đi các bảng câu hỏi, hai là hội thảo chung giữa EAG và APG được tổ chức tại Novosibirsk, Liên bang Nga vào

tháng 12/2018, khi đó một phiên riêng được tổ chức về mối liên hệ giữa TF và tội phạm có tổ chức.

37 Những gì rút ra từ những thảo luận tại cuộc hội thảo chung, cũng như phản hồi theo bảng câu hỏi là cơ sở cho những phát hiện ban đầu của báo cáo dự án và sẽ được thảo luận và thông qua tại Hội nghị thường niên của APG và EAG năm 2019.

2.4 GIABA – Nhóm hành động liên Chính phủ chống rửa tiền tại Tây Phi

Các biện pháp nhận biết khách hàng/cập nhật thông tin khách hàng (KYC/CDD) và tài chính toàn diện tại Tây Phi

38 Báo cáo này là đầu ra của một nghiên cứu được Nhóm hành động liên chính phủ chống rửa tiền tại Tây Phi (GIABA) thực hiện bắt đầu từ tháng 9/2016. Nghiên cứu này là hành động tiếp theo một nghiên cứu trước đó về tài chính toàn diện được thực hiện vào năm 2013. Nó được thực hiện nhằm hiểu được và giải quyết những thách thức trong việc thực hiện các biện pháp phòng ngừa KYC/CDD với trách nhiệm liên quan trong tài chính toàn diện. Trên cơ sở những phát hiện của nghiên cứu, các khuyến nghị đã được đưa ra nhằm giúp các cơ quan có thẩm quyền liên quan trong các nước thành viên GIABA thiết kế được những cơ chế KYC/CDD hiệu quả vừa thích hợp vừa phù hợp với tài chính toàn diện mà vẫn tuân thủ được và thuận lợi khi thực hiện các khuyến nghị của FATF và Phương pháp luận đánh giá (sửa đổi). Báo cáo này có thể xem được trên trang chủ của GIABA tại địa chỉ <https://www.giaba.org/reports/typologies/reports.html>.

Rửa tiền từ hoạt động làm giả thuốc tại Tây Phi

39 Nghiên cứu này nhằm mục đích hiểu được bản chất và tầm quan trọng của vấn đề rửa tiền từ hoạt động làm giả thuốc tại Tây Phi. Phương pháp luận được vận dụng bao gồm việc lựa chọn 4 nước (Côte d'Ivoire, Nigeria, Senegal và Togo) nhằm mục đích nghiên cứu sâu hơn, trong khi những nước khác thì trả lời theo các bảng câu hỏi. Mối liên hệ giữa ML và làm giả thuốc đã được phân tích trong các báo cáo của các nước, trong các phản hồi các bảng câu hỏi của các nước thành viên và những vụ việc điển hình do các cơ quan thực thi pháp luật cung cấp. Báo cáo này có thể tìm thấy trên trang chủ của GIABA tại địa chỉ <https://www.giaba.org/reports/typologies/reports.html>.

2.5 Nhóm Egmont

Những công nghệ tài chính mới nổi, rửa tiền và tài trợ khủng bố: Mô hình liên quan tiền ảo

40 Trong 12 tháng qua, Nhóm Egmont đã hoàn thành một số dự án quan trọng bao gồm cả dự án mô hình với tiêu đề Những công nghệ tài chính mới nổi, rửa tiền và tài trợ khủng bố: Mô hình liên quan tiền ảo. Trường các FIU đã thông qua báo cáo này vào tháng 5/2018 và cho phép chuyển tới tất cả các FIU, các đối tượng báo cáo có liên quan, các cơ quan thực thi pháp luật và các quan sát viên của Nhóm Egmont.

Báo cáo về Che giấu quyền chủ sở hữu hưởng lợi (tài liệu chung với FATF)

41 Báo cáo chung giữa FATF và Nhóm Egmont này có cái nhìn tổng quan đánh giá việc làm thế nào mà các pháp nhân, các trung gian chuyên nghiệp và các thảo luận pháp lý có thể trợ giúp cho tội phạm che giấu những tài sản và nguồn lợi phi pháp được. Mục đích của báo cáo là nhằm giúp cho các cơ quan, bao gồm cả FIUs, các tổ chức tài chính và các nhà cung cấp dịch vụ chuyên nghiệp khác trong các nước hiểu được bản chất những rủi ro mà họ phải đối mặt.

Tài liệu về bộ các dấu hiệu trong các vụ việc liên quan tham nhũng

42 Nhóm Egmont đã tổng hợp những dấu hiệu trong một tài liệu, mà khi xem xét trong bối cảnh giao dịch hoặc mối tương tác của khách hàng, sẽ hỗ trợ trong việc xác định được những dấu hiệu của tham nhũng và hành vi rửa những khoản thu từ tham nhũng. Mục tiêu trực tiếp của tài liệu này là nhằm tăng cường thông tin tình báo có ích cho các FIU, mà cơ quan này phải được hợp tác với các cơ quan thực thi pháp luật, các tổ chức tài chính và các tổ chức báo cáo ở tuyến đầu khác nhằm hoàn thiện hoạt động nhận dạng các giao dịch đáng ngờ và các hoạt động có thể liên quan đến tham nhũng.

43 Nhóm Egmont nhận thức được tầm quan trọng của các công việc với các chủ đề khác nhau được tiến hành bởi các tổ chức quốc tế, bao gồm cả FATF, Ngân hàng Thế giới, UNODC và INTERPOL, và những chủ đề này cũng cần phải được lưu ý khi xem xét đến vấn đề nhận dạng các giao dịch đáng ngờ hoặc những khoản thu có được từ tham nhũng hoặc các tội phạm nguồn khác.

44 Tài liệu này được Trưởng các FIU thông quan tại Hội nghị nhóm Egmont diễn ra tại Sydney (24-27/9/2018), không chỉ dừng lại ở đó mà sẽ được chỉnh sửa và bổ sung phụ thuộc vào phản hồi nhận được từ các nước thành viên, quan sát viên, các tổ chức quốc tế đối tác của Nhóm Egmont và các cơ quan có thẩm quyền khác nhau cũng như các đối tượng báo cáo.

Tài liệu của ECOFEL về tính độc lập và tự trị của FIU

45 Tài liệu này đã được soạn ra nhằm giúp các chính phủ (những người ra quyết định và ban hành chính sách), FIU và những cơ quan có trọng trách khác trong việc xác định và hiểu về những yếu tố cần có để định rõ quyền hạn và đẩy mạnh tính độc lập và tự trị trong hoạt động của FIU.

46 Tài liệu được thiết kế đáp ứng yêu cầu từ các thành viên Nhóm các đơn vị tình báo tài chính (EG) về việc phải có hướng dẫn về những đặc điểm nào cần có để đảm bảo FIU là độc lập và tự trị trong hoạt động. Tài liệu này tập trung vào việc miêu tả những đặc điểm khiến cho một FIU có được tính độc lập và tự trị. Tài liệu không phải là một chuẩn mực mới cũng không bàn luận về chiến lược nào để có thể đạt được những đặc điểm ấy.

3. XU HƯỚNG RỬA TIỀN VÀ TÀI TRỢ KHỦNG BỐ

47 Phần này của báo cáo đưa ra cái nhìn tổng quan về xu hướng rửa tiền và tài trợ khủng bố, bao gồm cả thông tin từ những nguồn mở về các nghiên cứu được thực hiện bởi các thành viên và quan sát viên của APG.

3.1 Nghiên cứu hoặc bài viết về các phương thức và xu hướng ML/TF được các thành viên và quan sát viên APG thực hiện.

ÚC

Báo cáo năm 2018 về Các tổ chức phi lợi nhuận và những dấu hiệu tài trợ khủng bố

48 Trong năm 2018, 8 FIU các nước Úc (Trung tâm Phân tích và báo cáo giao dịch), Brunei Darussalam (FIU, Autoriti Monetari Brunei Darussalam), Indonesia (Pusat Pelaporan dan Analisis Transaksi Keuangan), Malaysia (Ngân hàng Trung ương Malaysia), New Zealand (Cảnh sát New Zealand FIU), the Philippines (Ủy ban chống rửa tiền), Singapore (Văn phòng Báo cáo giao dịch đáng ngờ-Suspicious Transaction Reporting Office) và Vương Quốc Thái Lan (Văn phòng chống rửa tiền- Anti-Money Laundering Office) đã phối hợp với nhau phát triển và đưa ra những dấu hiệu cảnh báo đỏ như là một phần của nỗ lực hoạt động liên tục thực hiện theo Hội nghị chính thức về chống tài trợ khủng bố hàng năm.

49 Báo cáo cung cấp một bộ những dấu hiệu cảnh báo đỏ liên quan tới các tổ chức phi lợi nhuận (NPOs) đang có rủi ro cao bị lạm dụng để tài trợ cho khủng bố tại Đông Nam Á, Úc và New Zealand, đồng thời có mục đích là hỗ trợ cho các đối tượng báo cáo và NPOs có thể nhận biết và giảm thiểu những hoạt động đáng ngờ tiềm ẩn sự liên kết với hoạt động tài trợ cho khủng bố trong khu vực.

50 Những dấu hiệu được chỉ ra trong đó là dựa vào các vụ việc điển hình và thông tin tình báo có được từ các FIU, các cơ quan thực thi pháp luật và các nhà quản lý NPOs trong khu vực. Các tổ chức tài chính nắm giữ tài chính của các NPOs và có trách nhiệm báo cáo hoạt động đáng ngờ cũng đã cung cấp thông tin đầu vào cho tài liệu.

51 Xin hãy xem trang <https://www.austrac.gov.au/sites/default/files/2019-06/npored-flag-indicators.pdf> để cso thêm thông tin.

Đánh giá rủi ro về những nhà cái trực tuyến (On-course bookmakers)

52 Cuối năm 2018, AUSTRAC đã phát hành một báo cáo đánh giá rủi ro nghiên cứu về rủi ro ML/TF nói chung đối với lĩnh vực on-course bookmaking tại Úc.

53 Những dịch vụ do on-course bookmakers cung cấp được xác định dường như có mức độ rủi ro thấp về rửa tiền và trốn thuế, cũng chưa có ghi nhận về hoạt động tài trợ cho khủng bố. Bản chất ngày càng lụi tàn của lĩnh vực này và một loạt những yếu tố khác đã hạn chế mức độ tổn thương của khu vực này trước hoạt động ML và sự lạm dụng của các loại tội phạm khác và như vậy lĩnh vực này được coi là có rủi ro thấp. Tuy vậy, báo cáo lại chỉ ra rằng on-course bookmakers với những khoản thu lợi lớn, bao gồm cả những khoản thu do cung cấp các tài khoản cá cược trực tuyến, lại có mức độ tổn thương hơn trước sự lạm dụng của tội phạm so với các tổ chức khác.

54 Đánh giá rủi ro đã cung cấp thông tin chi tiết giúp cho lĩnh vực này hiểu và ứng phó với những rủi ro gắn liền với những dịch vụ do các on-course bookmakers cung cấp. Xin theo đường dẫn sau để xem đánh giá rủi ro:

<https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/course-bookmakers-money-laundering-and-terrorism-financing-risk-assessment>

Hướng dẫn trong lĩnh vực hưu trí

55 Tháng 12/2018, AUSTRAC đã công bố một hướng dẫn cho lĩnh vực hưu trí về việc làm thế nào để áp dụng những chi tiết trong Luật chống rửa tiền và chống tài trợ khủng bố năm 2006 trong hoạt động của họ.

56 Hướng dẫn đưa ra những mẫu được thiết kế chỉ để nhằm mục đích minh họa mà thôi, để nhấn mạnh tới việc làm thế nào lĩnh vực này có thể sử dụng được bộ công cụ AML/CFT để xác định, giảm thiểu và quản lý được những rủi ro ML/TF của lĩnh vực hưu trí này. Những mẫu này cung cấp cho những nhà kinh doanh quỹ hưu trí cái nhìn sâu hơn về việc làm thế nào lĩnh vực này có thể áp dụng những cách tiếp cận linh hoạt cho việc sử dụng bộ công cụ AML/CFT (phù hợp với hoạt động kinh doanh và mức độ rủi ro của chính họ).

57 Xin hãy xem hướng dẫn tại <https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/industry-specific-guidance-superannuation-sector>

CANADA

58 Đánh giá của FINTRAC năm 2018 về tài trợ khủng bố

<http://www.fintrac-canafe.gc.ca/intel/assess/tfa-2018-eng.asp>

59 Cảnh báo của FINTRAC về rửa tiền chuyên nghiệp (PML) thông quan thương mại và các tổ chức cung ứng dịch vụ tiền tệ

<http://www.fintrac-canafe.gc.ca/intel/operation/oai-ml-eng.asp>

FIJI

60 FIU của Fiji đã tiến hành một nghiên cứu không chính thức về các phương thức và xu hướng ML/TF. FIU Fiji tiếp tục cung cấp thông tin trong ấn phẩm Báo cáo thường niên của họ.

61 Các báo cáo hàng năm của FIU Fiji đưa vào những vụ việc điển hình xuất phát từ các báo cáo giao dịch đáng ngờ và các vụ việc đã truy tố được tội rửa tiền một cách hiệu quả tại Fiji. Các báo cáo cũng đã đưa vào đó những xu hướng mới nổi, đang tiếp diễn và những xu hướng đã dần giảm đi. Bản sao Báo cáo thường niên có thể tìm được trên trang chủ FIU Fiji: www.fijifiu.gov.fj

HONG KONG, TRUNG QUỐC

62 Đơn vị tình báo tài chính chung của Hong Kong (JFIU) đã phát hành một báo cáo phân tích chiến lược về các phương thức lừa đảo qua email, gồm những phân tích phức tạp về thông tin tài khoản, các hoạt động tài khoản và những phân tích chuyên đề về sự thay đổi sở hữu tại các công ty, chữ ký trên các tài khoản và nội dung thanh toán. Có thể khai thác báo cáo theo địa chỉ sau:

https://www.jfiu.gov.hk/info/doc/Strategic_Analysis_Report_on_Email_Scams.pdf

INDONESIA

63 Indonesia tiến hành các nghiên cứu thường xuyên về các phương thức và xu hướng ML/TF với các chủ đề khác nhau trong mỗi lần. Những nghiên cứu và ấn phẩm được đưa ra 1 năm 1 lần. Nếu như có một vấn đề hiện tại hoặc vấn đề đặc biệt liên quan đến phương thức và xu hướng ML/TF, Indonesia có thể tiến hành ngay một nghiên cứu không theo thường lệ. Tuy nhiên, những nghiên cứu và ấn phẩm này chỉ được ban hành nội bộ và chỉ được chia sẻ ra bên ngoài một cách hạn chế.

64 Trong quá khứ, Indonesia đã tiến hành những nghiên cứu về các phương thức ML/TF liên quan đặc biệt đến một số tội phạm nguồn, các phương thức chuyển tiền được sử dụng và hồ sơ của các đối tượng liên quan.

65 Những nghiên cứu mới đây về các phương thức và xu hướng ML/TF bao gồm cả mô hình liên quan đến các vụ việc ML đã được tòa án xử trong năm 2017. Nghiên cứu này đã chỉ ra rằng, những vụ việc được xử trong năm 2017, tội phạm nguồn chính được báo cáo chủ yếu liên quan đến ma túy. Những khía cạnh chính liên quan đến giao dịch là những giao dịch qua ATM, nộp tiền mặt vào quỹ và thanh toán số lượng lớn,

NHẬT BẢN

66 Báo cáo thường niên của Trung tâm tình báo tài chính Nhật Bản (JAFIC), trong đó có số liệu thống kê chi tiết, các vụ việc điển hình và các xu hướng, được ban hành trên trang chủ của JAFIC.

MALAYSIA

Đánh giá rủi ro quốc gia (NRA)

67 Lần 3 phối hợp NRA của Malaysia đã hoàn tất và được Ủy ban điều phối nước về chống rửa tiền (NCC) thông qua vào tháng 7/2018. Phương pháp luận của NRA đã được củng cố với phạm vi rộng hơn và cách nhìn về số liệu được xem xét lại. Bên cạnh đánh giá về rủi ro mối đe dọa và đánh giá rủi ro theo ngành (tổ chức tài chính và các ngành nghề phi tài chính), đánh giá rủi ro tài trợ khủng bố của các NPO cũng đã được NCC thông qua như 1 phần của đánh giá rủi ro nước.

68 Những tội phạm có rủi ro cao nhất trong Đánh giá rủi ro năm 2018 cũng tương đồng với những tội phạm được xác định trong NRA năm 2013, có nghĩa là: lừa đảo, buôn lậu, tham nhũng và buôn lậu ma túy bất hợp pháp, loại trừ tội phạm có tổ chức được đánh giá là có rủi ro cao hơn thay thế cho tội trốn thuế như là 1 trong 5 loại tội phạm có rủi ro cao nhất. Tất cả các tội phạm có rủi ro cao đều có số liệu về số cuộc điều tra nhiều, giá trị các khoản thu đáng ngờ được phát hiện và số tiền theo thông tin tình báo tài chính phát sinh.

69 Là một phần của quá trình NRA, NCC đã xác định những khu vực cần phải hoàn thiện để giảm thiểu những rủi ro mới được xác định. Theo cách thức này, Kế hoạch chiến lược nước năm 2016-2020 hiện tại (NSP) sẽ được xem xét lại và được hiệu chỉnh lại để tập trung hơn vào thúc đẩy những kế hoạch hành động hiện tại, các chiến lược giảm thiểu rủi ro mới (bao gồm cả những thiếu hụt mới được xác định) và những thay đổi trong các chuẩn mực quốc tế.

70 Cùng thời gian đó, truyền thông và tuyên truyền cảnh báo đã được tiến hành ngay sau khi NRA được thông qua, đặc biệt là có những buổi tổng quan lại cho các đối tượng báo cáo.

Thông báo ngắn gọn về mô hình và các dấu hiệu cảnh báo đỏ

71 Trong năm 2018 và 2019, FIU đã ban hành 5 thông báo ngắn gọn về mô hình và những dấu hiệu cảnh báo đỏ về những tội phạm sau: TF (tháng 4/2018), phổ biến vũ khí hủy diệt-PF (tháng 5/2018), tham nhũng (tháng 6/2018), lừa đảo (tháng 10/2018) và buôn lậu ma túy (tháng 1/2019). Những tội phạm này là những tội phạm có rủi ro cao được xác định qua NRA và dựa trên nhu cầu của khu vực tư nhân. Các tài liệu được phát hành với phạm vi lưu hành hạn chế cho các tổ chức báo cáo và nhằm mục tiêu:

- Cung cấp sơ bộ và tuyên truyền, cảnh báo về các xu hướng, kỹ thuật, phương thức và các kênh sử dụng của tội phạm;
- Tăng cường và làm giàu thêm kiến thức và sự hiểu biết về các mô hình của các tổ chức báo cáo;
- Giúp các tổ chức báo cáo trong việc xác định hành vi phạm tội từ các chỉ số cảnh báo đỏ do các khách hàng của họ thực hiện và các giao dịch tài chính liên quan.
- Giúp cho các tổ chức báo cáo có thể phát hiện sớm để ngăn chặn những hoạt động liên quan tới tội phạm cụ thể nào đó và hoàn thiện hơn nữa chất lượng báo cáo giao dịch đáng ngờ (STRs).

NEW ZEALAND

Rửa tiền qua các tổ chức chuyển tiền và các chuyên gia

72 Đơn vị tình báo tài chính của New Zealand (NZFIU) đã thực hiện một dự án chung nhằm xác định các tổ chức chuyển tiền và những người gác cổng chuyên nghiệp (các luật sư/kế toán viên/ các đại lý bất động sản), mà dịch vụ của những người này đã bị lạm dụng bởi những kẻ tội phạm để rửa tiền. Phương pháp luận bao gồm việc Cảnh sát New Zealand xem xét về tội phạm có tổ chức trong quãng thời gian 18 tháng từ tháng 1/2017, xác định những tổ chức tạo điều kiện cho sự dịch chuyển của những khoản thu phạm tội trong những vụ việc này; đồng thời đưa những số liệu vào các biểu đồ để phân tích với sự phân tích về dòng tiền và phân tích tương tự được tiến hành nhằm xác định những tổ chức tạo điều kiện thực hiện những giao dịch có giá trị cao và tạo điều kiện thúc đẩy xét xử đối với những tổ chức tham gia dịch chuyển những khoản thu phạm tội đó.

73 Những chủ đề chính đề cập trong dự án được tóm lược lại như sau:

74 Những nút thắt chính: Một mạng lưới cơ bản khoảng 65 cơ sở kinh doanh, các cá nhân và các nhà cung cấp dịch vụ tài chính dường như bị lạm dụng để rửa các khoản thu từ hoạt động tội phạm có tổ chức. Mạng lưới những “nút thắt” này được củng cố bởi một loạt các tổ chức chuyển tiền có cơ sở tại Auckland (MRs) và đã tạo điều kiện cho việc luân chuyển hơn 200 triệu đô-la giá trị giao dịch đáng ngờ từ năm 2016. Dường như là một phần lớn số tiền này có được từ tội phạm ma túy, lừa đảo và những tội phạm nghiêm trọng khác.

75 Văn hóa không tuân thủ AML/CFT trong hệ thống các tổ chức chuyển tiền (MRs): Phần lớn các MRs được xác định vào tầm ngắm của Cảnh sát và Bộ Nội vụ vì tiếp tục không tuân thủ với các nghĩa vụ về AML/CFT, bao gồm cả việc không nhận dạng khách hàng, không kiểm soát giao dịch hoặc không báo cáo giao dịch đáng ngờ.

Những sự dễ bị tổn thương này hầu như sẽ bị những kẻ tội phạm khai thác để đưa những nguồn tiền bất hợp pháp của chúng vào nền kinh tế hợp pháp.

76 Sự độc lập giữa các MRs: MRs làm việc gần như nhau, thu hút nguồn tiền, sử dụng các tài khoản ngân hàng thông thường, và thuê những người vận chuyển tiền mặt để thực hiện một loạt các giao dịch hợp pháp cũng như bất hợp pháp thay mặt cho khách hàng của họ. Họ sử dụng những mẫu hình kinh doanh phức tạp dựa trên sự sắp đặt những giao dịch chuyển tiền và giá trị không chính thức để tạo điều kiện cho những khoản thu bất hợp pháp dễ dàng hòa trộn với những khoản thu hợp pháp. Điều này thường cản trở khả năng lần theo dấu tiền một cách hiệu quả của lực lượng thực thi pháp luật vì những khoản thu bất hợp pháp thường được sử dụng để hoàn tất những giao dịch hợp pháp đã được thực hiện trước đó thay mặt cho những khách hàng không chủ tâm làm vậy.

77 Sử dụng những người vận chuyển tiền mặt: Những người vận chuyển tiền mặt làm việc thay cho các MRs thực hiện thu gom tiền mặt và phân bổ các nguồn này đến các ngân hàng New Zealand. Họ có rủi ro cao về rửa tiền vì họ giao dịch với số tiền mặt lớn và không thực hiện đầy đủ việc nhận dạng khách hàng cũng như nguồn tiền, cũng như chủ sở hữu hưởng lợi của những khoản tiền mà họ nắm giữ. Một vài người vận chuyển tiền mặt thường tiến hành thu tiền mặt trực tiếp từ các nhóm tội phạm có tổ chức và dường như sẽ trở thành mục tiêu của các cuộc điều tra.

78 Những phương thức dịch chuyển tiền: Các nhóm tội phạm có tổ chức sử dụng những người chuyên nghiệp như những người gác cổng cho nền kinh tế hợp pháp. Một khi những khoản thu bất hợp pháp được đưa vào hệ thống tài chính qua những người chuyên nghiệp này, chúng được hòa trộn với các khoản thu hợp pháp và được hội tụ thông qua các tín thác, mua tài sản, hoặc đơn giản là trả tiền mặt. Việc sử dụng những người này trong việc thiết kế các giao dịch và thu gom tiền mặt sẽ làm lu mờ những dấu vết của tiền và làm suy yếu nỗ lực của các cơ quan thực thi pháp luật nhằm lần theo luồng tiền về ngược lại nguồn của nó.

PHILIPPIN

Tăng cường giám sát chống rửa tiền bên cạnh những tiến bộ trong công nghệ tài chính

79 Vào ngày 21/8/2018, Hội đồng chống rửa tiền (AMLC) đã phê duyệt nghiên cứu về Môi trường quản lý AML đối với tiền ảo (VC) tại Philippines. Nghiên cứu được thực hiện để đánh giá sơ bộ hồ sơ giao dịch của các sàn giao dịch VC được công nhận, đặc biệt liên quan đến các giao dịch đáng ngờ, khách hàng nghi ngờ có liên quan đến các hoạt động bất hợp pháp và các giao dịch lớn. Các sàn giao dịch VC được quản lý bởi Bangko Sentral ng Pilipinas (BSP), khi được sử dụng để cung cấp dịch vụ tài chính, đặc biệt là cho các khoản thanh toán và chuyển tiền, theo Thông tư số 944 (Hướng dẫn cho các sàn VC) ngày 6/2/2017, liên quan đến Thông tư số 942 của BSP (Quy định cho các tổ chức tài chính phi ngân hàng). Nghiên cứu được công bố trên trang web của AMLC: <http://www.amlc.gov.ph/images/PDFs/Study%20on%20VC.pdf>

80 Nghiên cứu đã sử dụng phân tích mô tả trên những báo cáo giao dịch vượt ngưỡng (CTR) và báo cáo giao dịch đáng ngờ (STR) nhận được từ các sàn giao dịch VC được BSP công nhận từ ngày 6/3/2017 đến ngày 10/4/2018, bao gồm các giao dịch được thực hiện trên nền tảng của họ từ ngày 28/4/2014 đến ngày 6/4/2018, có tổng cộng 22.366 báo cáo giao dịch (bao gồm 1.086 CTR và 21.280 STR) với tổng giá trị là 3,1 tỷ

PHP (2,4 tỷ PHP là CTR và 0,7 tỷ PHP là STR). Nghiên cứu cho thấy các báo cáo giao dịch của sàn giao dịch VC tăng đáng kể cả về khối lượng và giá trị cho năm 2017, sau khi ban hành Thông tư số 944 của BSP vào tháng 2 năm 2017 và sau đó chấp thuận cho đăng ký các công ty tiền ảo vào tháng 9 và tháng 10/2017.

81 Việc thiết lập cơ chế quản lý của BSP đối với các sàn giao dịch VC đã tăng cường các biện pháp bảo vệ chống lại các rủi ro liên quan đến các VC, như kiểm soát ML và TF, quản lý rủi ro công nghệ và bảo vệ người tiêu dùng. Đặc biệt, việc đưa các sàn giao dịch VC làm đối tượng chịu sự điều chỉnh (CP) đã cho phép giám sát toàn diện hơn hành vi tài chính của các cá nhân và tổ chức có thể liên quan đến các hoạt động bất hợp pháp cũng như phối hợp và chia sẻ thông tin chặt chẽ hơn giữa các CP trong việc thực hiện giám sát AML, như đã thu được từ tường trình của các sàn giao dịch VC.

Đánh giá rủi ro của các tổ chức phi lợi nhuận (NPO)

82 Vào ngày 28/11/2018, AMLC đã thông qua Đánh giá rủi ro của khối NPO và ủy quyền cho phép chuyển giao tới tất cả các cơ quan liên quan. Đánh giá rủi ro NPO được thực hiện theo Khuyến nghị 8 trong số 40 Khuyến nghị của FATF. AMLC được hỗ trợ bởi các cơ quan quản lý NPO, Ủy ban Ngoại hối và Chứng khoán (SEC) và Bộ Phát triển và Phúc lợi Xã hội (DSWD). Hội đồng Chứng nhận NGO (PCNC) của Philippines và Ủy ban phát triển các mạng lưới NGO (CODE-NGO) cũng nêu những ý kiến có giá trị đối với nỗ lực nói trên.

83 Đánh giá rủi ro NPO đã trình bày và phân tích rủi ro ML/ TF của các NPO, dựa trên các cuộc điều tra và các vụ việc thực tế, các báo cáo tình báo và ý kiến đại diện cho khu vực. Các nguy cơ ML cho lĩnh vực này được đánh giá là Trung bình; Các nguy cơ TF được đánh giá là Cao-Thấp. Đánh giá độ nhạy cảm cho cả ML và TF là Trung bình. Mặc dù khung pháp lý nói chung có hiệu quả, việc thực thi luật pháp và các quy định cho thấy một số vấn đề.

84 Báo cáo đưa ra khuyến nghị về các chiến lược cụ thể cho cả khu vực công và NPO để giảm thiểu rủi ro ML và TF liên quan đến NPO. Những chiến lược này bao gồm phương thức tiếp cận lâu dài với các cơ quan quản lý và khu vực NPO, áp dụng các quy định dựa trên cơ sở rủi ro và giám sát NPO và sự phối hợp chặt chẽ hơn giữa chính phủ và khu vực NPO.

Tự tài trợ của ISIL ở Đông Nam Á

85 Nhóm làm việc về tài trợ chống khủng bố ở Đông Nam Á (SEA CTF WG), được thành lập tại Hội nghị thượng đỉnh CTF lần thứ ba năm 2017, đã tiến hành nghiên cứu về việc tài trợ cho ISIL và các nhóm có liên hệ với ISIL ở Đông Nam Á. Các nhóm làm việc đã đưa ra bốn báo cáo riêng biệt: (a) Tài trợ cho ISIL ở ĐNÁ: Bối cảnh khu vực, (b) Tài trợ từ bên ngoài cho ISIL ở ĐNÁ, (c) Tài trợ qua các đại lý Hawala cho ISIL và các tổ chức khủng bố có nguy cơ cao khác ở ĐNÁ, và (d) Tự tài trợ của ISIL ở ĐNÁ. Các báo cáo nói trên là những đánh giá của từng nhóm dự án chính dựa trên thông tin được thu thập từ các thành viên của SEA CTF WG.

86 AMLC của Philippines đã đi đầu trong việc kiểm tra sự tự tài trợ của ISIL-ĐNÁ để hiểu thêm về nó và đưa ra các chiến lược ngăn ngừa. Báo cáo về tự tài trợ đã xác định rằng các quỹ này bao gồm những khoản tiền được huy động từ các nguồn tội phạm, chẳng hạn như bắt cóc để đòi tiền chuộc, tống tiền người dân địa phương và buôn bán hoặc vận chuyển ma túy. Một phương pháp tự tài trợ khác cho TF là thông

qua các nguồn hợp pháp, chẳng hạn như hỗ trợ từ gia đình, đóng góp từ các đối tượng có thiện cảm, lợi nhuận kinh doanh và thu nhập hợp pháp. Các thành viên của SEA CTF WG và các khách mời đã chia sẻ thông tin về các nguồn tự tài trợ được sử dụng bởi các nhóm khủng bố hoặc các nhóm nguy cơ ở Đông Nam Á có liên kết với ISIL; thông tin tình báo tài chính sẵn có đã được phân tích, phân loại; thông tin nguồn mở; các mục tiêu ưu tiên hàng đầu đã được thống nhất hợp tác nhằm phát triển các chiến lược ngăn chặn, có thể được thực hiện thông qua các chương trình trao đổi cán bộ phân tích; và làm việc với các cơ quan thực thi pháp luật hoặc các cơ quan của khu vực để thực hiện các chiến lược ngăn chặn này.

87 Báo cáo được chia sẻ giữa các thành viên của SEA CTF WG và Nhóm tư vấn tình báo tài chính tại Hội nghị cấp cao CTF.

SINGAPORE

Các ấn phẩm ACIP về lạm dụng pháp nhân và rửa tiền dựa trên cơ sở thương mại

88 Hiệp hội công nghiệp AML/ CFT (ACIP), một hiệp hội hợp tác công tư của Singapore, đã xuất bản hai tài liệu về các thông lệ tốt nhất trong ngành liên quan đến các phương thức lạm dụng pháp nhân và tài trợ thương mại/ ML dựa trên cơ sở thương mại, bao gồm các biện pháp phòng ngừa và thông lệ tốt nhất mà ngành này đã áp dụng để giảm thiểu những rủi ro này.

Vui lòng xem báo cáo tại: <https://abs.org.sg/industry-guferences/aml-cft-industry-partnership>

3.2 Sự kết hợp giữa các loại hoạt động ML hoặc TF với các hoạt động phạm tội tiền thân

FIJI

90 Fiji đã bắt đầu xem xét lại NRA của mình vào tháng 11/2018. Việc xem xét lại tập trung vào việc cập nhật đánh giá các mối đe dọa ML mà Fiji phải đối mặt và mức độ nhạy cảm đối với các hoạt động ML của các ngành sau: ngân hàng, nhà cung cấp dịch vụ chuyển tiền, công ty kế toán, công ty luật và đại lý bất động sản.

91 Buôn lậu ma túy như một tội phạm tiền thân của tội ML đang là xu hướng và FIU đang hợp tác chặt chẽ với các nhà điều tra của Lực lượng Cảnh sát Fiji để hỗ trợ lập hồ sơ tài chính và truy tìm tài sản liên quan đến các vụ án ma túy.

Hong Kong, Trung Quốc

Vụ việc điển hình 1

92 Vào tháng 10/2015, Cục Hải quan và Tiêu thụ đặc biệt (C&ED) đã tiến hành một cuộc điều tra về một tổ chức bán hàng giả tại Hồng Kông. Một số quầy hàng, showroom và kho chứa hàng được phát hiện có liên quan đến việc lưu trữ và bán hàng giả. Vào tháng 1/2016, C&ED đã bắt giữ 09 người và thu giữ số hàng giả trị giá 5,8 triệu đô-la Hồng Kông. Cuộc điều tra tài chính cho thấy lượng tiền mặt đáng kể bị nghi là tiền thu được từ việc bán hàng giả, đã được gửi vào các tài khoản ngân hàng cá nhân của tổ chức tội phạm và tổng số tiền đã rửa là 5,75 triệu đô-la Hồng Kông.

93 Vào tháng 5/2018, năm thành viên của tổ chức này đã bị kết án về tội làm hàng giả. Trong số đó, ba bị kết án rửa tiền từ 11 đến 26 tháng tù. Vào tháng 12/2018, tòa án

đã ban hành lệnh tịch thu tài sản trị giá tương đương 1,56 triệu đô-la Hồng Kông do ba thành viên chủ chốt nắm giữ.

Vụ việc điển hình 2

94 Vào tháng 3/2017, C&ED đã tiến hành một chiến dịch chống ma túy dẫn đến việc bắt giữ một cặp vợ chồng và thu giữ 4,6 kg nghi là nọc cần sa và 1 triệu đô-la Hồng Kông bị nghi là tài sản thu được từ ma túy. Cuộc điều tra tài chính cho thấy cặp vợ chồng đã rửa tiền số tiền nghi là thu được từ phạm tội là 5,4 triệu đô-la Hồng Kông.

95 Vào tháng 3/2018, tòa án ban hành lệnh tịch thu tài sản trị giá tương đương 3,7 triệu đô-la HK. Vào tháng 11/2018, người chồng đã bị kết án theo mọi tội trạng và bị tuyên án bốn năm hai tháng tù giam.

INDONESIA

96 Theo thống kê STR gần đây nhất của Indonesia, các hoạt động tội phạm tiền thân chủ yếu gắn liền với ML là lừa đảo, tham nhũng và đánh bạc, trong đó tham nhũng là quan trọng nhất.

NHẬT BẢN

97 Năm 2018, các vụ ML liên quan đến Boryokudan (bao gồm các thành viên Boryokudan, đồng lõa và các bên liên quan khác) chiếm 12,3% của tất cả các vụ việc ML theo Đạo luật trừng phạt tội phạm có tổ chức.

98 Phương thức phổ biến được Boryokudan sử dụng là mở một tài khoản ngân hàng dưới tên giả để lấy tài sản thu từ hoạt động lừa đảo và bán hàng hóa bị đánh cắp.

99 Một nghi phạm tham gia vào việc buôn lậu cần sa đã sử dụng dịch vụ giao hàng tận nhà và sắp xếp cho khách hàng chuyển tổng cộng khoảng 1,6 triệu yên thanh toán vào tài khoản được mở dưới tên của người khác. Hắn bị bắt vì vi phạm Đạo luật về các quy định đặc biệt chống ma túy (che giấu các khoản thu được từ tội phạm liên quan đến ma túy).

MALAYSIA

100 Trong quá trình xác thực những phát hiện ban đầu của các đánh giá mang tính định lượng, các đánh giá mang tính định tính và kết luận tiếp theo cũng được thực hiện dựa trên kết quả của NRA như sau:

- Tham nhũng, lừa đảo và buôn lậu được coi là ba tội phạm liên kết chặt chẽ nhất với các tội phạm nghiêm trọng khác.
- Buôn lậu ma túy và vận chuyển người bất hợp pháp là hai tội phạm nghiêm trọng được coi là có liên hệ chặt chẽ nhất với các mối nguy hại có nguồn gốc từ ngoài nước.
- Lừa đảo được coi là tội phạm nghiêm trọng có liên quan chặt chẽ nhất đến các lĩnh vực được đánh giá, tiếp theo là tham nhũng và trốn thuế.

NEW ZEALAND

Lạm dụng sức lao động và gian lận nhập cư trong ngành xây dựng Auckland

101 NZFIU đã đóng góp cho một cuộc điều tra liên ngành nhằm vào thị trường lao động bất hợp pháp của Malaysia trong ngành xây dựng Auckland. Mục đích của cuộc điều tra là điều tra các tội phạm nhập cư bị nghi ngờ và triệt phá thị trường bất hợp pháp

trong ngành xây dựng Auckland. Kết thúc chiến dịch, 54 cá nhân đã bị trục xuất, 36 cá nhân tự nguyện rời khỏi New Zealand, 15 cá nhân bị gửi thông báo trục xuất và 190 cá nhân đã bị ngừng làm việc bất hợp pháp tại New Zealand; và nhiều tội khác đã bị xử lý bao gồm buôn người, giả mạo danh tính, giả mạo tài liệu, trợ giúp và xúi giục, ML và trốn thuế.

102 Đóng góp của NZFIU vào cuộc điều tra này tập trung vào việc cung cấp phân tích tài chính những thông tin báo cáo hoạt động đáng ngờ (SAR) và hoạt động tài khoản ngân hàng của các nghi phạm để hỗ trợ xác định mạng lưới tội phạm và xác định thêm các đối tượng đáng chú ý. Phân tích của NZFIU cho thấy tiền được chuyển giữa các doanh nghiệp xây dựng và được rút ra từ ngân hàng bằng tiền mặt dưới hình thức trả lương. Cuộc điều tra cũng xác định các giám đốc điều hành các công ty đã vi phạm các điều kiện thị thực của họ, xác định các khoản tiền được tuồn qua các công ty giả mạo. NZFIU tiếp tục cung cấp thông tin cho nhóm điều tra trên cơ sở từng vụ việc để thông tin cho các yêu cầu điều tra sâu hơn nếu có.

PAKISTAN

Vụ việc điển hình 1 - Hàng hóa cướp/ trộm/ ăn cắp

Bối cảnh của vụ việc:

103 Ông SMARZ là nhân viên của một đơn vị cấp vụ của chính phủ và đã duy trì một tài khoản tại Ngân hàng ABC ở Pakistan, nơi ông này nhận được một khoản tiền có giá trị cao thông qua tiền gửi trực tuyến và séc thanh toán bù trừ. Hành vi này không phù hợp với hồ sơ của ông ta và ngân hàng đã nghi ngờ về hoạt động tài khoản. Để xác nhận nguồn tiền, ngân hàng đã cố gắng liên lạc với ông SMARZ qua số điện thoại di động và gửi thư đến địa chỉ cư trú được cung cấp. Số điện thoại không thể liên lạc được và thư bị trả cho ngân hàng. Do xác minh không có kết quả, ngân hàng ABC đã báo cáo STR. Trong quá trình phân tích STR tại Đơn vị giám sát tài chính (FMU), người ta thấy rằng nghi phạm là nhân viên của một vụ thuộc chính phủ và nhận mức lương 17.000 PKR. Tuy nhiên, mặt khác, nhân viên này đã nhận được một khoản tiền lớn thông qua tiền gửi trực tuyến và thanh toán bù trừ từ các chi nhánh khác nhau của ABC Bank. Kể từ khi mở tài khoản ngân hàng của mình, các hoạt động trên tài khoản đã lên tới khoảng 17 triệu PKR.

104 Thông qua việc tìm kiếm trên các phương tiện thông tin đại chúng cho thấy một cá nhân có tên SMARZ đã bị lực lượng an ninh bắt giữ vì liên quan đến việc bán xe bị đánh cắp và các mặt hàng khác. Để xác nhận điều này phù hợp với nghi phạm trong STR, các cuộc tìm kiếm cụ thể đã được tiến hành và người ta thấy rằng ông SMARZ đã cung cấp số điện thoại di động của mình trên internet để bán khẩn cấp và giao dịch các phương tiện cũ. Dựa trên phân tích và hồ sơ ngân hàng, thông tin tình báo tài chính đã được chia sẻ với cơ quan hành pháp để điều tra về trộm cắp, cướp và các hành động khủng bố tiềm ẩn.

Vụ việc điển hình 2 - Buôn lậu ma túy / trốn thuế

Bối cảnh của vụ việc:

105 Các STR do công ty đổi tiền báo cáo về ba cá nhân thường xuyên mua ngoại tệ trên tài khoản theo phương thức cơ cấu. Các cá nhân được báo cáo đã duy trì nhiều tài khoản ở các ngân hàng khác nhau. Đã tìm thấy các thông tin bất lợi trên báo in và phương tiện truyền thông liên quan đến một trong những cá nhân được báo cáo. Được

biết, cá nhân này đã buôn lậu heroin trị giá 7 triệu GBP từ Pakistan đến Vương quốc Anh và đã bị bỏ tù hai mươi năm. Anh ta được ra tù năm 2005. Chính cá nhân này đã mở nhiều tài khoản ở Pakistan từ năm 2011 trở đi. Các tài khoản được mở tại các thành phố khác nhau và được sử dụng để lưu giữ tiền bất hợp pháp. Hơn nữa, phân tích cũng chỉ ra rằng hai nghi phạm khác đã không đăng ký nộp thuế thu nhập cá nhân với Hội đồng Liên bang về thuế mặc dù có doanh số giao dịch lớn trên tài khoản của mình.

Phương thức phạm tội

106 Nghi phạm cùng với các cá nhân khác liên hệ với nhau qua số điện thoại mạng thông thường, đã mua một lượng lớn ngoại tệ theo phương thức cơ cấu và chuyển ra nước ngoài. Các cá nhân có nhiều tài khoản ở các ngân hàng khác nhau. Một cá nhân bị cáo buộc liên quan đến buôn lậu heroin. Người này đã khéo léo mở nhiều tài khoản ở các ngân hàng khác nhau tại nhiều thành phố bằng cách khai báo các doanh nghiệp khác nhau ở mỗi ngân hàng để phân tán nguồn thu và trốn quản lý của các công ty thuế. Anh ta sử dụng các tài khoản trong một khoảng thời gian ngắn rồi đóng lại. Ngược với hồ sơ kinh doanh đã khai báo, anh ta đã thực hiện nhiều giao dịch có giá trị cao. Toàn bộ cách thức giao dịch của đối tượng trong mỗi tài khoản dường như rất đáng ngờ khi chuyển lượng tiền giá trị lớn từ tài khoản này sang tài khoản khác. Mặc dù luồng tiền lớn trong tài khoản của mình, hắn không đăng ký Mã số thuế nước (NTN). Người ta kết luận rằng, cá nhân bị cáo buộc này đã gửi tiền bất hợp pháp thu từ buôn lậu ma túy và chuyển tiền qua các tài khoản khác nhau. Từ việc xem xét tất cả các khía cạnh, thông tin tình báo tài chính đã được chia sẻ với cơ quan thực thi pháp luật để điều tra về khả năng buôn lậu ma túy và trốn thuế.

Vụ việc điển hình 3 - Buôn lậu ma túy

Bối cảnh của vụ việc:

107 Ngân hàng QRS gửi báo cáo STR trên cơ sở thông tin từ phương tiện truyền thông rằng Lực lượng chống ma túy (ANF) đã thu hồi 2,4 kg chất ma túy từ hành lý thuộc sở hữu của một phụ nữ (“ABC”) đang đi xe khách. Ngân hàng thu thập thêm thông tin từ các nguồn và tìm thấy một tài khoản phù hợp trong chi nhánh của họ. Dựa trên thông tin này, Ngân hàng QRS đã gửi báo cáo STR cho FMU.

Phương thức phạm tội

108 Nghi phạm ABC theo ảnh là chủ tài khoản tại Ngân hàng QRS, chi nhánh M từ năm 2003. Cô ta khai báo là nội trợ. Phân tích sao kê tài khoản cho thấy tiền đã được gửi và rút với số lượng nhỏ.

Vụ việc 4- Tham nhũng/ trốn thuế

109 Báo cáo STR do Ngân hàng Alpha và Công ty đổi tiền Beta gửi về ông AX và ông JN trong khi cả hai đều là chủ sở hữu của các nhà máy đường khác nhau. Các nghi phạm có liên quan đến các giao dịch đổi tiền lớn và vi phạm ngưỡng của Ngân hàng Nhà nước Pakistan thông qua việc cơ cấu và sử dụng các phương thức giao dịch khác nhau. Các cá nhân này đã mua một lượng lớn đô-la Mỹ trong một thời gian ngắn bằng tiền mặt mà không có bất kỳ mục đích kinh tế rõ rệt nào. Trong khi đó, họ lại duy trì nhiều tài khoản tiền PKR và ngoại tệ tại Ngân hàng Alpha, nơi mà các hoạt động giao dịch bất thường được báo cáo. Phân tích báo cáo STR cho thấy, các cá nhân này đã rút tiền từ tài khoản PKR để mua USD từ thị trường mở và sau đó gửi vào tài khoản ngoại

tệ. Sau đó, các khoản tiền này được chuyển ra nước ngoài vào các tài khoản cá nhân của họ.

110 Hơn nữa, người ta phát hiện ra rằng những cá nhân này là người thân của những người có ảnh hưởng chính trị (PEP), anh em của ông AX. Trong quá trình phân tích, người ta thấy rằng cùng với ông AX, anh em và cha mẹ của ông cũng đang duy trì các tài khoản tại cùng một chi nhánh của Alpha Bank. Người ta đã lưu ý tới số lượng tiền giao dịch lớn trên các tài khoản của các thành viên gia đình trong một giai đoạn cụ thể, bao gồm các giao dịch tài khoản với nhau và rút tiền mặt và tiền gửi có giá trị cao không phù hợp với khai báo thu nhập tại thời điểm mở tài khoản. Các giao dịch trong các tài khoản này được thực hiện để xóa dấu vết nguồn tiền và che giấu chủ sở hữu hưởng lợi. Lịch sử thuế của các thành viên gia đình tiết lộ rằng số tiền thuế phải nộp không tương xứng với hoạt động giao dịch trên các tài khoản.

111 Dựa trên những điều trên, có nghi ngờ rằng tài khoản của ông AX và JN có thể đã được sử dụng để nhận tiền từ các nguồn khác nhau làm nhiều quá trình kiểm toán và trốn tránh cơ quan thuế. Hơn nữa, do sự tham gia của PEP, có nghi ngờ rằng các hoạt động tài chính được thực hiện từ các Công ty đổi tiền và ngân hàng có thể liên quan đến việc lạm dụng quyền hạn hoặc hành vi tham nhũng. Do đó, thông tin tình báo tài chính đã được chia sẻ với cơ quan hành pháp (LEA) để tìm hiểu thêm và có hành động thích hợp.

THÁI LAN

112 Tiền thu được từ buôn lậu thuốc lá được sử dụng để tài trợ cho các vụ việc ở các tỉnh biên giới phía Nam. Việc buôn lậu được thực hiện bởi các thành viên ở cấp thực thi. Chủ cửa hàng buôn bán nhiều loại hàng lậu có liên quan mật thiết đến nhóm tội phạm. Người ta cũng phát hiện ra rằng, có một trường tôn giáo được sử dụng làm nơi tuyển dụng, tiêm nhiễm hệ tư tưởng và đào tạo, tạo điều kiện cho một số hoạt động khủng bố trong nước. Nhóm này cũng được các đối tượng buôn lậu ma túy hỗ trợ tài chính vì hoạt động của chúng cản trở việc phát hiện buôn lậu.

3.3 Xu hướng mới nổi; xu hướng giảm dần; xu hướng tiếp tục

BRUNEI DERUSSALAM

113 Xu hướng tiếp diễn chủ yếu được nhìn nhận tại các STR mà FIU nhận được trong năm 2018 là tỷ lệ lớn các báo cáo được nộp với dấu hiệu cảnh báo đỏ sau đây:

- Chủ tài khoản thường có nền tảng thu nhập thấp hoặc không có thu nhập;
- Nhiều giao dịch chuyển tiền điện tử được chuyển vào tài khoản từ một tài khoản khác trong cùng một ngân hàng;
- Nhiều lượt chuyển tiền điện tử từ tài khoản này sang tài khoản khác trong cùng một ngân hàng;
- Nhiều khoản tiền gửi dưới ngưỡng trong cùng một ngày;
- Rút tiền mặt ngay sau khi gửi tiền mặt hoặc chuyển khoản điện tử đến;
- Sử dụng tài khoản tiết kiệm cá nhân cho các hoạt động kinh doanh (đặc biệt đối với các công ty một thành viên sở hữu và doanh nghiệp siêu nhỏ); và
- Hành vi của khách hàng đáng ngờ (chủ tài khoản từ chối cung cấp cho ngân hàng xác nhận cho hoạt động trên tài khoản và tiến hành đóng tài khoản của chính họ).

114 Các xu hướng trên đường như là các yếu tố phổ biến của hoạt động tội phạm bao gồm nhận tiền gửi bất hợp pháp, lừa đảo (lừa đảo đầu tư), đôi tiền không được cấp phép và đôi khi, các hoạt động chuyển tiền không được cấp phép. Ngoài ra, các dấu hiệu cũng ám chỉ đến hoạt động bất hợp pháp tiềm ẩn như chuyển tiền thuê hoặc giao dịch trực tuyến mà chủ tài khoản đầu tư tiền thay mặt cho bên thứ ba.

TRUNG QUỐC

Rửa tiền thông qua các nền tảng gây quỹ cộng đồng mạng và phát sóng trực tiếp

115 Cùng với sự phát triển của công nghệ và đổi mới tài chính là sự xuất hiện của tài chính qua internet. Tài chính qua internet, nền tảng gây quỹ qua mạng và phát sóng trực tiếp đang đóng một vai trò quan trọng trong thị trường tài chính hiện nay, vì chúng đặc biệt thu hút khách hàng mới và mở ra các kênh mới cho doanh nghiệp. Tuy nhiên, bọn tội phạm có thể sử dụng hai nền tảng này để rửa tiền.

Rửa tiền bằng cách sử dụng các nền tảng gây quỹ cộng đồng mạng

116 Che giấu mục đích ML bất hợp pháp với mạng lưới gây quỹ qua mạng “hợp pháp”: Tội phạm có thể thiết lập các dự án gây quỹ qua mạng giả trên nền tảng để gây quỹ từ cái gọi là “các nhà đầu tư”, và các nhà đầu tư sẽ thu tiền thông qua thanh toán trực tuyến.

117 Sử dụng phương thức gây quỹ qua mạng xuyên biên giới như những kênh tài trợ khủng bố (TF) mới: Những kẻ khủng bố hoặc những người ủng hộ có thể sử dụng tên giả hoặc địa chỉ IP đăng ký giả mạo để dựng nên một dự án mạng lưới gây quỹ qua mạng. Thông qua những cách này, chúng có thể thu hút những nguồn tiền xuyên biên giới.

118 Sử dụng các nền tảng gây quỹ cộng đồng mạng như trung gian đầu tư để gây quỹ

Rửa tiền bằng cách sử dụng nền tảng phát sóng trực tiếp

119 Tội phạm có thể sử dụng thông tin nhận dạng giả mạo để thiết lập các nền tảng phát sóng trực tiếp và dựng nên những người hâm mộ giả nhằm thưởng số tiền lớn hoặc thu phí thông qua nền tảng phân tích đầu tư tương lai với các đối tượng gọi là chuyên gia đầu tư. Tất cả các phần thưởng và phí đó sẽ được chuyển đến tài khoản được chỉ định thông qua thanh toán trực tuyến. Sau khi phần trăm “phí cho các nền tảng” được khấu trừ bởi các nền tảng của mạng lưới được báo trước, tội phạm có thể rút số tiền còn lại. Phương thức ML dạng chi phí thấp này có thể trốn tránh trách nhiệm thuế và hoạt động giám sát về AML.

Các biện pháp AML của các nền tảng gây quỹ qua mạng và các nền tảng phát sóng trực tiếp

- Tập trung vào tính toàn vẹn thông tin và nhận dạng khách hàng một cách hiệu quả.
- Chú ý đến các giao dịch bất thường và xác định rủi ro ML một cách có hiệu quả.
- Thiết lập cơ chế xếp loại khách hàng và hệ thống chỉ số đánh giá rửa tiền của khách hàng.
- Tăng cường phân tích và giám sát các STR.
- Cải thiện tiêu chuẩn giám sát và phân tích dữ liệu AML.

Xu hướng rửa tiền và đặc điểm mới của các ngân hàng ngầm

120 Là một trong những phương thức chính của ML, các ngân hàng ngầm thường có các đặc điểm của hoạt động gia đình, hệ thống tổ chức chặt chẽ, cơ chế hoạt động ẩn và các kênh vốn cố định. Trong những năm gần đây, với sự đổi mới liên tục các phương thức giao dịch, các ngân hàng ngầm đã phát triển một số tính năng mới trong việc sử dụng các công cụ và phương thức hoạt động:

- Rửa tiền thông qua các tài khoản hải ngoại. Các tài khoản hải ngoại có thể che giấu người kiểm soát thực tế và nguồn tiền. Trong khi đó, tiền từ các tài khoản hải ngoại được giữ trong nước lại rất dễ kiểm soát, điều này khiến chúng trở thành một công cụ mới để các ngân hàng ngầm tiếp nhận và chuyển tiền ra nước ngoài.
- Các ngân hàng trong nước mở tài khoản không cư trú cho các tổ chức ở nước ngoài, nhưng rất khó để các ngân hàng đánh giá được tính xác thực của thông tin mở tài khoản gốc được gửi bởi các khách hàng không cư trú của tài khoản và các nguồn thực sự các khoản tiền trên tài khoản của người không cư trú.
- Xu hướng tài chính mới (mà đại diện là tài chính internet) tạo điều kiện thuận lợi cho các ngân hàng ngầm rửa tiền. Bằng cách sử dụng những khoản thanh toán của bên thứ ba như một kênh giao dịch, thương mại điện tử có các đặc điểm như hiệu quả cao, giao dịch không trực tiếp và khó giám sát, do đó, những các nền tảng như vậy đã trở thành phương thức giao dịch phổ biến cho các ngân hàng ngầm.

Fiji

Xu hướng tiếp diễn: Chiếm đoạt email và giả mạo email

121 Các ngân hàng thương mại, tổ chức tài chính, doanh nghiệp và thành viên của cộng đồng liên tục được FIU khuyến cáo nên thận trọng khi xử lý các hướng dẫn thanh toán qua email cho các giao dịch thương mại nhập khẩu và các giao dịch chuyển tiền cá nhân ra nước ngoài có giá trị lớn. FIU của Fiji ghi nhận xu hướng gia tăng các trường hợp cá nhân và doanh nghiệp trở thành nạn nhân của những mạng lưới chiếm đoạt và giả mạo email trong năm 2018.

122 Các trường hợp gần đây được báo cáo cho FIU Fiji trong năm 2018 về các trường hợp chiếm đoạt và giả mạo email bao gồm:

- Vào tháng 3/2018, một tài khoản email của một khách hàng ngân hàng địa phương đã bị chiếm đoạt và gửi hướng dẫn thanh toán giả mạo đến ngân hàng địa phương. Khoảng 575.000 đô-la FJ đã được chuyển vào một tài khoản ngân hàng nước ngoài thuộc một tổ chức tội phạm mạng.
- Vào tháng 9/2018, trong một vụ án liên quan đến ML qua mạng, 556.000 đô-la FJ đã bị lừa đảo chuyển từ tài khoản ngân hàng của một doanh nghiệp địa phương sang số tài khoản ngân hàng hải ngoại “không chính xác”. Trong trường hợp này, email kinh doanh của nhà cung cấp nước ngoài đã bị chiếm đoạt.
- Vào tháng 10/2018, số tiền khoảng 27.000 đô-la FJ thu được từ việc bán cổ phần đầu tư của một nhà đầu tư địa phương đang cư trú ở nước ngoài, đã được chuyển đến một tài khoản ngân hàng của tội phạm mạng tại một nước khác do email bị chiếm đoạt.
- Vào tháng 10/2018, tiền thu được từ thanh toán bất động sản khoảng 845.000 đô-la FJ đã được chuyển vào tài khoản ngân hàng nước ngoài của một tội phạm mạng giả danh là người thụ hưởng tài sản. Dường như các tài khoản email của người thụ hưởng và bên trong nước đã bị chiếm đoạt.

123 Bất kỳ giao dịch thương mại ở nước ngoài đáng ngờ hoặc chuyển tiền cá nhân lớn có thể liên quan đến việc chiếm đoạt và giả mạo email nào cũng phải được báo cáo ngay lập tức dưới dạng báo cáo giao dịch đáng ngờ cho FIU Fiji. Các ngân hàng thương mại và các nhà cung cấp dịch vụ chuyển tiền đã được nhắc nhở tiến hành rà soát thông tin khách hàng nâng cao đối với các chỉ thị thanh toán đáng ngờ.

FIU Fiji đã ghi nhận sự suy giảm trong các xu hướng sau:

- việc sử dụng tài liệu những giấy tờ giả mạo để thực hiện các giao dịch tài chính; và
- số lượng các trường hợp mạo danh được báo cáo cho FIU.

INDONESIA

124 Ngành ngân hàng vẫn đang bị tội phạm ML sử dụng để rửa những khoản thu phạm tội. Dựa trên các phán quyết của tòa án, những giao dịch chuyển khoản qua ATM, gửi tiền mặt qua giao dịch viên, giao dịch sử dụng thu thập dữ liệu điện tử (EDC) và chuyển khoản qua hoạt động ngân hàng trên điện thoại di động cho thấy chiều hướng tăng lên. Những giao dịch tiền mặt (tức là đưa và nhận tiền trực tiếp) cho thấy xu hướng giảm dựa trên nghiên cứu của Indonesia về kết quả các phán quyết của tòa án đưa ra năm 2017.

125 Gần đây, tội phạm lừa đảo và ma túy ngày càng gắn với ML, mặc dù tham nhũng vẫn là tội phạm tiền thân gắn với ML nhất.

NHẬT BẢN

126 Các trường hợp che giấu các khoản thu phạm tội trong năm 2017 bao gồm phần lớn các trường hợp kẻ phạm tội cố gắng chuyển tiền vào tài khoản ngân hàng dưới tên của người khác. Đây là một xu hướng chính được nhìn nhận trong tội phạm ML.

127 Thêm vào đó, tội phạm sử dụng các phương thức khác nhau để tránh sự theo dõi của các cơ quan điều tra gồm: bán hàng ăn cắp dùng tên giả, che giấu các khoản thu phạm tội trong nhà kho theo hợp đồng đứng tên người khác.

LÀO

128 Trong tháng 2 năm 2018 đến tháng 12 năm 2018, làm séc giả hoặc sử dụng séc giả là xu hướng ML giảm dần theo thống kê tội phạm tiền thân. Tuy nhiên, lừa đảo lại là xu hướng tiếp tục xuất hiện.

MACAO, TRUNG QUỐC

129 Trong suốt khoảng thời gian từ tháng 1 đến tháng 6/2018, Văn phòng tình báo tài chính (GIF) đã nhận tổng số 2.187 STR, với 1.128 STR từ lĩnh vực trò chơi, 617 STR từ lĩnh vực tài chính (bao gồm ngân hàng, bảo hiểm và trung gian tài chính) và 442 STR từ các ngành khác.

130 Các phương thức ML phổ biến được phát hiện từ các STR nhận được như sau:

- ☐ Chuyển đổi chip mà không có/ chỉ có các hoạt động đánh bạc tối thiểu;
- ☐ Rút tiền mặt lớn bất thường;
- ☐ Mua hàng hóa xách tay và vật có giá trị;
- ☐ Nghi ngờ ngân hàng ngầm / dịch vụ chuyển tiền thay thế;
- ☐ Gửi tiền mặt đáng kể với nguồn tiền không thể kiểm chứng;

- ☐ Nghi ngờ sử dụng thẻ tín dụng / thẻ ghi nợ để mua hàng hóa có giá trị cao và chiết khấu bằng tiền mặt;
- ☐ Đổi chip / người ghi điểm thưởng đổi điểm thưởng thay mặt cho bên thứ ba;
- ☐ Sử dụng ATM, dịch vụ ngân hàng điện thoại, máy gửi tiền mặt;
- ☐ Đổi tiền / chuyển sang tiền mặt;
- ☐ Giao dịch định thực hiện nhưng không thành công;
- ☐ Giao dịch ngoại hối với nguồn tiền không xác định;
- ☐ Sử dụng séc / chuyển khoản, v.v. để chuyển tiền;
- ☐ Không thể cung cấp ID / thông tin cá nhân quan trọng; và
- ☐ Chuyển tiền điện tử đáng ngờ.

131 Từ tháng 1 đến tháng 6/2018, 60 STRs đã được chuyển giao cho Văn phòng công tố. Những vụ việc này chủ yếu liên quan đến lừa đảo.

132 Theo như quan sát các STR nhận được, sự gia tăng lừa đảo trong chuyển tiền và sử dụng chuyển khoản bằng séc / tài khoản, đã là tâm điểm được lưu ý của ngành ngân hàng trong một vài tháng gần đây. Ngoài các trường hợp điển hình là ngân hàng thụ hưởng địa phương nhận được điện báo từ ngân hàng đặt lệnh hoặc email từ nạn nhân tố cáo rằng các khoản chuyển tiền có liên quan đến các hành vi lừa đảo, một số vụ việc đã được báo cáo cho Văn phòng Công tố dựa trên thông tin tình báo nhận được trong nước hoặc ở nước ngoài. Điều này cho thấy hợp tác quốc tế và chia sẻ thông tin hiệu quả đã góp phần vào các cuộc điều tra, truy tố và kết án hiệu quả và thành công trong một số vụ lừa đảo.

133 Một số trường hợp, chẳng hạn như lừa đảo qua truyền thông xã hội, lừa đảo hẹn hò trực tuyến và lừa đảo mua sắm điện tử đã xuất hiện trong nửa đầu năm 2018. Cảnh sát tư pháp đã duy trì hợp tác chặt chẽ với các cơ quan thực thi ở nước ngoài, và nhắc nhở công chúng phải đề phòng và không tiết lộ thông tin tài khoản và mã xác nhận giao dịch cho bất kỳ ai để tránh bị mất tiền.

MALAYSIA

Xu hướng tiếp diễn qua phân tích STR

134 Xu hướng gia tăng số STR được báo cáo với tổng mức tăng hàng năm là 23% từ năm 2008 có thể có sự đóng góp từ sự nhận thức tăng lên và việc giám sát giao dịch nói chung được nâng cao bởi các tổ chức báo cáo. Nó cũng có được từ sự cam kết hiệu quả của khu vực công và tư, bao gồm cả việc chia sẻ thông tin rủi ro về tội phạm có rủi ro cao, hồ sơ có rủi ro TF và nền tảng chia sẻ thông tin thường xuyên giữa khu vực công và tư. Các STR được báo cáo chủ yếu từ lĩnh vực ngân hàng, sòng bạc và kinh doanh dịch vụ tiền tệ.

135 Các tội phạm bị nghi ngờ chính được các tổ chức báo cáo là gian lận / lừa đảo, trốn thuế, tội phạm có tổ chức và tham nhũng.

Xu hướng mới nổi qua phân tích STR

136 Những kẻ lừa đảo chuyển từ việc sử dụng tài khoản cá nhân sang thiết lập những tài khoản doanh nghiệp để tránh sự nghi ngờ.

Xu hướng gia tăng qua điều tra (ML, TF và tội phạm tiền thân)

137 Giao dịch tiền mặt vẫn là phương thức ưa thích để di chuyển các khoản thu bất hợp pháp (nhận, chuyển và chi tiêu).

138 Sử dụng tài khoản của bên thứ ba bao gồm cả những người cho mượn tài khoản để nhận và chuyển các khoản thu bất hợp pháp.

139 Rửa qua các hàng hóa có giá trị cao, như đồ trang sức và hàng hiệu.

NEW ZEALAND

Mối đe dọa rửa tiền đối với Nam Thái Bình Dương

140 Phân tích của NZFIU chỉ ra rằng ngành ngân hàng ở các đảo Nam Thái Bình Dương đang là mục tiêu cho ML, lừa đảo và khả năng xâm nhập hình sự. Có trường hợp, một công dân New Zealand bị nghi ngờ có mối liên hệ với tội phạm có tổ chức đã được phát hiện cố gắng thiết lập cơ chế rửa tiền tại một số nước ở Nam Thái Bình Dương. Ông ta là một đại lý thành lập công ty và có kiến thức sâu rộng về các hệ thống pháp lý, ngân hàng quốc tế và AML. NZFIU lo ngại rằng cá nhân này đang toan tính tạo điều kiện cho hoạt động rửa tiền xuyên nước qua Nam Thái Bình Dương thay mặt cho các nhóm tội phạm có tổ chức.

141 Trong một mạng lưới khác không liên quan nhưng trong đó có toan tính tương tự nhằm thành lập ngân hàng, chính phủ một nước Nam Thái Bình Dương gần đây đã được đề xuất đổi quyền đối với tài nguyên thiên nhiên có giá trị thương mại với việc cấp giấy phép ngân hàng cho một công ty được đăng ký tại một nước thứ ba. NZFIU đánh giá rằng đề xuất này gần như chắc chắn là lừa đảo và có thể là một nỗ lực để có được quyền tiếp cận vào ngành ngân hàng Nam Thái Bình Dương cho các mục đích bất chính.

Gia tăng xuất hiện băng đảng ở Nam Thái Bình Dương

142 Số lượng thành viên băng đảng gia tăng di chuyển đến các nước ở Nam Thái Bình Dương là môi trường tốt cho các băng đảng thực hiện một loạt các hoạt động tội phạm có tổ chức, đặc biệt là mang các chất bất hợp pháp ra và vào khu vực và vào New Zealand. Các nhóm tội phạm có tổ chức (OCG) của New Zealand có liên hệ gia đình mạnh mẽ với Nam Thái Bình Dương, tăng cơ hội tuyển quân và kết nối các mạng lưới với New Zealand. Các kỹ thuật ML bị phát hiện bởi NZFIU bao gồm buôn lậu tiền mặt, chuyển tiền điện tử, cơ cấu gửi tiền mặt và sử dụng các nước ở Nam Thái Bình Dương như những thiên đường thuế.

Rửa tiền thông qua các nền tảng đánh bạc trực tuyến

143 Việc báo cáo tới cho FIU của NZ cho thấy xu hướng ML tiếp diễn thông qua các nền tảng đánh bạc trực tuyến. Báo cáo SAR cho thấy các cá nhân có liên hệ với mạng lưới ma túy và OCG tiếp tục sử dụng các trang web cờ bạc trực tuyến, nhận các khoản thanh toán lớn vào tài khoản ngân hàng ở New Zealand như “những khoản hoàn lại tiền”. Vì các trang web này được vận hành ở hải ngoại, chúng gần như chắc chắn bị lạm dụng để né tránh các biện pháp kiểm soát AML của New Zealand và cho phép những kẻ phạm tội dịch chuyển các khoản tiền bất hợp pháp vào và ra khỏi nước này mà không bị phát hiện.

PAKISTAN

144 Xu hướng gia tăng trong việc tiếp nhận các STR liên quan đến trốn thuế đã được nhận thấy trong năm 2018.

145 Xu hướng tiếp diễn trong việc tiếp nhận các STR liên quan đến Hawala /Hundi đã được nhận thấy trong năm 2018.

4. CÁC VỤ VIỆC ĐIỂN HÌNH VỀ ML VÀ TF

4.1 Tài trợ khủng bố

MALAYSIA

146 Các nhà điều tra đã xác định tổng cộng hơn 7.000 USD được huy động thông qua các đối tượng có cảm tình với khủng bố tại địa phương kể từ năm 2016, theo chỉ đạo của những kẻ khủng bố Malaysia ở Syria thông qua một ứng dụng nhắn tin được mã hóa chặt chẽ. Sau đó, một phần quan trọng của những khoản tiền huy động này đã được chuyển bởi các đối tượng hỗ trợ tài chính trong mạng lưới thông qua các công ty chuyển tiền đến các nước gần Syria và Iraq hoặc quá cảnh qua các thẻ chế khác.

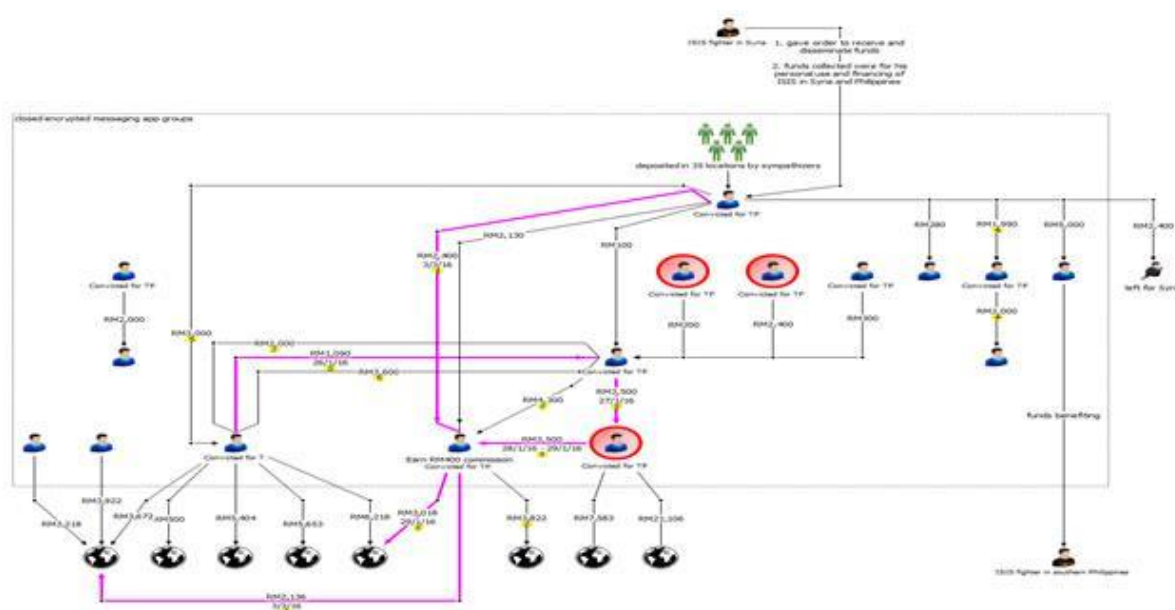
147 Các đối tượng hỗ trợ tài chính đã cố gắng che giấu các dấu vết của việc chuyển tiền bằng cách tự chuyển tiền qua lại nhiều lần trước khi chuyển ra nước ngoài. Người ta tin rằng, đích sử dụng các khoản tiền này có thể gồm mua xe tải để vận chuyển hàng hóa, túi thuốc nổ hoặc hỗ trợ chi phí đi lại và sinh hoạt của những kẻ khủng bố dịch chuyển đến hoặc ở trong Syria.

148 Một trong những nghi phạm đã được nhận dạng bởi một tổ chức báo cáo sau khi hệ thống giám sát giao dịch của tổ chức này tìm thấy một dấu vết tài chính giữa những đối tượng tạo điều kiện tài chính mà tên của chúng đã được cảnh báo bởi các cơ quan có thẩm quyền trước đó.

149 Nhìn chung, tổng cộng chín đối tượng hỗ trợ tài chính trong mạng lưới này đã bị kết án tổng cộng 65 năm tù (từ bốn đến mười năm) cho các hoạt động tài trợ khủng bố được quy định theo các phần 130N (b), 130O (1) và 130Q (1) của Bộ luật hình sự.

150 Các phương thức TF được sử dụng bao gồm:

- ☐ Chuyển tiền điện tử / Sử dụng tài khoản ngân hàng nước ngoài.
- ☐ Hoạt động ngân hàng ngầm / dịch vụ chuyển tiền thay thế / Hawala.



PHILIPIN

MG và cuộc vây hãm thành phố M

151 Nhóm Maute (MG) là một nhóm được Daesh / Nhà nước Hồi giáo ở Iraq và Syria (ISIS) truyền cảm hứng có trụ sở tại miền Nam Philippines. Nhóm này bao gồm các gia tộc được biết đến trong khu vực thuộc về các gia đình nổi tiếng.

152 Dựa trên các phân tích và phát hiện, các thành viên thuộc mạng lưới CJ (một tổ chức khủng bố nước ngoài) thực hiện chuyển tiền quốc tế đến Philippines từ tháng 1 đến tháng 2/2017. Những giao dịch này đều được nhận thông qua cùng một đại lý chuyển tiền và mạng lưới các đối tượng sử dụng nền tảng chuyển tiền quốc tế.

153 Thông tin từ các quan chức cảnh sát nước ngoài chỉ ra rằng các quỹ đã được cung cấp tại nước I dưới hình thức chuyển tiền hawala, theo đó các tay súng nước ngoài của nước I chiến đấu cho ISIS nằm tại Syria được chỉ dẫn bán tài sản ở nước I. Tiền thu được từ các giao dịch bán này chỉ thị chuyển cho CJ đặt tại nước I, trong khi giá trị các quỹ có từ việc bán tài sản này lại được cung cấp thông qua ISIS cho các tay súng nước ngoài của nước I tại Syria. Sử dụng hệ thống này, các tay súng nước ngoài ở Syria đã có thể tiếp cận các quỹ và tiền được cung cấp trong nước I mà không cần chuyển tiền quốc tế, chuyển tiền hoặc thực sự vận chuyển tiền. Thông tin bổ sung cũng chỉ ra rằng, các tay súng nước ngoài của nước I chiến đấu cho ISIS đã khởi hành đến Syria và đã để lại tài khoản ngân hàng và thẻ ngân hàng của họ cho các thành viên của CJ sử dụng.

Mạng lưới có liên kết với MG gửi từ nước T đến Philippines

154 Thông tin từ Nước I chỉ ra rằng các quỹ hỗ trợ cho Cuộc vây hãm thành phố M đã được gửi đến Philippines từ một mạng lưới các cá nhân nằm tại Nước T. Thông tin bổ sung cũng chỉ ra rằng cùng một mạng lưới các cá nhân trong Nước T này cũng gửi tiền về Nước T khoảng 20.000 đô la Mỹ đã được gửi đến Philippines từ Nước T. Các cá nhân nói trên đã nhận được tiền ở Philippines thông qua hai lần chuyển tiền riêng biệt.

Mạng lưới có liên kết với MG gửi cho Nước I

155 Một mạng lưới các cá nhân được xác định gửi tiền từ M City đến nước I vào cuối năm 2016. Tiền được gửi chủ yếu bằng cách sử dụng hai doanh nghiệp chuyển tiền, CMAL và EMT. Chủ sở hữu của CMAL và người có thể là vợ của anh ta, cùng với một cá nhân khác, đã thực hiện 12 giao dịch gửi từ Philippines đến nước I từ tháng 7/2016 đến tháng 1/2017. Có thể các giao dịch này được liên kết với các hoạt động kinh doanh hợp pháp, với mỗi người nhận tại nước I điều hành một doanh nghiệp; tuy nhiên, các giao dịch này dường như không liên quan đến hoạt động kinh doanh. Các doanh nghiệp nói trên đã không được đăng ký, và không có bất kỳ hồ sơ nào về hoạt động xuất nhập khẩu liên quan.

Mạng lưới các đối tượng nữ hỗ trợ tài chính ở tại Philippines

156 Có thể có một mạng lưới các đối tượng nữ hỗ trợ tài chính ở tại Nam Philippines đã chuyển tiền thay mặt cho các nhóm liên kết ISIS và ISIS ở Đông Nam Á.

157 Đối tượng nữ hỗ trợ tài chính ME đã nhận được tiền từ nước M và nước K từ những cá nhân cũng đã gửi tiền cho đối tượng nữ hỗ trợ tài chính MM. Cả hai đối tượng nữ hỗ trợ tài chính ME và MM đều nhận được tiền ở Philippines từ một cá nhân nhất định tại nước M và một cá nhân nhất định tại nước K từ năm 2015 đến 2016. Mạng lưới này cũng đã gửi tiền cho người vợ thứ hai của Dr. MA. Đối tượng nữ hỗ trợ tài chính

ME và một đôi tượng nữ hỗ trợ tài chính EI khác đều gửi tiền cho người vợ thứ hai của Dr. MA tại nước M trong năm 2016.

Các tay súng khủng bố nước ngoài

158 Bảy tay súng nước ngoài của nước I đã được nhận dạng và đi đến Philippines trước khi bao vây thành phố M. Phân tích đã xác định rằng nhiều khả năng những cá nhân này sẽ không có tiền hoặc quỹ để tổ chức đi lại, bao gồm hộ chiếu, thị thực và tự mua vé được. Thông tin chỉ ra rằng, một số công dân của nước I được cho là đã nhận hỗ trợ cho việc đi lại của bảy tay súng nước ngoài của nước I đi đến Philippines. Cũng có nghi ngờ rằng, một công dân khác của nước I đã hỗ trợ cho việc đi lại của ba tay súng nước ngoài còn lại của nước I. Các cơ quan của nước I đã bắt giữ các cá nhân nói trên với cáo buộc tài trợ khủng bố.

Xác định công ty chuyển tiền có rủi ro cao

159 CMAL được coi là đối tượng chuyển tiền có rủi ro TF cao. CMAL không còn đăng ký như một tổ chức cung cấp dịch vụ tiền tệ (MSP) nhưng dường như được đăng ký ngay trước cuộc bao vây diễn ra. CMAL chưa bao giờ được đăng ký với AMLC dưới dạng chuyển tiền (MR) và chưa gửi bất kỳ báo cáo giao dịch nào. Chủ sở hữu của CMAL được ghi nhận là HPM, người này không vận hành tài khoản doanh nghiệp cho CMAL nhưng sử dụng tài khoản ngân hàng cá nhân của mình để hỗ trợ cho các giao dịch chuyển tiền. CMAL cũng được xác định bởi FIU của nước A là đại lý chuyển tiền có nhận tiền từ một nhóm trong nước và thực hiện cơ cấu các giao dịch gửi đến Philippines vào tháng 4/2013. Nhóm trong nước A bị nghi ngờ có liên kết với tài trợ khủng bố. Các giao dịch này đại diện cho phần lớn các giao dịch nhận được thông qua CMAL cho đến năm 2016.

160 Trong khoảng thời gian từ tháng 11/2013 đến tháng 6/2018, nền tảng trung gian chuyển tiền quốc tế đã nộp 22 SAR trong đó xác định CMAL là đại lý chuyển hoặc tchi trả trong 49 giao dịch chuyển tiền đáng ngờ được thực hiện từ ngày 11/7/2013 đến ngày 20/3/2017. Phần lớn các SAR được nộp là do nghi ngờ TF.

161 CMAL đã thực hiện thêm 6 lần với vai trò đại lý chi trả thay vì đại lý chuyển tiền dựa trên các giao dịch chuyển tiền đáng ngờ. Hầu hết các giao dịch chuyển tiền đáng ngờ được gửi đến CMAL, với tư cách là đại lý chi trả, đều khởi phát trong Philippines, sau đó đến Indonesia, nơi đã chuyển các khoản tiền có giá trị cao nhất.

4.2 Sử dụng ngân hàng hải ngoại, công ty kinh doanh quốc tế và tín thác hải ngoại

TRUNG QUỐC

162 Vào tháng 12 năm 2017, cơ quan giám sát, cơ quan thuế và cảnh sát đã điều tra một nghi phạm, người đã giả mạo sử dụng những biên lai đổi tiền trong thương mại để có được những khoản thu trợ cấp giảm giá và che giấu những khoản có được từ tội phạm về thuế thông qua hoạt động ngân hàng ngầm và nhiều công ty được đăng ký tại Thành phố H.

163 Vào tháng 2/2018, vụ việc đã được giải quyết. Nghi phạm X thành lập công ty giả mạo Y, mua hóa đơn VAT thông qua bên thứ ba, sau đó giả mạo hóa đơn nộp thuế cho công ty Y. Nghi phạm X và Nghi phạm Z cũng có hành vi phạm tội về thuế bằng cách giả mạo hóa đơn, mua tờ khai hải quan, làm giả những hàng hóa đầu ra và đối ngoại hối bất hợp pháp. Theo cảnh sát, tổng giá trị hóa đơn VAT và hoàn thuế đã đạt

hơn hàng triệu nhân dân tệ. Hiện tại, vụ việc đã được chuyển cho công tố viên để truy tố.

PAKISTAN

164 Ông bà XYZ (gia đình kinh doanh nổi tiếng ở Pakistan) có dính líu đến chuyển vốn trái phép và trốn thuế bằng cách sử dụng các công ty hải ngoại. Các STR được các công ty đổi tiền báo cáo về trên cơ sở các giao dịch cơ cấu mua ngoại tệ (USD) và cổ tình vi phạm ngưỡng mua ngoại tệ của Ngân hàng Trung ương thông qua cơ cấu và sử dụng các công ty đổi tiền khác nhau. Số tiền liên quan (được xác định thông qua CTR) là đáng kể và đã gây nghi ngờ. FMU đã xác định rằng, các nghi phạm duy trì nhiều tài khoản ngoại tệ tại các ngân hàng khác nhau. Các khía cạnh giao dịch tổng thể cho thấy rằng họ đã rút tiền từ tài khoản nội tệ của mình để mua ngoại tệ, gửi vào tài khoản ngoại tệ, cuối cùng chuyển ra nước ngoài. Trong quá trình phân tích STR, tên của các nghi phạm cũng được tìm thấy trong các giấy tờ bị rò rỉ dưới dạng chủ sở hữu các công ty hải ngoại và họ đang tiến hành bán công ty của mình cho một công ty nước ngoài. Cũng có dấu hiệu không khai báo trong việc bán các công ty cho người mua nước ngoài. Người ta nghi ngờ rằng ông bà XYZ đã thực hiện khai báo không trung thực và gian lận, vi phạm các quy định ngoại hối, chuyển vốn khi không được ủy quyền, trốn thuế và các hành vi phạm tội khác. Tổng giám đốc FMU đã ra lệnh đóng băng các tài khoản. Thông tin tình báo tài chính đã được chia sẻ với nhiều cơ quan theo Luật AML.

165 Trên cơ sở giới thiệu của FMU, cơ quan thuế đã thu hồi số tiền thuế 6,2 tỷ PKR.

PHILIPPIN

166 Vào tháng 5/2017, FIU của nước U đã yêu cầu cung cấp thông tin thông qua trang Web bảo mật của nhóm Egmont (ESW) về các cá nhân và tổ chức khác nhau được cho là tham gia rửa tiền, lừa đảo chứng khoán và chuyển tiền điện tử.

167 Thông tin liên quan đến GLADS, một tổ chức hoàn toàn thuộc sở hữu của GRALE được đăng ký tại Philippines. Thông tin phát hiện ông DT, người có lợi ích đa số tại GRALE, đã tài trợ cho việc thành lập Quỹ thu nhập G (“Quỹ”) vào tháng 10/2011. Ông DT đóng vai trò là người được ủy thác, chủ tịch, chủ tịch và tổng giám đốc và là nhà quản lý đồng đầu tư của Quỹ từ năm 2012 đến 2014. Quỹ dự định tạo thu nhập cho các nhà đầu tư /cổ đông của mình bằng cách đầu tư chủ yếu vào các giấy nợ cá nhân được ký bởi các sinh viên sau đại học và chuyên tu và sinh viên mới tốt nghiệp trong các lĩnh vực việc làm có thu nhập cao. Vào tháng 1/2012, GRALE trở thành giám sát viên cho Quỹ đối với tất cả các tài liệu có liên quan đến những khoản vay thích hợp, bao gồm cả các giấy nhận nợ ban đầu thông qua Thỏa thuận phục vụ khoản vay.

168 GRALE bị cáo buộc bắt đầu làm mất tiền và ông DT đã nghĩ ra một gian kế là tạo ra các khoản vay giả mạo mà Quỹ phải trả để giữ cho công ty của ông ta sống sót và duy trì lối sống xa hoa của mình. Theo kế hoạch lừa đảo của ông DT, những khoản thu từ tiền cho vay được chuyển đến TF-LLC, một công ty trách nhiệm hữu hạn mà ông DT cũng kiểm soát, thay vì chuyển tới một ngân hàng chính thức phát hành khoản vay cho người vay.

169 Vụ lừa đảo được phát hiện khi các nhân viên của GRALE gửi nhầm bản sao kê khoản vay cho bạn cùng phòng đại học trước đây của ông DT, người được nêu tên đang có một khoản vay với số dư gốc là 342.000 USD. Vào tháng 12/2014, Văn phòng Điều tra của nước U đã thẩm vấn bạn cùng phòng đại học của ông DT, người này cho biết

chưa từng tiến hành kinh doanh, vay tiền hoặc nhận khoản vay từ ông DT, GRALE hoặc Quỹ. Điều này dẫn đến việc Ủy ban chứng khoán của nước U mở cuộc điều tra về ông DT, bắt giữ và đưa ra nhiều cáo buộc dân sự chống lại ông này. Một trong những người được ủy thác của Quỹ, ông MS, đã có bản khai cáo buộc ông DT đã khuyên những người được ủy thác độc lập của Quỹ đầu tư gián tiếp vào một loạt các giao dịch bao thanh toán tại Philippines. Điều này sẽ bao gồm cả việc cho vay các khoản tiền vào một trong hai công ty trách nhiệm hữu hạn tiềm năng đóng vai trò trung gian tại Nước U - LCLLC hoặc LC2LLC (“Các công ty LC”). Đến lượt mình, các công ty LC này sẽ cho các đối tác ở Philippines vay các khoản tiền dưới dạng một phần của hàng loạt giao dịch bao thanh toán. Các khoản thanh toán lãi và trả nợ gốc của các đối tác giao dịch bao thanh toán sau đó sẽ được gửi lại cho Quỹ thông qua các Công ty LC. Quỹ bị cáo buộc đã cho vay tổng cộng 8,065,759.44 USD từ tháng 4/2013 đến tháng 10/2014 cho các công ty LC. Tuy nhiên, số tiền được chuyển từ Quỹ đến các công ty LC không được đầu tư mà thay vào đó, được chuyển sang tài khoản hoạt động của GRALE. Từ đó, một số khoản thu được giữ lại cho chi phí hoạt động của GRALE, và một số được chuyển cho GLADS, công ty Philippines hoàn toàn thuộc sở hữu của GRALE. Ngoài ông DT, trong số những cá nhân đăng ký thành lập GLADS còn có các luật sư người Philippines có mối liên kết với một văn phòng luật sư nổi tiếng trong nước.

170 Một số quỹ đã bị cáo buộc rửa tiền trong ELI Corp, một công ty đăng ký thành lập ở Philippines. Ông DT rõ ràng đã đưa ra những giấy nhận nợ giả mạo cho rằng các công ty LC do ông BS đại diện, cho vay tiền đối với ELI Corp do ông WD nào đó làm đại diện. Các giấy nhận nợ giả được phát hành từ tháng 4 đến tháng 11/2015 có tổng giá trị là 210,30 triệu PHP. Những khoản tiền trên được cho là được ELI Corp cho vay đối với nhiều tổ chức kinh doanh khác nhau của Philippines thông qua các Thỏa thuận về vốn lưu động (“WCA”). Nhưng hóa ra những WCA này cũng là giả mạo.

171 FIU Philippines đã hành động dựa trên những yêu cầu và phản hồi được cung cấp bao gồm những người hưởng lợi cuối cùng có thể có của các quỹ có nguồn gốc từ các công ty do ông DT kiểm soát từ nước U.

172 Vào tháng 11/2017, nước U phát hiện thông tin mới do FIU cung cấp rất hữu ích, và do đó, đã đưa ra một yêu cầu khác, lần này tập trung vào những người tham gia mới được FIU xác định trong phản hồi trước đó để đưa vào điều tra vụ án. FIU cũng đã thực hiện theo yêu cầu và cung cấp thông tin tìm kiếm được trong vòng ba tháng kể từ khi nhận được yêu cầu tiếp theo.

4.3 Sử dụng tiền ảo

AUSTRALIA

Tạm ngừng đăng ký kinh doanh tiền kỹ thuật số do liên quan đến tội phạm có tổ chức

173 AUSTRAC đã tạm ngừng đăng ký của hai doanh nghiệp đổi tiền kỹ thuật số sau khi Cảnh sát liên bang Úc (AFP) bắt giữ một người đàn ông.

174 Vụ việc bắt giữ của AFP được tiến hành sau một cuộc điều tra đối với những người có trách nhiệm cho cáo buộc nhập ma túy qua biên giới được kiểm soát bằng đường gửi bưu kiện quốc tế. Các cuộc điều tra đã dẫn các sỹ quan của AFP đến việc đưa ra lệnh khám xét và niêm phong chất steroids, tiền Úc và tiền kỹ thuật số vào đầu năm 2019. Hình phạt đã được đưa ra cho một số cá nhân liên quan đến việc nhập khẩu, buôn lậu và sở hữu hoảng 30kg ma túy bất hợp pháp, bao gồm cả MDMA, cocaine, methamphetamine và ketamine

175 Người ta cũng cáo buộc bằng nhóm tội phạm sử dụng nhiều trang dark web, tài khoản bitcoin và các doanh nghiệp hợp pháp để sản xuất, thanh toán và phân phối ma túy bất hợp pháp.

176 Trong một hành động khác, Lực lượng đặc nhiệm tịch thu tài sản phạm tội do AFP dẫn đầu đã thực hiện tạm giữ tài sản liên quan đến cuộc điều tra. Lệnh đã được lấy từ Tòa án bang Victoria để tạm giữ tài sản trị giá hơn AUD2 million.

177 Nó bao gồm hàng loạt tài khoản ngân hàng, các bất động sản, phương tiện giao thông, xe máy, tiền mặt và tiền kỹ thuật số. Các lệnh tạm giữ dduwwocj đưa ra theo Đạo luật về tịch thu tài sản phạm tội năm 2002 (Cth).

178 Sau các cuộc bắt giữ, AUSTRAC đã ngừng đăng ký cho 2 doanh nghiệp đối tiền kỹ thuật số nơi 1 trong những người đàn ông bị bắt giữ là thành viên chính, laoij bỏ khả năng họ được tiếp tục hoạt động kinh doanh này.

TRUNG QUỐC

Vụ việc điển hình thứ nhất

179 Tập đoàn A giao dịch với U-bao, là một hệ thống lưu thông tiền kỹ thuật số. Các nghi phạm liên quan đã sử dụng U-bao để thu tiền bất hợp pháp, các khoản tiền này đổ vào hệ thống U-bao thông qua nhiều tài khoản. Hàng trăm đối tác có liên quan, những ghi chú / mã các giao dịch là “U-bao”. Có nhiều thông tin tiêu cực công khai về Tập đoàn A, bao gồm cả việc kinh doanh đa cấp. Các tài khoản của một nghi phạm có rất nhiều giao dịch liên quan đến công ty của Tập đoàn A. Tổng giá trị giao dịch liên quan đến vụ việc này đã lên tới hàng triệu nhân dân tệ và thông tin liên quan về vụ việc này đã được chuyển cho cảnh sát.

Vụ việc điển hình thứ hai

180 WEIKA là một loại tiền ảo được phát hành qua nền tảng mạng xuyên biên giới. Loại tiền này có thể được sử dụng để tiêu dùng và có thể tăng giá trị thông qua việc mua cổ phần liên quan đến số lượng WEIKA nhất định. WEIKA thu phí các thành viên. Tài khoản của Nghi phạm B thường xuyên có khoản tiền vào và ra, và các khoản tiền này được chuyển qua các lĩnh vực và khu vực khác nhau. Ghi chú / mã giao dịch của Nghi phạm B và các đối tác là “Onecoin”, “mã kích hoạt WEIKA”, “mua gói động lực”, v.v. Họ bị nghi ngờ sử dụng WEIKA theo kiểu kinh doanh đa cấp và rửa tiền, tổng số tiền trong trường hợp này đã lên tới hàng triệu nhân dân tệ.

ĐÀI LOAN

181 IRS, là một pháp nhân được thành lập ở quốc gia S năm 2016, đã kinh doanh Bitcoin theo mô hình Ponzi để lừa đảo các nhà đầu tư. Từ tháng 10 năm 2016, cá nhân A là người chịu trách nhiệm khu vực Đài Loan, Trung Quốc và phụ trách điều hành hoạt động chung của tập đoàn, tuyển dụng nhà đầu tư, phân phối tiền thưởng, v.v. cá nhân A và các đồng phạm đã tổ chức nhiều cuộc hội thảo để giải thích các kế hoạch đầu tư, cơ chế lợi nhuận và khen thưởng của IRS cho những người tham gia. Họ đảm bảo rằng 31 sản phẩm được đầu tư sẽ được định giá hàng ngày và mức lợi nhuận tối đa nhà đầu tư có thể nhận được có thể lên đến 255% số tiền đầu tư sau một năm. Bằng cách này, cá nhân A đã lừa đảo khoảng 30 nghìn nhà đầu tư và giá trị của các khoản tiền lên tới xấp xỉ 51 triệu USD.

182 Cá nhân A và cộng sự đã chuyển đổi số tiền thu được từ tội phạm dưới hình thức VC và bất động sản. Trong quá trình điều tra, những tài sản đang được cá nhân A và cộng sự nắm giữ đã bị thu giữ. Tháng 12/2018, Văn phòng Công tố viên quận Đài Trung đã truy tố cá nhân A và đồng phạm vi phạm Đạo luật Ngân hàng và Đạo luật Giám sát tiếp thị đa cấp.

HONG KONG, TRUNG QUỐC

183 Tháng 7/2017, 136,9 Bitcoin (trị giá khoảng 13,64 triệu đô la Hồng Kông) đã bị tin tặc đánh cắp trên sàn giao dịch Bitcoin đặt tại quốc gia A. Số Bitcoin bị đánh cắp này trên thực tế đã được chuyển cho ông A vào tháng 8 năm 2017. Sau đó, ông A đã bán Bitcoin và chuyển số tiền thu được vào một tài khoản ngân hàng ở Hồng Kông, Trung Quốc. Theo yêu cầu của quốc gia A, số tiền 4,6 triệu HKD và 0,73 triệu USD trong tài khoản ngân hàng đã bị giữ lại ở Hồng Kông, Trung Quốc. Cuộc điều tra đang được tiến hành.

NHẬT BẢN

184 Một nam nhân viên văn phòng đã mua VA (tài sản ảo) sử dụng tài khoản và thông tin thẻ tín dụng của người khác bất hợp pháp. Cá nhân này đã đổi tài sản ảo sang Yên Nhật thông qua một trang web trao đổi ở nước ngoài và chuyển tiền vào tài khoản ngân hàng dưới tên của một người khác. Cá nhân bị này bị bắt vì vi phạm Đạo luật trừng phạt tội phạm có tổ chức (che giấu tài sản phạm tội).

NEW ZEALAND

Mua bán ma túy bất hợp pháp qua web đen bằng bitcoin.

185 Năm 2018, một cá nhân đã bị kết án vì nhập khẩu và cung cấp một lượng lớn ma túy thuộc diện kiểm soát loại C. Cá nhân đã mua các chất này từ các trang web đen bằng Bitcoin. Sau đó, anh ta đã bán lại cho khách hàng ở New Zealand và quốc tế thông qua các quảng cáo đăng trên mạng đen; chấp nhận Bitcoin, Ethereum và tiền mặt khi thanh toán.

186 Khi kết thúc vụ việc, NZP đã tìm thấy hơn 400 nghìn đô la tiền mặt và tiền điện tử trị giá khoảng 180 nghìn đô la New Zealand trên ví tiền của người phạm tội. Tổng cộng, hơn 1,5 triệu đô la New Zealand đã bị tạm giữ theo quy trình tố tụng hình sự của New Zealand.

PHILIPIN

187 Một cá nhân đã sử dụng công ty của mình mà ban đầu đã đăng ký là chủ sở hữu duy nhất với mục đích khác để kinh doanh đa cấp Bitcoin như là một vỏ bọc để giải thích nguồn gốc các khoản thu nhập và sản trao đổi VC của công ty nhằm tạo điều kiện thanh toán và đầu tư. Theo chương trình này, các nhà đầu tư được hứa hẹn lãi suất hai chữ số sau mỗi vài tuần. Các nghi phạm sử dụng hình thức kinh doanh đa cấp và tuyển dụng các bên trung gian với vai trò là người tuyển dụng các nhà đầu tư mới, chiến lược phủ mạng lưới trên phạm vi rộng khắp cả nước. Kẻ phạm tội cuối cùng đã bị bắt giữ. Nhiều tháng trước khi bị bắt, các hệ thống trao đổi của VC đã gắn cờ các hoạt động, giao dịch và cá nhân đáng ngờ liên quan đến âm mưu này, từ đó đưa đến việc báo cáo giao dịch đáng ngờ của nhóm tội phạm và đồng bọn.

SINGAPORE

Sử dụng tiền ảo - Tiền thu được từ gian lận email xuyên quốc gia được sử dụng để mua Bitcoin.

188 Tiền thu được từ một vụ lừa đảo qua email liên quan đến các nạn nhân ở Hoa Kỳ đã được chuyển đến một tài khoản ngân hàng Singapore được sử dụng bởi một công ty Singapore cung cấp sàn giao dịch trực tuyến và cổng thanh toán cho tiền ảo. Bằng cách sử dụng các tài liệu giả mạo, kẻ phạm tội đã mở một tài khoản giao dịch trực tuyến sau đó ghi có các khoản thu từ tội phạm. Kẻ sau phạm tội sau đó đã mua Bitcoin, bất kể giá cả, thông qua sàn giao dịch trực tuyến. Do mô hình giao dịch bất thường, tài khoản giao dịch trực tuyến đã bị công ty Singapore chặn. Khi nhận được thư thu hồi từ ngân hàng, công ty Singapore đã thanh lý số Bitcoin mà kẻ phạm tội đã mua. Các khoản tiền đã bị cảnh sát thu giữ. Các cuộc điều tra đang được tiến hành.

4.4 Sử dụng các dịch vụ chuyên nghiệp (luật sư, công chứng viên, kế toán viên)

FIJI

Sử dụng người gác cổng để cáo buộc tạo điều kiện cho các giao dịch EFTPOS bất thường

189 FIU đã nhận được một báo cáo giao dịch đáng ngờ từ một ngân hàng địa phương về các giao dịch đáng kể được thực hiện trên một thiết bị đầu cuối EFTPOS trong một ngày cuối tuần. Nó được coi là đáng ngờ vì thiết bị đầu cuối EFTPOS là một cơ sở mới được cài đặt tại một công ty luật địa phương nhỏ.

190 FIU xác định rằng một công dân người Fiji, cá nhân A, cư trú tại quốc gia B đã tiếp cận cá nhân X, trưởng đại diện của một công ty luật ở địa phương để mua một máy EFTPOS để nhận tiền đầu tư thay mặt cho đơn vị của mình, Công ty A.

191 Công ty luật địa phương đã mua lại cơ sở EFTPOS mặc dù không có khả năng kinh tế rõ ràng để đặt cơ sở hạ tầng cho máy EFTPOS. Một tuần sau, hai thẻ tín dụng nước ngoài đã được sử dụng một cách gian lận để thực hiện bảy giao dịch trong vòng ba tuần với tổng trị giá khoảng 2 triệu đô la FJ thông qua thiết bị đầu cuối EFTPOS tại công ty luật địa phương. Các khoản tiền đã được chuyển vào tài khoản ủy thác của công ty luật.

192 Được xác định rằng cá nhân X được cho là có liên quan đến vụ lừa đảo cùng cá nhân A và Công ty A để lừa đảo lấy tiền bằng máy EFTPOS. Cá nhân X đã nhận được khoảng \$ 221.000,00 FJ từ các giao dịch chuyển tiền gian lận trong khi Công ty A nhận được khoảng \$ 650.000,00 FJ vào tài khoản ngân hàng địa phương. Còn lại \$ 1.129.000,00 FJ trong tài khoản ủy thác của công ty luật đã bị tạm giữ.

193 Tiền đã được rút một cách nhanh chóng từ tài khoản của Công ty A ở ngân hàng địa phương để trả cho các cá nhân và dùng để đầu tư vào các tài sản. Đã được xác định rằng đồng hồ đeo tay Rolex đắt tiền đã được mua từ tiền thu được từ tội phạm. Các cơ quan thực thi pháp luật biên giới địa phương đã có sự phối hợp và trao đổi chặt chẽ về vấn đề này

194 FIU đã ban hành một thông báo hướng dẫn cho ngân hàng địa phương nhằm hạn chế việc tất cả các tài khoản ngân hàng liên quan đến âm mưu tinh vi này bao gồm cả vấn đề về chủ sở hữu hưởng lợi của các khoản tiền để bảo đảm và giảm thiểu việc thất thoát các khoản thu từ tội phạm. FIU đã chuyển giao vụ việc này cho cảnh sát Fiji và vụ việc vẫn đang được điều tra.

Hành vi phạm tội có thể xảy ra:

- Gian lận.
- Sở hữu tài sản bị nghi ngờ là tiền của tội phạm.
- Rửa tiền.

Các dấu hiệu:

- Sử dụng luật sư làm người gác cổng để tạo điều kiện cho gian lận.
- Sử dụng các phương thức giao dịch kinh doanh không quen thuộc không tương xứng với bản chất kinh doanh.
- Mua tài sản có giá trị và các mặt hàng xa xỉ.

Hoàn thuế VAT gian lận

195 Một công ty kế toán địa phương bị cáo buộc đã nộp tờ khai thuế gian lận với cơ quan thuế địa phương. Người ta nghi ngờ rằng công ty đã thổi phồng các chi phí được báo cáo trong các yêu cầu hoàn thuế VAT của khách hàng của họ. Công ty cũng đã gửi các bản sao hóa đơn và biên lai gian lận để chứng minh cho các yêu cầu chi phí gian lận. Các khách hàng của công ty kế toán sau đó đã nhận được tiền hoàn thuế VAT từ cơ quan thuế địa phương cho biết họ không được hưởng bất kỳ khoản hoàn trả nào. Điều này cũng dẫn đến việc cơ quan thuế địa phương của Fiji mất một khoản tiền đáng kể. Các hành vi phạm tội có thể là rửa tiền, có được tài sản bằng cách lừa dối và không trung thực khi khai báo lãi/lỗ. Vụ việc hiện đang được điều tra bởi cơ quan thực thi pháp luật địa phương.

NEW ZEALAND

Kế toán kết hợp các công ty của New Zealand thay mặt cho OCGs

196 Một kế toán viên ở New Zealand đã hợp nhất một số công ty, những công ty này sau đó đã được OCG sử dụng để tạo điều kiện cho việc nhập khẩu ma túy vào quốc gia. Nhân viên kế toán này đã nộp hồ sơ thành lập công ty và đăng ký làm giám đốc và/hoặc cổ đông của các công ty. Các tài khoản ngân hàng của công ty được sử dụng để tài trợ cho việc nhập khẩu ma túy và/hoặc nhận lại số tiền thu được từ tội phạm ma túy ở phạm vi quốc tế. Có thể kế toán cũng đang làm sai lệch hồ sơ tài chính của các công ty này (tức là ‘chế biến sổ sách, chứng từ’) để che giấu hoạt động bất hợp pháp, mặc dù điều này chưa được xác định. Sử dụng luật sư để che giấu việc mua tài sản của thành viên OCG.

197 Một thành viên của OCG New Zealand đã ký thỏa thuận mua tài sản, sử dụng luật sư để sắp đặt các khoản tiền và các thỏa thuận. Công ty mẹ của thành viên OCG là một công ty luật đã nhận được một khoản thế chấp cho một tài sản hiện có và cung cấp các khoản tiền này để giải quyết việc mua tài sản của thành viên OCG thông qua một tài khoản ủy thác khác của Luật sư dưới sự bảo trợ của một “tài sản tái cấp vốn”. Thành viên OCG thực hiện thanh toán thường xuyên cho một tài khoản giao dịch mới được mở đứng tên mẹ của mình, từ đó thế chấp được thực hiện. Việc xác nhận một khoản nợ giữa thành viên đó và mẹ của anh ta tách biệt quỹ thành viên OCG khỏi các giao dịch tài sản, việc này nhằm hạn chế các cơ quan thực thi pháp luật thu giữ tiền và/hoặc tài sản.

SINGAPORE

Sử dụng Dịch vụ Chuyên nghiệp - Công ty được thành lập để nhận các khoản thanh toán hối lộ từ nước ngoài.

198 Một công ty luật cung cấp dịch vụ thư ký công ty đã hỗ trợ một doanh nhân nước ngoài thành lập công ty và các luật sư của công ty luật này là giám đốc của công ty đã đăng ký. Với vai trò là giám đốc công ty, các luật sư đã nộp đơn mở tài khoản công ty tại ngân hàng và trao toàn quyền kiểm soát tài khoản ngân hàng cho doanh nhân nước ngoài là người mà họ khai báo với các ngân hàng là chủ sở hữu hưởng lợi của công ty.

199 Doanh nhân nước ngoài sau đó đã sử dụng công ty là một kênh để nhận hối lộ thay cho các quan chức nước ngoài. Anh ta cũng tự coi mình là nhân viên của công ty để hợp pháp hóa các khoản tiền mà anh ta đã thực hiện chuyển tiền từ tài khoản ngân hàng của công ty vào tài khoản cá nhân của mình hoặc các tài khoản khác dưới sự kiểm soát của anh ta. Các khoản tiền bị cáo buộc tham nhũng được chuyển đến các tài khoản của anh ta sau đó được chuyển cho các quan chức nước ngoài.

200 Cục Điều tra chống Tham nhũng (CPIB) chủ động đề nghị các cơ quan có thẩm quyền nước ngoài tiến hành một cuộc điều tra chung về các quan chức tham nhũng đã nhận hối lộ ở Singapore. Cuộc điều tra đang diễn ra.

THÁI LAN

201 Một trường tôn giáo tư thục ở một tỉnh biên giới phía nam đã trả hoa hồng cho một công ty “nâng cấp hồ sơ” trường học này để nhận được sự hỗ trợ tài chính của chính phủ cho mỗi học sinh của trường và sau đó được sử dụng để hỗ trợ các hoạt động khủng bố trong khu vực.

4.5 Rửa tiền trên cơ sở thương mại và chuyển giá

AFGHANISTAN

Vụ việc điển hình thứ nhất

202 Sau khi xác minh với Cục Hải quan và Thuế vụ, người ta thấy rằng các tài liệu hải quan của Công ty X đã bị giả mạo. Đó là một “công ty trên giấy tờ”, không có hồ sơ nhập khẩu hay xuất khẩu với Cục Hải quan và Thuế vụ, nhưng tiền được ghi có vào tài khoản của công ty một cách có hệ thống bởi một số cá nhân. Các tài khoản của công ty sau đó đã bị ghi nợ bởi ông Y, người này đã sử dụng tiền để chuyển tiền và trao đổi. Ông Y cũng buôn lậu tiền mặt qua các sân bay nội địa đến các tỉnh khác thuộc quốc gia. Thông tin tình báo tài chính từ FIU đã dẫn đến việc cơ quan thực thi pháp luật mở một cuộc điều tra.

Vụ việc điển hình thứ 2

203 Kết quả phân tích tài chính được thực hiện tại các công ty cho thấy các công ty đã chuyển một lượng lớn tiền mặt ra nước ngoài chủ yếu cho quốc gia A và B liên quan đến hàng hóa nhập khẩu. Tuy nhiên, giá trị của hàng hóa nhập khẩu đã được Cục Hải quan xác minh chỉ chiếm một phần rất nhỏ trong tổng số tiền gửi ra nước ngoài. Các công ty cũng đã chuyển một số tiền lớn cho quốc gia C và D mà không có hàng hóa nào được thực nhập vào quốc gia đó.

204 Việc xác minh tài chính của FIU đối với các hóa đơn của các tổ chức báo cáo cũng cho thấy các công ty đã chuyển tiền qua hóa đơn từ các ngân hàng khác nhau để nhập cùng một hàng hóa.

205 Sau khi FIU chuyển giao vụ việc cho cơ quan thực thi pháp luật, Lực lượng đặc nhiệm chống tội phạm đã mở một cuộc điều tra rửa tiền.

206 Điều tra này không chỉ phát hiện việc phát hành các hóa đơn thanh toán khác nhau cho cùng một hàng hóa, mà còn cho thấy các công ty đã giả mạo hóa đơn thanh toán. Các hóa đơn được các công ty đưa ra tại tòa án đã được xác minh và một hội đồng chuyên gia được thành lập để xác định xem các hóa đơn đó có phải là hóa đơn thật hay không. Hội đồng chuyên gia xác nhận rằng các hóa đơn đã bị giả mạo.

207 Trong quá trình điều tra, các bị cáo đã đưa hối lộ cho các quan chức để xóa án và hủy bỏ vụ án, dẫn đến việc họ bị bắt giam ngay lập tức vì tội cố gắng hối lộ các quan chức.

208 Trong khi các đối tượng đang bị giam giữ, cuộc điều tra rửa tiền đã hoàn tất và vụ án rửa tiền đã bị truy tố.

209 Theo yêu cầu của cơ quan thực thi pháp luật liên quan, FIU đã biên soạn và gửi 30 tập tài liệu, khoảng 1500 trang tài liệu có giá trị cho cơ quan thực thi pháp luật.

210 Các sản phẩm giá trị gia tăng này bao gồm:

- Tài liệu hỗ trợ giao dịch chuyển tiền cùng với thông tin về các kênh giao hàng, người thụ hưởng và khu vực pháp lý mà việc chuyển tiền được thực hiện.
- Thông tin về quà tặng được cung cấp bởi các công ty này cho nhân viên của các ngân hàng để đổi lấy việc thực hiện các giao dịch.
- Giới thiệu nhân viên FIU để tham khảo ý kiến và cung cấp ý kiến chuyên gia cho cơ quan thực thi pháp luật
- Thông tin về số Mã số thuế (TIN) của các công ty bị truy tố.
- Cung cấp thông tin về mục đích chuyển tiền, nhận được từ các khu vực pháp lý mà việc chuyển tiền được thực hiện.
- Đóng băng các tài khoản ngân hàng liên quan đến vụ việc theo yêu cầu của cơ quan thực thi pháp luật.
- Cung cấp thông tin về sự khác biệt giữa số tiền được chuyển qua hóa đơn thực và số tiền được hiển thị trong hóa đơn giả mạo.
- Thông tin về nội dung của hóa đơn giả mạo, thủ tục chuyển tiền từ ngân hàng và tổng số tiền được chuyển bởi các cá nhân bị kết án cùng với hóa đơn.
- Thành lập một hội đồng kiểm tra kỹ thuật bao gồm đại diện của ba ngân hàng và được FIU chủ trì và gửi báo cáo kiểm tra kỹ thuật của hội đồng này đến cơ quan thực thi pháp luật.
- Thông tin liên quan đến đặc điểm của các cá nhân thay mặt các công ty này chuyển tiền ra nước ngoài trong giai đoạn 2013 - 2015.
- Thông tin liên quan đến người có thẩm quyền và người được ủy quyền của các công ty này nếu không có giám đốc công ty và phó giám đốc.

211 Điều đáng nói là các sản phẩm giá trị gia tăng nói trên đã được FIU gửi đến cơ quan thực thi pháp luật theo tổng số 15 yêu cầu của các cơ quan này.

212 Do kết quả của vụ truy tố này, các cá nhân bị buộc tội đã bị kết án rửa tiền và bị kết án bốn năm tù với hiệu lực ngay lập tức. Việc kết án này được đưa ra dựa trên Luật AML và dẫn đến việc tịch thu một số tiền nhất định. Vụ án được mở để kháng cáo (tại thời điểm chuẩn bị báo cáo mô hình này năm 2019).

FIJI

213 FIU Fiji đã nhận được một STR liên quan đến cá nhân M nhận được số tiền đáng kể từ Công ty D.

214 Người ta cũng xác định rằng cá nhân M cũng là giám đốc và cổ đông của Công ty D. Công ty D đã nhận được khoảng 510.138,00 đô la FJ từ Công ty E ở quốc gia B. Các khoản chuyển tiền này được cho là để thanh toán hóa đơn, mua hàng hóa và thanh toán thương mại. FIU Fiji phát hiện rằng cá nhân M cũng là giám đốc và cổ đông của Công ty E tại quốc gia B và không có hàng xuất khẩu từ Công ty D sang Công ty E để khớp với các khoản thanh toán chuyển tiền. Số tiền này sau đó được chuyển vào tài khoản ngân hàng địa phương của cá nhân M và được sử dụng để mua tài sản.

215 FIU tiếp tục xác định rằng cá nhân M đã nhận được khoảng 897.913,00 FJ từ cá nhân N ở quốc gia B. Những khoản tiền này sau đó được cá nhân M sử dụng để mua một tài sản khác.

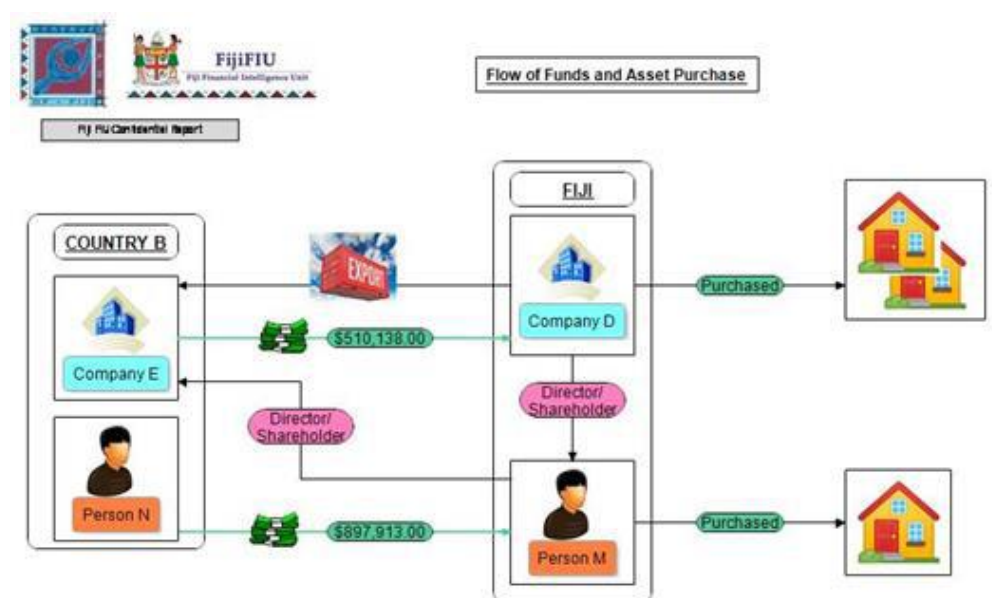
216 Một báo cáo đã được chuyển giao cho FIU của quốc gia B và cho Cơ quan Hải quan & Thuế vụ (FRCS) để tiếp tục điều tra và lập hồ sơ.

Vi phạm có thể xảy ra:

- Rửa tiền qua thương mại
- Vi phạm về thuế.

Các dấu hiệu:

- Các khoản chuyển tiền đáng kể đến.
- Chuyển tiền nhanh chóng từ doanh nghiệp sang tài khoản cá nhân.
- Nhiều tổ chức liên quan được sử dụng để chuyển tiền.
- Đầu tư bất động sản.



INDONESIA

217 JT đã gửi tiền ra nước ngoài với số lượng lớn được báo cáo trong 5.419 giao dịch chuyển tiền quốc tế (IFTI) với tổng số tiền là 3,6 nghìn tỷ IDR (250 triệu USD) cho 2.365 bên (cá nhân và công ty). JT là một trong những chủ sở hữu của một công ty thương mại nhập khẩu, đổi tiền và công ty giao nhận vận tải. Dựa trên một cuộc kiểm tra các tài khoản của JT, người ta thấy rằng đối với bất kỳ khoản chuyển tiền ra nước ngoài nào, JT luôn đính kèm các tài liệu hóa đơn liên quan đến việc mua hàng hóa nhập khẩu từ các công ty cung ứng nước ngoài. Trung Quốc, Hồng Kông - Trung Quốc và Nhật Bản là các quốc gia đã nhận được số tiền lớn nhất từ JT. Chuyển tiền sang Trung Quốc lên tới Rp1.085.182.450.627 (USD74.840.169) liên quan tới 710 bên.

218 Khi đối chiếu dữ liệu liên quan đến hàng hóa do JT nhập vào với dữ liệu Hải quan của Tổng cục Hải quan và Thuế tiêu thụ đặc biệt (DGCE), dường như có sự khác biệt giữa các hóa đơn được JT đính kèm trong các ngân hàng với dữ liệu hiện có trong DGCE. Sau quá trình xử lý dữ liệu phù hợp, có thể thấy rằng hóa đơn trong các ngân hàng chưa bao giờ được ghi lại trong dữ liệu DGCE (nghĩa là hóa đơn sai hoặc hư cấu).

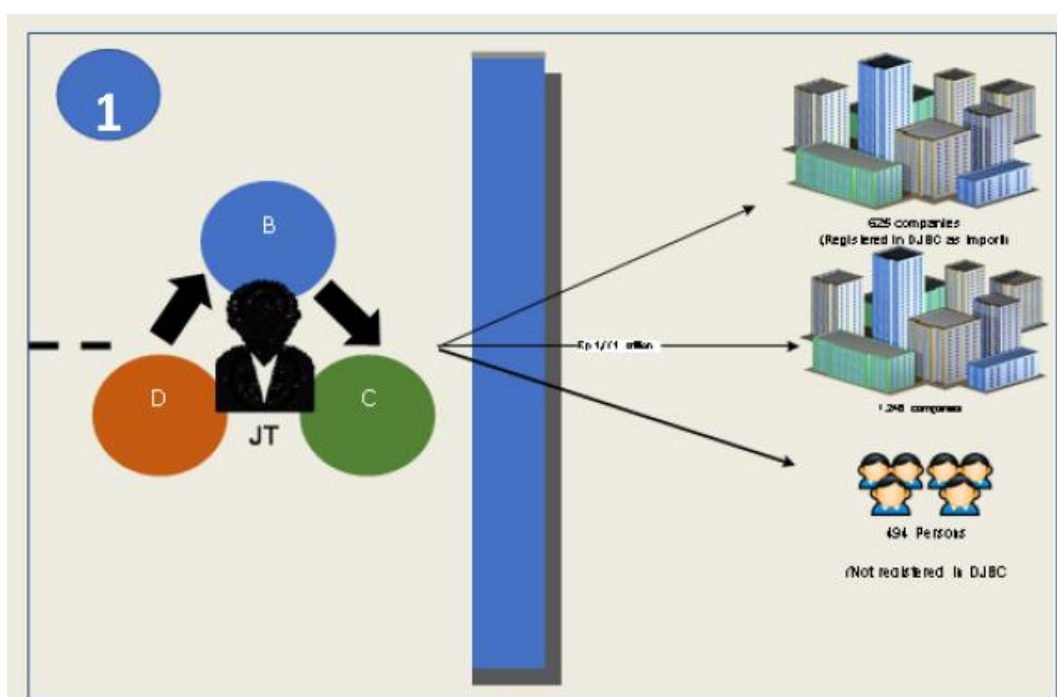
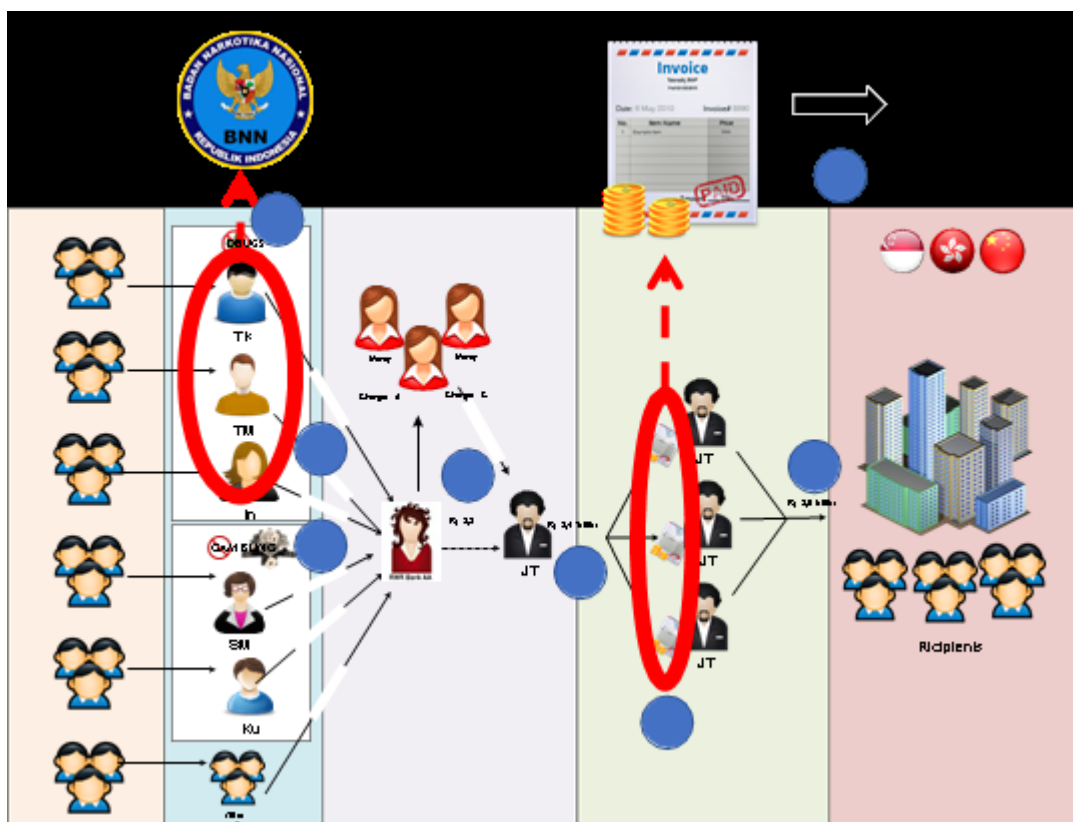
219 Có 2.365 người nhận tiền ở nước ngoài. Hầu hết trong số họ (1.246 bên) là các công ty không tham gia vào hoạt động nhập khẩu và 494 trong số họ là các cá nhân. Phần còn lại là các công ty tham gia vào hoạt động xuất nhập khẩu.

220 RWR là một trong những nguồn tiền được chuyển vào tài khoản JT ở ngân hàng A. RWR đã chuyển R7777 tỷ (53.241.379 USD) vào tài khoản JT ở ngân hàng A. Các khoản tiền này sau đó đã được gửi tới Ngân hàng B với số tiền là 30,8 tỷ Rp, Ngân hàng C với số tiền là 1,34 nghìn tỷ Rp (92,413,793 USD) và Ngân hàng D với số tiền là Rp796,17 tỷ (USD 54,908,275).

221 Dựa trên phân tích của PPATK đối với tài khoản RWR, trong Ngân hàng A giai đoạn 2014-2015, tổng các khoản chuyển tiền đến trong tài khoản lên tới 9,62 nghìn tỷ IDR (USD663.448.275) từ nhiều bên. Một số bên được xác định có liên quan đến hoạt động tội phạm liên quan đến ma túy, cụ thể là TK liên quan đến 965 giao dịch với số tiền là IDR313,2 tỷ đồng (21.600.000 USD), TM liên quan đến 328 giao dịch với số tiền là 114,53 tỷ đồng (1,002,068 USD) và số tiền AAS 9,86 tỷ IDR (680.000 USD) và 45.000 USD. Ủy ban chống ma túy quốc gia (BNN) đã được thông báo về những bên liên quan đến tội phạm ma túy.

222 Tài khoản RWR cũng được cho là đã được sử dụng để nhận tiền từ các bên liên quan đến chơi bạc trực tuyến và tiếp tục gửi tiền ra nước ngoài thông qua tài khoản JT. Các tài khoản JT được cho là đã sử dụng vì lợi ích của RWR. Điều này được củng cố bằng mô hình giao dịch trên tài khoản JT chi nhánh ở dạng chuyển giao bằng giao dịch.

223 Dưới hình thức chuyển qua giao dịch, xu hướng thực hiện giao dịch trên tài khoản cá nhân của JT và RWR, dao động từ hàng triệu đến hàng tỷ rupiah và chủ yếu được thực hiện thông qua ngân hàng trực tuyến. Dựa trên thông tin ngân hàng, mục đích mở tài khoản của JT và RWR là dành cho các giao dịch kinh doanh.

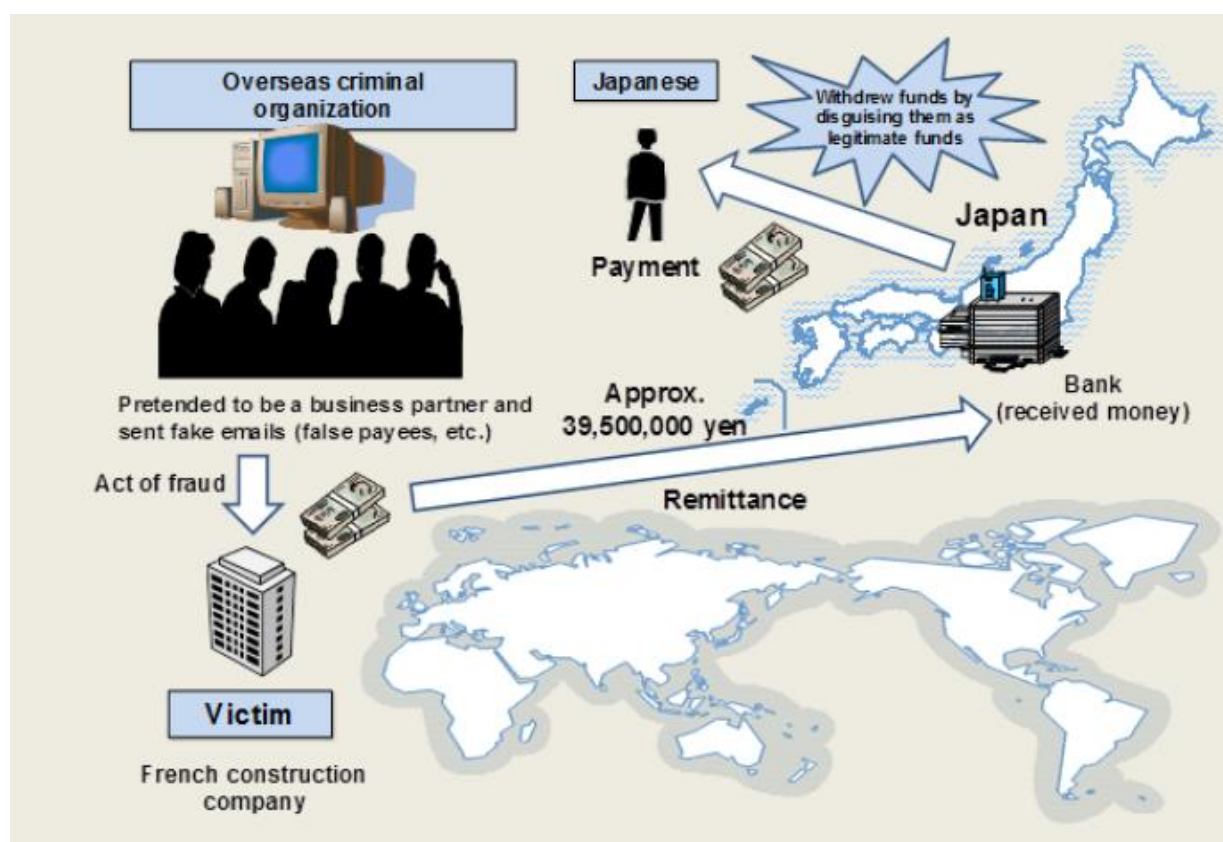


NHẬT BẢN

224 Khi bán một chiếc xe bị đánh cắp, một người đàn ông thất nghiệp đã tráo biến số xe của một chiếc xe khác cho chiếc xe bị đánh cắp và xuất khẩu sang quốc gia khác thông qua một công ty quản lý xuất khẩu mà không biết rằng chiếc xe đã bị đánh cắp. Anh ta bị bắt vì vi phạm Đạo luật trừng phạt tội phạm có tổ chức (che giấu khoản thu phạm tội).

225 Một người đàn ông Nhật Bản đã gửi email giao dịch giả mạo cho một công ty xây dựng ở Pháp và yêu cầu họ chuyển tiền vào tài khoản ngân hàng ở Nhật Bản được

mở dưới tên người khác. Khi rút tiền, anh ta đã giải thích sai cho nhân viên ngân hàng rằng những khoản tiền đó là khoản kiều hối liên quan đến các giao dịch thương mại thông thường, từ đó ngụy trang tiền thành lợi nhuận kinh doanh hợp pháp. Do đó, anh ta bị bắt vì vi phạm Đạo luật trừng phạt tội phạm có tổ chức (che giấu khoản thu phạm tội) và lừa đảo.



NEW ZEALAND

Hàng hóa thương mại được sử dụng thanh toán trong hoạt động đánh bắt cá bất hợp pháp.

226 Một công ty đánh cá của New Zealand bị buộc tội gian lận tình vi và quy mô lớn liên quan đến việc báo cáo dưới mức đánh bắt. Điều này liên quan đến hai loại vi phạm - đưa ra thông tin sai về lợi nhuận đánh bắt và bán cá khi chưa khai báo cho các Bộ chủ quản. Một số sản phẩm khai thác bất hợp pháp sau đó đã được xuất khẩu cho một công ty Úc, nơi cung cấp cho nhà xuất khẩu New Zealand một chiếc thuyền mới để thanh toán cho việc đánh bắt bất hợp pháp. Phương pháp này cho thấy việc trao đổi giá trị (một chiếc thuyền mới là thanh toán cho lượng cá đánh bắt bất hợp pháp) thông qua dòng thương mại quốc tế thay vì trao đổi tiền mặt.

PAKISTAN

227 FMU đã nhận được một STR về một nghi phạm liên quan đến rửa tiền thông qua thương mại. Nghi phạm A, đang tiến hành kinh doanh tại thành phố Karachi và đã mở một tài khoản ngân hàng. Một thời gian sau khi mở tài khoản, nghi phạm đã nộp EIF (mẫu nhập khẩu điện tử) để chứng nhận từ ngân hàng. Khi tìm hiểu, ngân hàng xác định rằng nhà nhập khẩu có liên quan đến rửa tiền thông qua thương mại. Nghi phạm đã nhập khẩu vải màu xám từ quốc gia khác thông qua các công ty có trụ sở tại quốc gia đó

và khai báo gian dối rằng vải xám được nhập từ Trung Quốc. Cục Tình báo Hải quan cũng thu giữ vải và tổng cộng 106 container liên quan đến buôn lậu.

228 Nghi phạm hiện có một tài khoản ngân hàng ở Karachi và Cục Tình báo Hải quan đang điều tra sự việc. Thông tin tình báo tài chính này sau đó đã được chuyển cho cơ quan thực thi pháp luật để điều tra thêm và có hành động cần thiết theo các quy định của Đạo luật AML, 2010.

PHILIPIN

229 Cơ quan đặc nhiệm chống ma túy Philipin đã bắt giữ ZTC, một công ty có quốc tịch tại quốc gia C, trong một hoạt động mua bán. ZTC đã bị bắt quả tang bán methamphetamine hydrochloride, địa phương gọi là shabu, cho một cơ quan của chính phủ. Ngoài ma túy, nhiều tài liệu tài chính mà anh ta sở hữu cũng bị thu giữ, đặc biệt là các khoản tiền gửi của các khoản tiền bị nghi ngờ thu được từ mua bán ma túy vào tài khoản ngân hàng của một số người/tổ chức là QH, XQ, WL, CG, WH, RDS, MAD, BJC, JE và các doanh nghiệp YSMW.

230 Các hoạt động mua bán ma túy của ZTC có từ trước năm 2009 khi anh ta bị bắt bởi các cơ quan chính phủ, cũng vì bán số lượng lớn ma túy bất hợp pháp.

Một số yêu cầu điều tra tài chính

231 FIU Philippines đã nhận được yêu cầu từ một số cơ quan chính phủ để tiến hành một cuộc điều tra tài chính đối với các doanh nghiệp QH, WH và YSMW liên quan đến các hoạt động mua bán ma túy bất hợp pháp. Theo đó, một số hồ sơ tài chính liên quan đến các doanh nghiệp QH, WH và YSMW đã bị các cơ quan của chính phủ thu giữ do các nhân vật liên quan đến ma túy bị bắt giữ ở miền Trung Philipin. Hơn nữa, điện thoại di động thu giữ từ các tù nhân trong các cơ sở nhà tù khác nhau có chứa tin nhắn văn bản ám chỉ cụ thể đến các tài khoản ngân hàng của doanh nghiệp YSMW và QH được sử dụng để tạo điều kiện thuận lợi cho các hoạt động mua bán ma túy bất hợp pháp.

232 FIU đã tiến hành điều tra các ngân hàng về các tài khoản của các đối tượng này. Việc hợp tác cũng được thực hiện với: (1) các cơ quan đăng ký tài sản khác nhau của chính phủ để xác minh quyền sở hữu tài sản và nắm giữ kinh doanh của các đối tượng; và (2) các cơ quan thực thi pháp luật để xác định hồ sơ nghi phạm và hỗ trợ trong việc thực hiện các hoạt động giám sát.

Kết quả điều tra tài chính

233 Không có giao dịch tài chính nào được xác định của ZTC ngoại trừ việc các khoản tiền gửi cho người khác được tìm thấy mà anh ta sở hữu.

234 Tin nhắn văn bản được trích xuất từ điện thoại di động của các tù nhân đã cho thấy tài khoản ngân hàng của các doanh nghiệp YSMW đã được sử dụng để tạo điều kiện thuận lợi cho các khoản tiền thu được từ buôn bán ma túy. Công ty đã được đăng ký để tham gia bán buôn/bán lẻ túi xách. Các giao dịch tài chính trong tài khoản ngân hàng đã ghi nhận nhiều khoản tiền lớn, bất thường so với hoạt động thông thường của một doanh nghiệp. Hơn nữa, người ta thấy rằng các tài khoản ngân hàng của công ty không bị kiểm soát hoàn toàn bởi chủ sở hữu đã được đăng ký là LTE, mà bị kiểm soát bởi DS và TS, cả hai đều là công dân của quốc gia C.

235 Mặt khác, QH, XQ và WH có quan hệ họ hàng và tất cả đều có quốc tịch tại quốc gia C. Họ khai báo nguồn thu nhập từ, (a) một cửa hàng máy tính mà sau đó được

xác định là không tồn tại và (b) Tập đoàn HK, một công ty có hoạt động kinh doanh được cho là tham gia vào việc bán mực máy tính và phụ kiện. Các cuộc điều tra tài chính trên tài khoản của họ cho thấy hàng tỷ peso đã đổ vào tài khoản của họ, điều này là bất thường so với những thông tin được cung cấp về hoạt động kinh doanh của họ.

236 CG, có quốc tịch tại quốc gia C, sở hữu một số doanh nghiệp mà gần đây các doanh nghiệp này đã ngừng hoạt động. Trong các tài liệu nhận biết khách hàng, cá nhân này khai báo tiền lương là nguồn thu nhập chính của mình. Năm 2018, cá nhân này thành lập doanh nghiệp du lịch và bất động sản. Có thể thấy rằng, từ hồ sơ giao dịch của các doanh nghiệp, hàng tỷ peso đã đổ vào tài khoản ngân hàng của công ty ngay cả ở giai đoạn mới khởi nghiệp. Mặt khác, WL, tương tự là công dân của quốc gia C, tuyên bố rằng cô ta là người quản lý tài chính của Công ty GPT, được biết là có liên quan đến cờ bạc trực tuyến. Điều tra tài chính cho thấy hàng trăm triệu peso đã đổ vào tài khoản của cá nhân này. Cá nhân này cũng thực hiện một số lần chuyển tiền vào tài khoản ngân hàng của WFG, vợ của CG.

237 Người ta xác định rằng các khoản chuyển tiền ra bên ngoài từ tài khoản của các đối tượng là nhiều người có lợi ích có thể liên quan đến các hoạt động mua bán ma túy bất hợp pháp. Quyền sở hữu của các giao dịch không được thiết lập và không được chứng minh là được thực hiện trong quá trình kinh doanh thông thường.

238 Việc thu hồi các khoản tiền gửi trong việc sở hữu ZTC cho thấy mối liên kết của QH, XQ, WL, CG, WH, YSMW Enterprises, RDS, MAD, BJC và JE trong các hoạt động mua bán ma túy bất hợp pháp. Mỗi quan hệ được thiết lập giữa các cá nhân do có sự trao đổi của các cá nhân thông qua các khoản chuyển tiền qua các ngân hàng và sử dụng các doanh nghiệp cung cấp dịch vụ về tiền tệ. Ngoài ra, các giao dịch tài chính của các cá nhân được phát hiện có liên quan đến các cá nhân và tổ chức khác là những đối tượng được tra hỏi trong nhiều vụ kiện tịch thu dân sự khác nhau do FIU đệ trình, liên quan đến vi phạm luật chống ma túy của Philipin, dựa trên các giao dịch chuyển khoản mà các cá nhân thực hiện thông qua hệ thống ngân hàng.

239 Việc không chứng minh số tiền được giao dịch qua tài khoản của các cá nhân có được từ các nguồn thu nhập hợp pháp có thể dẫn đến kết luận rằng hàng trăm triệu peso của các cá nhân này là từ các nguồn thu nhập khác. Các giao dịch vào tài khoản của các cá nhân không phải là giao dịch thông thường của các loại hình doanh nghiệp. Hoạt động không nhất quán của các tài khoản và bản chất của các nguồn thu nhập của các cá nhân cho thấy không có bất kỳ chứng minh hợp lý nào về các giao dịch tài chính nói trên.

240 Tổng cộng sáu trăm năm mươi (650) tài khoản ngân hàng được duy trì trong mười ba (13) tổ chức tài chính, bao gồm Php773,003,483.06 và USD142.407,25 đã bị đóng băng và hiện đang bị tịch thu dân sự.

SINGAPORE

Cung cấp các mặt hàng xa xỉ được chỉ định – Công ty và Giám đốc của công ty đã bị truy tố vì cung cấp các mặt hàng xa xỉ được chỉ định cho Cộng hòa Dân chủ nhân dân Triều Tiên (DPRK), gian lận và rửa tiền

241 Cá nhân N là một trong những giám đốc của Công ty T. Từ năm 2010 đến 2017, Công ty T đã cung cấp hàng hóa xa xỉ được chỉ định trị giá hơn 6 triệu đô la Singapore,

bao gồm rượu vang, nước hoa và mỹ phẩm, cho một cửa hàng bách hóa ở DPRK trong 80 lần.

242 Khi cửa hàng bách hóa ở DPRK trì hoãn thanh toán cho hàng hóa đã đặt hàng và gây ra vấn đề về dòng tiền trong Công ty T, cá nhân N đã nghĩ ra một kế hoạch lừa đảo và sử dụng Công ty T để gửi hóa đơn thương mại giả cho năm ngân hàng để lừa đảo tài trợ 81 lần, tổng số tiền là hơn 95 triệu đô la Mỹ.

243 Vào tháng 7 năm 2018, cá nhân N và Công ty T đã bị buộc tội cung cấp các mặt hàng xa xỉ được chỉ định cho DPRK theo Quy định của UN-DPRK. Cá nhân N cũng bị buộc tội gian lận liên quan đến gian lận hóa đơn tài chính. Công ty T cũng bị buộc tội rửa tiền từ vụ gian lận hóa đơn tài chính.

244 Việc khởi tố cá nhân N và Công ty T đang diễn ra.

4.6 Hệ thống chuyển tiền ngầm/Các dịch vụ chuyển tiền khác/Hawala

TRUNG QUỐC

Vụ việc điển hình thứ nhất

245 Vào tháng 7 và tháng 11 năm 2014, Cơ quan giám sát đã cung cấp STR cho cảnh sát. Cảnh sát đã nộp hồ sơ vào tháng 5 năm 2015 và điều tra Nghi phạm Y và các đồng bọn của anh ta.

246 Trường hợp này liên quan đến ba tổ chức chuyển tiền ngầm: quẹt thẻ bằng máy POS, buôn bán ngoại tệ bất hợp pháp và rút tiền mặt qua biên giới bằng ATM. Họ thành lập một chuỗi chuyển tiền ngầm tích hợp. Cho đến tháng 6 năm 2018, tất cả 41 nghi phạm liên quan đến vụ án này đã bị kết án vì hoạt động bất hợp pháp.

Vụ việc điển hình thứ hai

247 Vào tháng 9 năm 2018, Cơ quan giám sát, cùng với cảnh sát địa phương, đã phát hiện ra một vụ án chuyển tiền ngầm. Nghi phạm C và đồng bọn đã buôn bán ngoại tệ trái phép ở hai thành phố. Họ đã sử dụng tài khoản của một nghi phạm ở Thành phố J, ngoại tệ được thu thập từ các tài khoản ở nước ngoài và tiền được thu thập từ các tài khoản trong nước. Tổng số tiền trong trường hợp này đã đạt hơn một tỷ nhân dân tệ.

ĐÀI BẮC TRUNG QUỐC

248 Vào tháng 5 năm 2017, một kế hoạch Ponzi do Tập đoàn Y phát triển đã được ông B đưa vào Đài Bắc Trung Quốc với sự hỗ trợ của một công dân Malaysia. Ông B và đồng phạm đã tổ chức một số hội thảo nhỏ để tuyên bố rằng Tập đoàn Y đã phát minh ra phần mềm có thể được sử dụng để kiếm lợi nhuận từ xổ số thể thao. Tùy thuộc vào số tiền đầu tư, lãi suất hàng năm mà các nhà đầu tư có thể đạt được là từ 84% đến 180%. Để đánh lừa nhiều nhà đầu tư hơn và nhận được nhiều tiền hơn, ông B và đồng phạm đã phát triển các chương trình phản hồi để cung cấp một lượng lớn các ưu đãi hoặc các giải thưởng khác khiến các nhà đầu tư sẵn sàng giới thiệu các nhà đầu tư mới tham gia hoặc đầu tư. Tính đến tháng 9 năm 2018, ông B và đồng phạm đã lừa đảo khoảng 3.000 nhà đầu tư và số tiền lấy được của các nạn nhân là khoảng 198 triệu USD.

249 Để trốn tránh cuộc điều tra, ông B và đồng phạm đã giấu tiền nhận được từ các nhà đầu tư tại nơi cư trú của ông B và đồng phạm, số tiền lên tới khoảng 200 triệu Đài tệ. Có khoảng 232 triệu Đài tệ đã được chuyển ra nước ngoài thông qua các đại lý

chuyển tiền ngầm. Một số tiền đã được sử dụng cho các khoản đầu tư khác dưới tên của họ hoặc chuyển đổi thành ngoại tệ hoặc VA. Trong quá trình điều tra, các tài sản liên quan đến vụ án như tiền mặt, tiền ảo, ô tô, bất động sản và tài khoản ngân hàng đã bị thu giữ. Vào tháng 11 năm 2018, Văn phòng Công tố đã truy tố ông B và các đồng phạm vì vi phạm Luật ngân hàng, Luật kiểm soát rửa tiền và Luật giám sát tiếp thị đa cấp.

250 Khi điều tra một vụ bắt cóc không liên quan, CIB đã tìm thấy công ty H, điều hành giao dịch điện tử do Wu đứng đầu, thực sự điều hành một đường dây chuyển tiền ngầm, bao gồm một trao đổi ngoại tệ bất hợp pháp, bao gồm CNY, USD và NTD tại các vùng lãnh thổ và khu vực pháp lý bao gồm Đài Bắc Trung Quốc, Hồng Kông, Trung Quốc và các khu vực pháp lý Đông Nam Á. Các nghi phạm đã phạm tội rửa tiền thông qua việc mở tài khoản OBU và lạm dụng các công ty ma không liên quan. Số tiền chuyển lên tới 20 tỷ Đài tệ và số tiền lãi bất chính lên tới 180 triệu NTD. CIB đã thành công đưa ra một kiến nghị lên tòa án vào ngày 25 tháng 9 năm 2018, theo Luật kiểm soát rửa tiền (bao gồm tịch thu) và Bộ luật tố tụng hình sự. Một khoản tương đương 430 triệu NTD trong tài khoản ngân hàng liên quan đã bị thu giữ. Dưới sự hợp tác giữa Đài Bắc Trung Quốc và Trung Quốc, năm nghi phạm đã bị bắt tại Trung Quốc và bảy nghi phạm đã bị bắt tại Đài Bắc Trung Quốc

INDONESIA

Vụ việc điển hình thứ nhất

251 Vào tháng 7 năm 2014, HF tuyên bố trung thành với ISIS. Sau đó, ông ta liên lạc qua điện tín cho BS (một Chỉ huy ISIS ở Đông Nam Á đến từ Indonesia). HF nhận được một lệnh từ BS để hỗ trợ các nhu cầu của Tập đoàn MIT (Nhóm khủng bố của Indonesia kết hợp với ISIS) và tiến hành một cuộc tấn công. Dựa trên kết quả tìm kiếm dữ liệu IFTI, PPATK nhận thấy rằng có một dòng tiền vào tháng 7 năm 2015 từ Trung Đông lên tới 3.789,77 USD.

252 Ngoài ra, HF được biết là đã kiểm soát các tài khoản cá nhân khác, vốn được sử dụng để nhận tiền từ các nhóm khủng bố trong nước. Theo các nhà chức trách, số tiền này đã được gửi cho một số bên ở Philippines vào tháng 7 năm 2015, đặc biệt, 10.500 USD đã được gửi qua MSP để mua vũ khí cho các tổ chức khủng bố sử dụng. Vào tháng 1 năm 2016, cảnh sát đã bắt giữ HF vì liên quan đến vụ nổ súng và ném bom ở Thamrin, Boulevard Jakarta. HF đã bị giam cầm sáu năm vì tội khủng bố và tài trợ khủng bố.

Vụ việc điển hình thứ hai

253 Vào ngày 5 tháng 5 năm 2015, AS đã gặp AJ, cả hai đều có liên kết với ISIS, khi đang thăm AA trong tù. Tại cuộc gặp mặt, AJ đã đề nghị khẩn trương giúp đỡ một số phần tử ở Indonesia đến Syria để gia nhập ISIS. Nguồn tiền được chuyển vào tài khoản ngân hàng dưới tên AJ hầu hết có nguồn gốc từ các phần tử trong nước và có số tiền lên tới 300 triệu IDR (~ 21.428 USD). Các khoản tiền đã được sử dụng để mua vé đến Syria. Trong giai đoạn tháng 4 năm 2016, AJ đã hướng dẫn US gửi tiền cho SM bằng cách sử dụng số tiền peso tương đương của Philippines lên tới 200 triệu IDR (~ 14.285 USD) thông qua chuyển khoản MSB cho mục đích mua vũ khí để sử dụng trong huấn luyện quân sự tại Indonesia.

NHẬT BẢN

254 Nghi phạm người Việt Nam có khách hàng muốn gửi tiền từ Nhật Bản đến Việt Nam. Họ đã có khách hàng gửi tiền vào tài khoản ngân hàng của họ tại Nhật Bản, được mở dưới tên người khác. Họ đã mua hàng hóa và thực phẩm tiện lợi bằng tiền và xuất khẩu sang Việt Nam dưới vỏ bọc của một giao dịch hợp pháp. Các hàng hóa xuất khẩu sau đó được bán tại Việt Nam và do đó chuyển đổi thành tiền mặt. Phương thức này có hiệu quả tương đương với giao dịch chuyển tiền quốc tế. Các nghi phạm đã bị bắt vì vi phạm Luật trừng phạt tội phạm có tổ chức (tội che giấu quá trình phạm tội) và Luật Ngân hàng (chuyển tiền ngầm).

255 Một trường hợp tiền được chuyển bởi khách hàng vào tài khoản được mở bằng tên của người khác đã được sử dụng để mua máy móc và thiết bị nông nghiệp nặng, với máy móc và thiết bị đã mua được xuất khẩu sang nước ngoài trong một giao dịch được ngụy trang thành một giao dịch hợp pháp và chuyển đổi thành tiền mặt. Phương thức này có hiệu quả tương đương với một giao dịch chuyển tiền quốc tế.

PAKISTAN

256 Một người khiếu nại báo cáo rằng ông ta đã nhận được các cuộc gọi từ các số điện thoại Afghanistan và một số điện thoại địa phương yêu cầu một khoản tiền 1 triệu Rupee làm tiền chuộc. Những kẻ gọi điện tiết lộ chúng là thành viên của Phong trào Taliban Pakistan (TTP) và cảnh báo rằng nếu không nộp tiền chuộc, ngôi nhà của ông ta sẽ bị đánh bom. Người khiếu nại và cháu trai của ông ta đã đến một nơi ở Peshawar và trao khoản tiền chuộc cho một cá nhân lạ mặt.

257 Cuộc điều tra cho thấy tiền được chuyển qua Hawala tới Afghanistan. Một nhóm điều tra chung (JIT) đã được thành lập. Báo cáo phổ biến tiền mặt (CDR) phân tích cho thấy các liên hệ giữa hai bên và điều tra thêm cho thấy cả hai bị cáo đều có liên kết với JuA. Khi bị bắt, cả hai thú nhận có liên quan đến việc chuyển khoản tiền chuộc. Cuộc điều tra cho thấy những cá nhân khác có liên quan vẫn còn nhiều và một số kẻ tội phạm đã được tuyên bố. Các cuộc điều tra tiếp theo đang được tiến hành

4.7 Sử dụng internet (mã hóa, truy cập qua ID, chuyển tiền quốc tế, etc.)

FIJI

Thỏa thuận thương mại điện tử dẫn đến việc thua lỗ đáng kể

258 FIU đã nhận được một STR từ Ngân hàng D cho rằng Công ty C là nạn nhân của một thỏa thuận thương mại điện tử. FIU phát hiện ra rằng các thư điện tử kinh doanh của Công ty C với nhà cung cấp nước ngoài của họ đã bị xâm nhập bởi một tin tặc trong khu vực pháp lý F. Tin tặc đã chặn các email qua lại và hướng dẫn Công ty C chuyển khoảng 266.000,00 đô la Mỹ sang số tài khoản ngân hàng nước ngoài. Tin tặc đã gửi email cho Công ty C với một địa chỉ email tương tự như nhà cung cấp nước ngoài của Công ty C.

259 FIU cung cấp một báo cáo phổ biến trường hợp cho FIU nước ngoài tương ứng để điều tra. Theo đó, số tiền đó đã bị tiêu biến cho các thực thể khác nhau trong cùng một ngày. Tuy nhiên, đích đến cuối cùng của khoản tiền đó không thể xác định được.

Hành vi phạm tội có thể xảy ra:

- Có được lợi thế tài chính thông qua sự lừa dối.
- Không trung thực.

Các dấu hiệu:

- Email được xây dựng kém nhằm thuyết phục người nhận bỏ qua lỗi.
- Thay đổi chi tiết thanh toán và chi tiết người thụ hưởng vào phút cuối

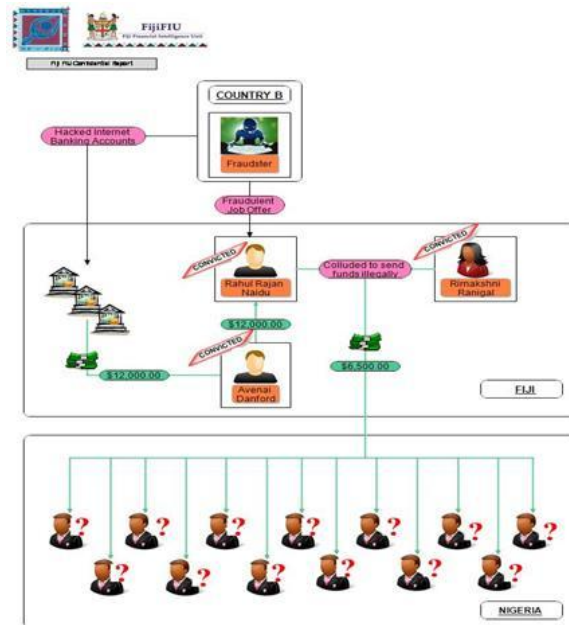
Thông đồng để tạo điều kiện thu lợi bất chính thông qua chuyển khoản internet banking trái phép

260 Ông Rahul Rajan Naidu đã nhận được lời mời làm việc từ một “Jasmin Olich of Global Link Money Services”, để thực hiện đánh giá bí mật về các dịch vụ của Western Union bằng cách gửi và nhận tiền qua Western Union. Ông Rahul Rajan Naidu được thông báo rằng tiền sẽ chỉ được chuyển vào tài khoản ngân hàng Westpac mà sau đó ông sẽ rút ra, khấu trừ tiền hoa hồng của mình và chuyển phần còn lại cho các cá nhân khác nhau ở các vùng của Nigeria.

261 Vì ông Rahul Rajan Naidu không có tài khoản tại Westpac, ông đã tiếp cận bạn mình, ông Shoeb Nur Ali, một người phát lương (pay master) tại Fiji Meats Limited để hỗ trợ ông tìm một người có tài khoản tại ngân hàng Westpac nhưng không sử dụng đến tài khoản đó. Ông Shoeb Nur Ali đã hỏi bạn của mình, ông Avenai Danford, nếu ông sẵn sàng cho phép ông Rahul Rajan Naidu sử dụng tài khoản của mình để nhận tiền. Ông Avenai Danford đã đồng ý và nhận 12.000,00 đô la vào tài khoản ngân hàng Westpac của mình từ những chuyển khoản internet banking trái phép từ ba nạn nhân. Ông Avenai Danford đã rút và đưa những khoản tiền này cho ông Rahul Rajan Naidu.

262 Sau đó, ông Rahul Rajan Naidu đã yêu cầu ông Shoeb Nur Ali cung cấp các bản sao ID của ông Shoeb Nur Ali và của ba đồng nghiệp của ông Shoeb Nur Ali. Bà Rimakshni Ranigal, Cán bộ giao dịch khách hàng tại một đại lý thu đổi ngoại tệ, đã sử dụng những giấy tờ này cùng với các bản copy của một số ID khác mà ông Rahul Rajan Naidu có được để chuyển tiền 12 lần tới Nigeria.

263 Không ai trong số 12 cá nhân trên, những người được ghi nhận là người gửi các khoản tiền này, có mặt khi tiền được gửi đi và họ cũng không biết rằng tiền được gửi đi bằng tên và ID của họ. Vào ngày 4 tháng 9 năm 2018, ông Rahul Rajan Naidu bị cáo buộc bốn tội danh rửa tiền, ông Avenai Danford và bà Rimakshni Ranigal mỗi người bị cáo buộc một tội danh rửa tiền. Vào ngày 18 tháng 9 năm 2018, ông Rahul Rajan Naidu, ông Avenai Danford và bà Rimakshni Ranigal đã bị kết án lần lượt là sáu năm chín tháng, ba năm và năm năm.



4.8 Sử dụng hệ thống hoặc phương pháp thanh toán mới

ÚC

264 Vào tháng 6 năm 2018, Bộ trưởng Bộ Nội vụ, xác nhận rằng AUSTRAC và Ngân hàng Liên bang Úc (CBA) đã đạt được thỏa thuận, trong đó CBA đã thừa nhận 53.750 hành vi vi phạm Đạo luật chống rửa tiền và chống khủng bố của Úc năm 2006 (Đạo luật AML/CTF). CBA đồng ý nộp phạt tài chính 700 triệu AUD, mức phạt dân sự lớn nhất từng được đưa ra tại Úc.

265 CBA thừa nhận đã có những sai phạm liên quan đến Máy gửi thông minh (IDMs), cụ thể hơn là sai phạm trong việc quản lý rủi ro đối với các máy IDM của mình và sai phạm khi không cung cấp kịp thời các báo cáo giao dịch lớn và giao dịch đáng ngờ. CBA cũng thừa nhận các sai phạm liên quan việc quản lý thông tin khách hàng và tài khoản khách hàng.

266 Sai phạm trong việc tuân thủ của CBA đã dẫn đến việc một số tội phạm nguy hiểm và có tổ chức đã khai thác lĩnh vực tài chính để rửa tiền thu được từ các hoạt động tội phạm của chúng, bao gồm cả tiền mua bán ma túy bất hợp pháp trong cộng đồng.

267 Trường hợp này cung cấp một ví dụ về bản chất thực sự của hoạt động tội phạm có tổ chức và cách thức mà tội phạm có thể khai thác lĩnh vực tài chính khi các đối tượng báo cáo không tuân thủ nghĩa vụ phòng chống rửa tiền/tài trợ khủng bố của họ.

268 Hình phạt là hình phạt dân sự lớn nhất trong lịch sử doanh nghiệp Úc. Vào tháng 6 năm 2018, AUSTRAC đã ban hành một số thông cáo truyền thông về vấn đề này: <http://www.austrac.gov.au/media/mediarelease>.

269 Kết quả của vụ việc này đã gửi một điệp mạnh mẽ đến ngành công nghiệp rằng việc không tuân thủ nghiêm trọng Đạo luật phòng chống rửa tiền và Đạo luật phòng chống khủng bố của Úc năm 2006 (Đạo luật AML/CTF) là không thể chấp nhận được, do kết quả của thủ tục tố tụng dân sự đã chỉ ra một ví dụ thực tế về hậu quả của việc tuân thủ kém.

270 Vụ việc cũng nhắc nhở về trách nhiệm của các tổ chức tài chính, hội đồng quản trị và quản lý cấp cao của họ trong việc phải đảm bảo tổ chức của mình thực hiện

nghiêm túc các nghĩa vụ phòng chống rửa tiền/tài trợ khủng bố và họ phải xây dựng một văn hóa doanh nghiệp để hỗ trợ việc này.

TRUNG QUỐC

Vụ việc điển hình thứ nhất

271 Vào tháng 6 năm 2017, Nghi phạm D đã cung cấp mã xác thực Alipay QR của mình cho bạn gái của anh ta (người đã bị kết án) để nhận tiền bán ma túy và chuyển tiền vào ID trò chơi của bạn gái anh ta. Nghi phạm D đã sử dụng tài khoản của mình để che giấu nguồn gốc và bản chất của khoản tiền phạm tội, và đã dính líu đến tội rửa tiền. Vào tháng 4 năm 2018, tòa án đã kết án Nghi phạm D hai tháng tù giam cùng với một hình phạt.

Vụ việc điển hình thứ hai

272 Năm 2017, Nghi phạm E có liên quan đến buôn bán ma túy và đã nhận được khoản thanh toán cho việc bán ma túy bằng cách sử dụng WeChat hoặc tiền mặt. Nghi phạm E đã chuyển tiền cho vợ cũ (Nghi phạm F) thông qua các phương tiện tương tự. Tòa án xác định rằng Nghi phạm F đã cung cấp tài khoản WeChat của mình cho Nghi phạm E nhằm che giấu nguồn gốc và bản chất của khoản tiền phạm tội và hỗ trợ chuyển số tiền thu được. Hai đối tượng này đã bị kết án về tội rửa tiền. Vào tháng 3 năm 2018, tòa án đã kết án Nghi phạm F bảy tháng tù giam cùng với một hình phạt.

FIJI

Thao túng quy trình và hệ thống nội bộ

273 Bà Vika Sadrau đã làm việc Bưu điện Fiji Limited với tư cách là Nhân viên dịch vụ Khách hàng chịu trách nhiệm xử lý Đơn hàng Tiền điện tử (Electronic Money Orders - EMO).

274 Từ tháng 3 đến tháng 5 năm 2015, bà Vika Sadrau đã lấy 55.779,32 đô la tiền bất chính bằng cách thao túng hệ thống EMO. Bà Vika Sadrau đã xử lý một giao dịch EMO cho một khách hàng và sử dụng cùng một mật khẩu ID EMO để tạo nhiều khoản thanh toán phức tạp cho cùng một giao dịch.

275 Sau đó, Vika Sadrau đã thay đổi số tiền thanh toán và chi tiết về người thụ hưởng và lấy lệnh thông qua từ người giám sát mình để thực hiện thanh toán cho bản thân. Bà Vika Sadrau đã xử lý các khoản thanh toán cho mình với tổng trị giá 55.779,32 đô la. Sau đó, bà ta đã gửi \$ 21,000.00 vào tài khoản ngân hàng của mình.

276 Bà Vika Sadrau đã thừa nhận tội trộm cắp và tội rửa tiền. Vào ngày 22 tháng 8 năm 2018, bà Vika Sadrau đã bị kết án 18 tháng vì tội trộm cắp và bốn năm tù vì tội rửa tiền. Trường hợp này minh họa cho việc vi phạm các thủ tục kiểm soát nội bộ.

HONG KONG, TRUNG QUỐC

277 Một tài khoản Stored Value Facilities (SVF) đã được tìm thấy đã ghi lại các lần nạp tiền hoặc chuyển khoản thường xuyên từ các tài khoản khác trong khoảng thời gian từ tháng 12 năm 2017 đến tháng 6 năm 2018. Các khoản tiền gửi vào không được sử dụng để thực hiện bất kỳ giao dịch mua bán nào, thay vào đó chúng chủ yếu được rút từ các tài khoản ngân hàng cá nhân liên kết và một lượng nhỏ tiền sau đó đã được gửi trả lại cho người gửi ban đầu. Việc giám sát các giao dịch cho thấy có một số điều khoản của các tin nhắn chuyển khoản có liên quan đến cá cược bóng đá và tên của các đội

tuyển nước tham gia một giải đấu bóng đá quốc tế. Nghi ngờ rằng tài khoản SVF này có thể được sử dụng để đánh bạc bất hợp pháp, nhà cung cấp dịch vụ SVF đã báo cáo cho JFIU.

278 Theo phân tích của JFIU, một số chủ tài khoản đã báo cáo các địa chỉ trong cùng một khu dân cư và số điện thoại di động của một chủ tài khoản được liên kết trực tiếp với một trang web cá cược bóng đá bất hợp pháp. Các tài khoản SVF đã được sử dụng để nhận tiền cược, bằng cách nạp tiền mặt và chuyển khoản, liên quan đến một đường dây cá cược bóng đá trực tuyến bất hợp pháp được điều hành bởi một tổ chức. Các khoản tiền cá độ được hợp nhất thông qua các tài khoản SVF và sau đó được chuyển sang tài khoản ngân hàng cá nhân do các thành viên của tổ chức hoặc các tài khoản nguồn của SVF, tùy thuộc vào kết quả của các trận đấu. Thông tin này được báo cáo đến một cơ quan thực thi pháp luật địa phương để theo dõi các động thái tiếp theo.

INDONESIA

279 Sau một cuộc tấn công vào Surakarta (một thành phố khu vực ở trung tâm Java), một số tiền chuyển khoản được sử dụng để tài trợ cho cuộc tấn công được xác định là từ tài khoản ngân hàng của các cá nhân đã từng liên lạc với ông Y, một Chỉ huy ISIL của Đông Nam Á đang cư trú ở Syria. FIU và Cơ quan thực thi pháp luật xác định ông Y (Syria) đã chuyển khoảng 1.000 USD vào tài khoản PayPal của ông H (Indonesia). Ông H đã rút hết số dư ở PayPal rồi chuyển khoản vào tài khoản ngân hàng của mình và sau đó chuyển nó cho ông M (Indonesia). Ông M sau đó đã chuyển số tiền này vào nhiều tài khoản ngân hàng khác nhau, những khoản tiền này tiếp tục được chuyển thành tiền mặt và giao cho những kẻ khủng bố. Ông M, người có liên quan đến việc tài trợ cho vụ tấn công đã bị kết án theo Luật chống tài trợ khủng bố. Ngoài ra, ông Y đã bị liệt vào danh sách trừng phạt UNSCR 1267 và Danh sách khủng bố trong nước của Indonesia.

NHẬT BẢN

280 Một nam nhân viên văn phòng nhận được thông tin về tiền điện tử qua email từ một thành viên của nhóm lừa đảo biết rằng thông tin đó được lấy một cách bất hợp pháp. Anh ta bị bắt vì vi phạm Đạo luật trừng phạt tội phạm có tổ chức (vì đã nhận tiền có nguồn gốc tội phạm)

4.9 Rửa tiền thu được từ hoạt động trốn thuế

TRUNG QUỐC

Vụ việc điển hình thứ nhất

281 Vào tháng 12 năm 2017, cơ quan giám sát đã nhận được các STR về 4 tập đoàn lớn từ một tổ chức tài chính. Sau khi điều tra thêm, cơ quan giám sát đã cung cấp thông tin cho cảnh sát địa phương. Cảnh sát nhận thấy rằng Tập đoàn G đã làm sai các hóa đơn VAT. Vào tháng 4 và tháng 5 năm 2018, sáu nghi phạm đã bị bắt giữ. Tại thời điểm viết báo cáo này, ba nghi phạm vẫn bị giam giữ và ba nghi phạm còn lại đang được tại ngoại chờ xét xử.

282 Trong thời gian từ tháng 1 năm 2017 đến tháng 4 năm 2018, các công ty liên quan đến vụ việc này đã làm sai lệch hơn một nghìn hóa đơn VAT đặc biệt, trốn thuế hàng triệu nhân dân tệ.

Vụ việc điển hình thứ hai

283 Vào tháng 2 năm 2018, cơ quan giám sát đã cung cấp các STR về giả mạo hóa đơn đặc biệt cho cảnh sát. Vào tháng 6 năm 2018, cảnh sát và cơ quan thuế địa phương đã thành lập một Đoàn liên ngành để điều tra vụ án này. Vào tháng 7 năm 2018, nhóm đã tiêu diệt thành công bốn ổ nhóm tội phạm, năm băng đảng tội phạm và bắt giữ 23 nghi phạm. Đoàn liên ngành cũng đã bắt giữ hơn một nghìn con dấu công ty, hàng trăm thẻ ngân hàng và chìa khóa USB, hơn 80 sổ sách tài chính, 90 giấy phép kinh doanh của các công ty vỏ bọc, 50 đĩa kiểm soát thuế, hàng ngàn hóa đơn VAT giả mạo và đóng băng hàng triệu nhân dân tệ.

FIJI

Rửa tiền kinh doanh thông qua kinh doanh thâm dụng tiền mặt

284 Công ty A đã bị tố cáo rằng đã thực hiện gửi một lượng tiền mặt lớn và sau đó dùng tiền mặt này để mua các séc ngân hàng.

285 FIU đã chứng minh rằng Công ty A đã không nộp tờ khai thuế trong năm 2016 và 2017. Tuy nhiên, công ty đã nhận được khoản tiền gửi khoảng 6,4 triệu tiền FJ . Phân tích sâu hơn cho thấy rằng cổ đông, Cá nhân O và vợ anh ta-cá nhân P đã nhận được khoảng \$740,000.00 dưới dạng tiền gửi vào tài khoản ngân hàng của họ và cũng không nộp tờ khai thuế

286 Một báo cáo cảnh báo về trường hợp này đã được gửi cho cơ quan thuế về Công ty A, Người O và Người P để điều tra

Các hành vi phạm tội có thể là:

- Tội trốn thuế.

Các dấu hiệu:

- Gửi một lượng tiền mặt quá lớn.
- Sử dụng thành viên gia đình để trợ giúp việc trốn thuế.
- Sử dụng kinh doanh chuyên sâu về tiền mặt để rửa tiền.

Viện có trốn thuế bằng cách đa dạng hóa hoạt động kinh doanh và sử dụng thành viên gia đình

287 FIU đã nhận được một STR về cá nhân A, người được cho là đã chuyển tiền kinh doanh vào tài khoản ngân hàng cá nhân của anh ta. Cá nhân A là giám đốc của Công ty X và đồng thời cũng vận hành một trạm bơm nhiên liệu trong cùng tòa nhà.

288 FIU đã tiến hành kiểm tra tài chính và xác định rằng Cá nhân A đã sử dụng tài khoản ngân hàng cá nhân của mình để thanh toán cho Công ty Y để cung cấp nhiên liệu cho trạm bơm. FIU đã tiến hành kiểm tra thêm và xác định rằng Cá nhân A đã nhận được một lượng lớn tiền mặt và séc gửi vào tài khoản ngân hàng cá nhân của mình. Nó đã được chứng minh rằng rằng hầu hết khoản tiền mặt và séc này được rút trên tài khoản kinh doanh của Công ty X.

289 FIU đã nắm giữ thông tin tình báo trước đó về con trai của Cá nhân A, người cũng bị tố cáo về một số hành vi trốn thuế. FIU đã tiến hành kiểm tra thêm và ghi nhận các khoản nộp thuế còn tồn đọng cho Cá nhân A và con trai ông ta

290 Một báo cáo đã được gửi tới cơ quan thuế để cảnh báo về các tội phạm trốn thuế.

Các hành vi phạm tội có thể là:

- Tội trốn thuế.

Các dấu hiệu:

- Không khai nộp thuế với cơ quan thuế.
- Gửi một lượng lớn tiền kinh doanh vào tài khoản cá nhân.
- Sử dụng thành viên trong gia đình để trốn thuế.
- Đa dạng hóa hoạt động kinh doanh để trốn thuế.

Sử dụng bên thứ ba để trốn thuế

291 Công ty Y bị tố cáo là đã gửi một lượng tiền mặt đáng kể dưới dạng ‘hoàn trả khoản vay’ từ một nhân viên. FIU đã nhận được một báo cáo trước đây về Công ty Y cho các hoạt động tương tự

292 FIU đã xác định rằng Công ty Y đã nhận một lượng tiền gửi lên tới gần 12 triệu tiền FJ từ năm 2016 đến năm 2018 và không nộp tờ khai thuế trong khoảng thời gian này. Các hồ sơ khác cũng chỉ ra rằng các giám đốc của công ty Y cũng là giám đốc của một vài công ty khác và các công ty này cũng đã từng bị tình nghi liên quan đến các hoạt động trốn thuế.

293 Một báo cáo về trường hợp này cũng đã được gửi đến cơ quan thuế để điều tra.

Các hành vi phạm tội có thể là:

- Tội trốn thuế.

Các dấu hiệu:

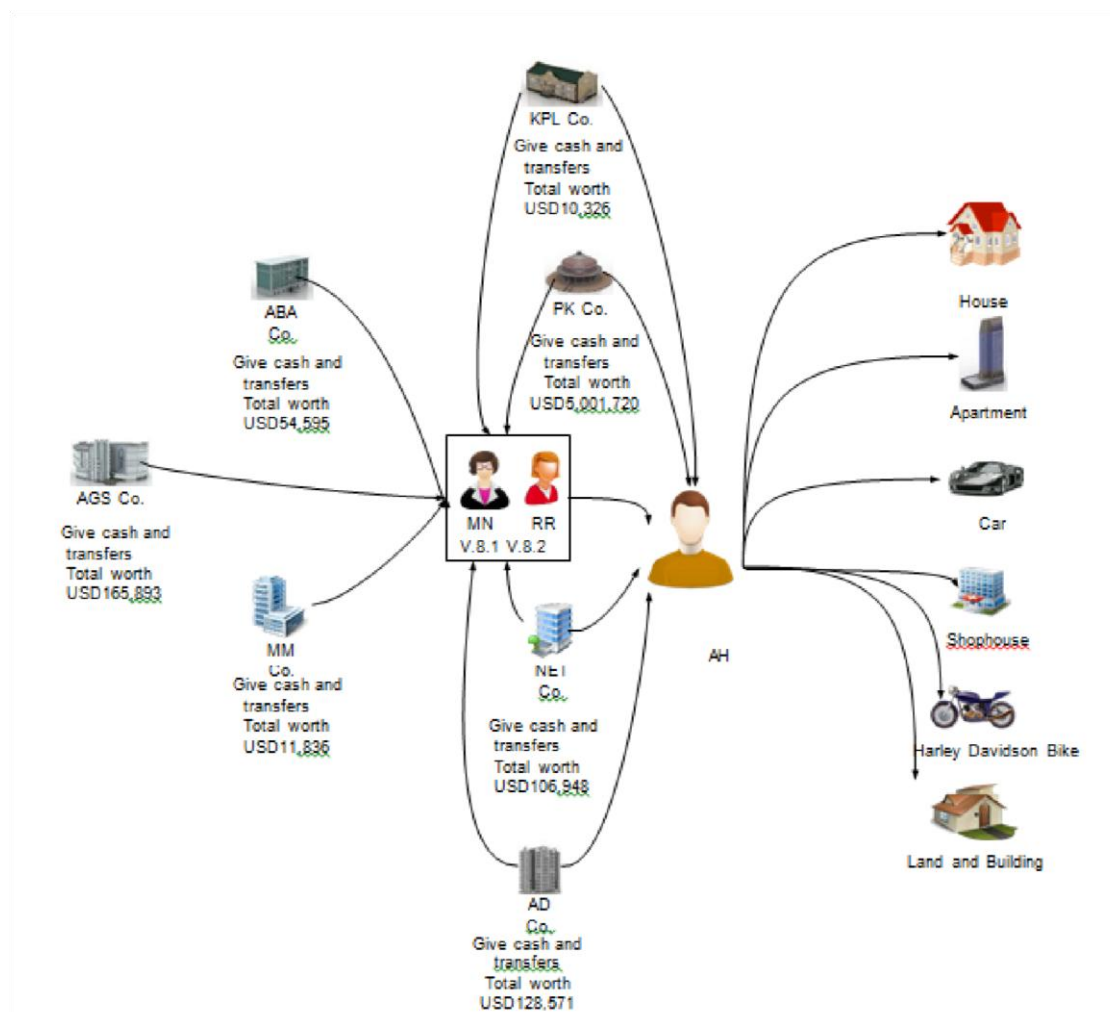
- Có một lượng lớn tiền mặt gửi vào ngân hàng.
- Sử dụng bên thứ ba.
- Sử dụng các công ty liên kết.

INDONESIA

294 AH là Giám đốc điều hành của Tập đoàn LPS Co. Ông ta đã sản xuất hàng loạt hóa đơn thuế dựa trên các giao dịch giả mạo và bán chúng cho bảy công ty. Ông ta đã thu được tổng số tiền lên tới 3.510.621 USD. Hầu hết số tiền ông ta nhận được từ việc bán hóa đơn thuế giả là tiền mặt và phần còn lại được gửi đến tài khoản ngân hàng cá nhân của ông ta. Ông cũng yêu cầu nhân viên của mình nhận tiền mặt và gửi tiền đó vào tài khoản ngân hàng cá nhân của ông ta.

295 Sau khi nhận được tiền trong tài khoản ngân hàng cá nhân của mình, AH đã mua tài sản bằng tên của ông ấy và tên của người thân/gia đình của ông ấy (ví dụ: vợ và con của ông ấy). Ông ta đã mua đất và tài sản bằng cách sử dụng số tiền mặt lên tới 71.428 USD trong một ngày. Ông ta cũng xây dựng nhà ở chung hoặc văn phòng trên mảnh đất đã mua để có thêm tiền và đầu tư vào các công ty khác. Để che giấu hơn nữa nguồn gốc của số tiền, ông ta đã kết hợp các khoản tiền bất hợp pháp với tiền của công ty mình.

296 Theo các thông tin thu thập được từ cơ quan Thuế, ông ta đã giữ tiền bằng đồng IDR nhưng sau đó rút tiền ra bằng đồng USD.



PAKISTAN

Bối cảnh của vụ việc:

297 Nhiều tài khoản đã được mở bởi nghi phạm ở các ngân hàng khác nhau và dưới tên vợ /chồng, con gái và con trai của ông ta. Một lượng lớn tiền liên quan đến một doanh nghiệp dệt may cả bằng nội tệ và ngoại tệ đã được chuyển đến các tài khoản của thành viên gia đình để trốn thuế.

Cách thức hoạt động:

298 Một cá nhân, ông X, đã mở tài khoản cá nhân và đối tác ở các chi nhánh khác nhau của các ngân hàng khác nhau. Một trong nhiều tài khoản đã được một ngân hàng báo cáo cho FMU vì một mô hình tiền gửi bất thường vào tài khoản trong một khoảng thời gian ngắn đã được xác định.

299 Số tiền mặt khoảng 62 triệu đồng PKR được gửi qua 80 giao dịch trong đó 77 giao dịch được cơ cấu. Các khoản tiền tích lũy được sau đó đã được rút qua bốn công cụ trong cùng một ngày để ủng hộ một cá nhân có tên là Z với mục đích mua một tài sản. Cần lưu ý rằng tất cả các giao dịch tiền gửi có cấu trúc được thực hiện trong khoảng thời gian nửa giờ thông qua nhiều phiếu gửi tiền. Hơn nữa, người ký các phiếu gửi tiền cũng được tìm thấy là cùng một người. Hoạt động như vậy trong tài khoản không có ý nghĩa về mặt logic hay tính kinh tế. Hơn nữa, khách hàng không cung cấp bất kỳ chi tiết nào về nguồn tiền được gửi bằng tiền mặt vào tài khoản và khách hàng không cung cấp bằng chứng tài liệu cho ngân hàng liên quan đến việc mua bất động sản.

300 Trong quá trình phân tích, người ta đã xác định rằng số tiền thu được ở trên là từ hoạt động kinh doanh của nghi phạm. Những khoản tiền đó đã được chuyển qua tài khoản sở hữu của vợ hoặc chồng của nghi phạm bằng cách giao dịch tiền mặt có cấu trúc để tránh bị báo cáo với FMU.

301 Các tài khoản của các thành viên gia đình của nghi phạm được xác định thông qua một tìm kiếm cơ sở dữ liệu nội bộ của FMU và doanh thu cao đã được phát hiện trong các tài khoản đó. Điều thú vị là nghi phạm và các thành viên gia đình của anh ta đã được tìm thấy là có đăng ký Mã số thuế nước. Chỉ có nghi phạm đã tự đóng thuế thu nhập trong khi không có thành viên nào trong gia đình anh ta đóng thuế thu nhập, mặc dù thực tế là họ đang thực hiện các giao dịch có giá trị cao trong tài khoản tương ứng của họ.

302 Từ các hoạt động được mô tả ở trên, người ta đã nghi ngờ rằng các cá nhân được báo cáo có liên quan đến trốn thuế thu nhập. Do đó, cơ quan tình báo tài chính đã gửi báo cáo đến cơ quan thuế

4.10 Bất động sản, bao gồm cả vai trò của các công ty Bất động sản

TRUNG QUỐC

303 Nghi phạm V là đại diện pháp lý, cổ đông và người giám sát của nhiều công ty đầu tư và công nghệ. Một trong những công ty này đã xúc tiến một dự án, mà dự án đó yêu cầu chủ sở hữu nhà phải sử dụng nhà của họ để đảm bảo các khoản vay từ ngân hàng. Công ty sẽ trả một khoản thu nhập cố định cho chủ sở hữu nhà, và cũng trả tiền gốc và lãi của khoản vay. Các đối tác giao dịch cũng bao gồm các công ty đầu tư, công ty tài chính vi mô và công ty thương mại. Dự án này đã được xác định rằng có các đặc điểm của việc gây quỹ bất hợp pháp và nó sẽ có rủi ro cao nếu chuỗi cung ứng vốn bị phá vỡ. Các thông tin về trường hợp này và các tin tức tình báo khác đã được cung cấp cho cảnh sát.

PAKISTAN

304 Bị cáo X đã chiếm đoạt được sáu tài sản ở Anh trị giá 6.885.625 GBP trong giai đoạn 2004-2006. Các tài sản này sau đó đã được chuyển thành các tài sản giữa các công ty được kiểm soát bởi một số bị cáo khác với mức giá tăng từ 5 đến 16 lần so với giá gốc. Trên cơ sở giá tăng cao, các bị cáo đã chiếm đoạt được khoản tạm ứng thế chấp với tổng trị giá 49.276.250 GBP thông qua định giá tài sản không trung thực. Trong giai đoạn 2004 đến 2006, 20 giao dịch đã được thực hiện để chuyển một số tiền gian lận là 28.883.098 GBP cho các ngân hàng Pakistan. Ông X đã bị kết án 13 năm tù bởi một tòa án ở Anh vào năm 2011. Trong khi đó, bị cáo Y, đã trốn sang Pakistan. Ông Y, theo

báo cáo, đã mang hơn 25 triệu GBP tài sản bị đánh cắp đến Pakistan. Các nhà chức trách Anh đã yêu cầu hỗ trợ để thu hồi tài sản tội phạm do những bị cáo ở Pakistan nắm giữ bất hợp pháp. Sau khi bắt đầu một cuộc điều tra, Ban nước thực thi giải trình (NAB) đã thu thập thông tin tài chính có liên quan từ nhiều cơ quan và tổ chức tài chính khác nhau và do đó, 12 khu dân cư và đất nông nghiệp đã bị cảnh cáo theo điều 23 của Pháp lệnh Trách nhiệm Nước Pakistan (thông báo của NAB để tránh việc chuyển nhượng tài sản). Trường hợp này hiện đang ở giai đoạn điều tra.

4.11 Liên quan đến nạn buôn người trái phép

AFGHANISTAN

305 Công ty cung ứng dịch vụ tiền (MSP X) hoạt động với tư cách là người bảo lãnh bằng cách nhận tiền trả góp để đi lao động ở nước ngoài từ các công dân Afghanistan. MSP X phối hợp tuyển dụng với một tổ chức nước ngoài (XYZ) bất chấp các quy định về tuyển dụng lao động ở nước ngoài. Những người Afghanistan được tuyển dụng đã gửi các khoản tiền trả góp vào tài khoản ngân hàng của MSP X và MSP X không thể cung cấp hồ sơ chứng minh cho các khoản tiền gửi này. Những người Afghanistan được tuyển dụng sau đó đã bị buôn lậu ra nước ngoài thông qua các tuyến đường có rủi ro rất cao tại các tỉnh biên giới Afghanistan.

306 Do đó, giấy phép của công ty này đã bị thu giữ và vụ việc nói trên đã được gửi đến cơ quan thực thi pháp luật liên quan để tiến hành các thủ tục theo pháp luật.

FIJI

307 Bà GC và chị gái sinh đôi của mình – bà SR điều hành các công ty lữ hành độc lập và họ đã đăng quảng cáo trên báo về việc tuyển dụng các cá nhân có nhu cầu đến New Zealand để thu hoạch trái cây và xây dựng. Quảng cáo đã thu hút 17 cá nhân, họ được hứa hẹn trả lương cao, được lo chỗ ở, ăn uống, đi lại và sáu ngày làm việc từ 7 giờ sáng đến 5 giờ chiều. 17 cá nhân này đã được cấp thị thực du khách New Zealand và được thông báo giấy phép lao động sẽ được cấp khi họ đến New Zealand. Họ phải trả phí tư vấn, phí thuê nhà, phí hành chính, cấp hộ chiếu và tiền vé với tổng giá khoảng 3.768,00 FJ mỗi người.

308 17 cá nhân này được yêu cầu chỉ ký vào các đơn xin cấp thị thực bỏ trống thông tin và bà GC và bà SR đã điền các thông tin giả mạo vào các đơn này.

309 Sau khi đến New Zealand, hầu hết 17 cá nhân nêu trên đã được ông FA đón tại sân bay. Các nạn nhân sau đó đã được đưa đến một nơi mà họ phải ngủ chung phòng với những người lạ khác giới, ngủ trên đệm hoặc dưới sàn nhà và thay quần áo trong cùng một phòng. Các nạn nhân phải trả tiền cho việc đi lại và đồ ăn đôi lúc là đồ sống và mất vệ sinh. Các cá nhân này cũng được chi trả số tiền ít ỏi.

310 Một số nạn nhân đã liên lạc với NZP để thông báo về tình hình của họ. Các cuộc điều tra đã được tiến hành đồng thời ở New Zealand và Fiji.

NEW ZEALAND

Công nhân làm vườn bị buộc tội buôn bán nô lệ và buôn người

311 Một công nhân vườn cây ăn quả Hawke's Bay gần đây đã bị buộc tội buôn bán nô lệ và buôn người vì những vi phạm ở Samoa và Hawke's Bay. Anh ta bị cáo buộc đã dụ dỗ công dân Samoa đến New Zealand với lời hứa về những công việc được trả lương

cao, nhưng khi họ đến, anh ta đã tịch thu hộ chiếu của họ, kiểm soát và theo dõi họ chặt chẽ, bắt họ phải chịu hành hung và đe dọa. Anh ta đã ký hợp đồng với các nạn nhân ở nhiều vườn cây khác nhau ở Hawke's Bay, nhận các khoản thanh toán thông qua các tài khoản ngân hàng cá nhân của mình cho các dịch vụ hợp đồng lao động được thực hiện.

PHILIPPIN

312 Cơ quan tình báo Philippines được một cơ quan thực thi pháp luật Philippines thông báo về việc ba công dân Philippines và tám công dân nước ngoài bị cáo buộc liên quan đến buôn bán người và khiêu dâm trẻ em. Các bị cáo điều hành một tụ điểm tình dục máy tính (cybersex den) ở Central Visayas và tuyển dụng trẻ vị thành niên để tham gia vào các hành vi khiêu dâm. Năm 2014, Cảnh sát Thủ đô ở nước U đã tịch thu máy tính, máy tính bảng, điện thoại di động, máy ảnh, ổ cứng và DVD chứa hình ảnh và video không đứng đắn của trẻ em Philippines thuộc sở hữu của một người nước ngoài - ông C. Các video cho thấy trẻ em Philippines bị ông C và các phụ nữ Philippines trưởng thành lạm dụng tình dục/thể xác. Các tài liệu thu hồi cũng cho thấy một số lần chuyển tiền cho ba công dân Philippines. Qua theo dõi, số tiền được phát hiện có nguồn gốc từ nước U và C và được chuyển đến Philippines thông qua hai đại lý chuyển tiền và một ngân hàng địa phương, trung bình khoảng 2 nghìn Php mỗi lần chuyển tiền. Tổng số tiền được phát hiện là 2,38 triệu Php liên quan đến các khoản chuyển tiền và tiền gửi khác nhau và Php2,06 triệu được rút. Qua các phát hiện này, lệnh đóng băng, kiến nghị tịch thu dân sự đã được ban hành và việc nộp đơn kiện rửa tiền đã được thực hiện đối với các bị cáo vào năm 2016.

4.12 Sử dụng người đại diện, lạm dụng tín nhiệm, thành viên trong gia đình hoặc bên thứ ba

TRUNG QUỐC

Vụ việc điển hình thứ 1

313 Qua điều tra, cơ quan chức năng phát hiện Nghi phạm U đã tham ô hàng triệu nhân dân tệ bằng cách lạm dụng vị trí của mình. Nghi phạm U sau đó yêu cầu Nghi phạm B gửi tiền vào tài khoản của Nghi phạm B. Theo sự sắp xếp của vợ Nghi phạm U (Nghi phạm O), Nghi phạm D đã rút tiền, sau đó chuyển phần lớn số tiền cho Nghi phạm P – anh/em rể của O. Sau đó, Nghi phạm P đã chuyển tiền cho con trai của Nghi phạm O dưới tên khách sạn của anh ta. Nghi phạm O sau đó đã yêu cầu Nghi phạm D chuyển số tiền còn lại cho vợ của Nghi phạm P (người bị kiểm soát bởi Nghi phạm O), và sau đó Nghi phạm O đưa thẻ ngân hàng cho con trai bà.

314 Vào tháng 11/2018, Nghi phạm O bị kết án tội rửa tiền và bị kết án 02 năm tù giam, 02 năm án treo và phạt tiền. Nghi phạm P bị kết án tội tương tự và 10 năm tù giam, 01 năm án treo và phạt tiền.

Vụ việc điển hình thứ 2

315 Nghi phạm Q nhận hối lộ và bị kết án về tội nhận hối lộ. Trong quá trình điều tra, Nghi phạm Q và vợ đã yêu cầu anh trai của họ - Nghi phạm K chuyển hàng triệu nhân dân tệ và hàng ngàn đô la Hồng Kông. Nghi phạm K sau đó đã đưa một số tiền mặt cho Nghi phạm T. Vào tháng 04/2018, tòa đã kết án Nghi phạm K hai năm và mười tháng tù giam và một khoản tiền phạt. Nghi phạm T bị kết án ba năm mười tháng tù giam cùng với một khoản tiền phạt.

Vụ việc điển hình thứ 3

316 Trong một cuộc điều tra về việc hối lộ của Nghi phạm R, em gái của Nghi phạm R – Nghi phạm G bị tình nghi rửa tiền. Từ năm 2012 - 2016, mặc dù nhận thức rõ về các hoạt động của Nghi phạm R, Nghi phạm G vẫn tiếp tục giữ và gửi số tiền hối lộ của Nghi phạm R vào tài khoản ngân hàng của mình. Nghi phạm G sau đó đã mua nhà, xe theo sự sắp xếp của R. Vào tháng 12 năm 2018, Nghi phạm G đã bị kết án một năm tù giam, một năm quản chế cùng với một khoản tiền phạt.

ĐÀI LOAN

317 Năm 2016, giá cổ phiếu của công ty T - một công ty niêm yết đã sụt giảm. Ông C quyết định thao túng giá cổ phiếu của Công ty T. Ông C hợp tác với một nhà đầu cơ thị trường chứng khoán - ông D và sử dụng 42 tài khoản chứng khoán do họ kiểm soát để mua và bán một lượng lớn cổ phiếu của công ty T. Họ đã sử dụng các tài khoản chứng khoán này để thực hiện các giao dịch nhằm tạo ấn tượng về giao dịch nhanh chóng của cổ phiếu của công ty T. Họ cũng đưa ra những tin tức giả mạo về việc vốn nước ngoài sẽ được đầu tư vào công ty T. Vì vậy, các nhà đầu tư không nắm rõ đã nhầm rằng cổ phiếu của công ty T đáng để đầu tư và đã giao dịch cổ phiếu của công ty T. Giá cổ phiếu của công ty T đã bị thao túng từ khoảng 6NT mỗi cổ phiếu vào tháng 8 năm 2016 đến khoảng 20NT mỗi cổ phiếu vào tháng 2 năm 2017.

318 Hội đồng quản trị của Công ty T đã được bầu lại vào tháng 5 năm 2017. Ông C loan báo thông tin giả mạo rằng ông sẽ tham gia cuộc bầu cử và giành quyền quản lý để các nhà đầu tư không nắm rõ tham gia đầu tư. Tuy nhiên, ông C và đồng sự liên tiếp bán cổ phiếu của Công ty T mà họ đã mua với giá thấp hơn trước đó cho các nhà đầu tư vào tháng 2 hoặc tháng 3/2018 (thời điểm giá cổ phiếu của Công ty T cao và giao dịch nhanh chóng) và thu được lợi nhuận lớn. Tổng lợi nhuận mà họ nhận được là khoảng 1,1 tỷ NT. Ông C và đồng phạm bị buộc tội vi phạm Luật Chứng khoán và Giao dịch vào tháng 8 năm 2018.

FIJI

Vi phạm lợi dụng lòng tin của chủ lao động và thao túng hệ thống và quy trình nội bộ

319 Bà Rosheen Praveena Raj và bà Rine Munivai Sorby được tuyển dụng làm nhân viên tài chính tại Đại học Thần học Thái Bình Dương (PTC). Họ chịu trách nhiệm xử lý séc tiền lương và hóa đơn. Từ năm 2006 - 2011, bà Rosheen Praveena Raj và bà Rine Munivai Sorby đã thao túng hệ thống này để biến thủ số tiền với tổng giá trị 582.244,42 FJ\$. Do được chịu trách nhiệm cho tất cả các tài khoản phải trả bao gồm cả bảng lương, bà Rosheen Praveena Raj đã can thiệp vào bảng tính tiền lương hàng tuần, chứng từ thanh toán và séc để xử lý các khoản thanh toán tiền lương vượt quá 96,576,86 FJ\$ cho chính mình và 73,099.93 FJ\$ cho bà Rine Munivai Sorby.

320 Những hành vi lừa đảo nêu trên được phát hiện khi ông Nilesch Avinesh Sharma được bổ nhiệm làm Giám đốc Tài chính và Quản trị vào năm 2012. Ông đã phát hiện ra sự bất thường lớn trong hồ sơ tài chính và tiến hành điều tra và kiểm toán nội bộ để xác định nguyên nhân của những bất thường này. Bà Rosheen Praveena Raj và bà Rine Munivai Sorby đã can thiệp vào séc thanh toán hóa đơn để thanh toán tổng số tiền là 412,567,61 FJ\$ cho chính họ. Ngày 18/9/2018, bà Rosheen Praveena Raj và bà Rine Munivai Sorby bị kết tội rửa tiền. Ngày 19/9/2018, bà Rosheen Praveena Raj và bà Rine Munivai Sorby đã bị kết án 11 và 10 năm tù.

Chuyển tiền lớn giữa các cá nhân không liên quan giữa các nước

321 Cơ quan tình báo tài chính nhận được một báo cáo giao dịch đáng ngờ về việc Cá nhân Y nhận được số tiền khoảng 167,000.00 FJ\$ từ một cá nhân không liên quan – Cá nhân X ở nước D.

322 Cá nhân Y khai báo rằng số tiền này dành cho việc xây dựng bất động sản của Cá nhân Y. Cơ quan tình báo tài chính Fiji đã xác minh được cá nhân Y đã mua đất trị giá 100.000,00\$ vào năm 2018. Cá nhân Y đã không khai báo bất kỳ thu nhập nào trong hai năm qua và cá nhân này dường như không có việc làm.

323 Cơ quan tình báo tài chính cũng đã phát hiện Cá nhân X có khả năng là người được các cơ quan thực thi pháp luật ở nước D để ý và có thể đã sử dụng Người Y để rửa tiền ở Fiji.

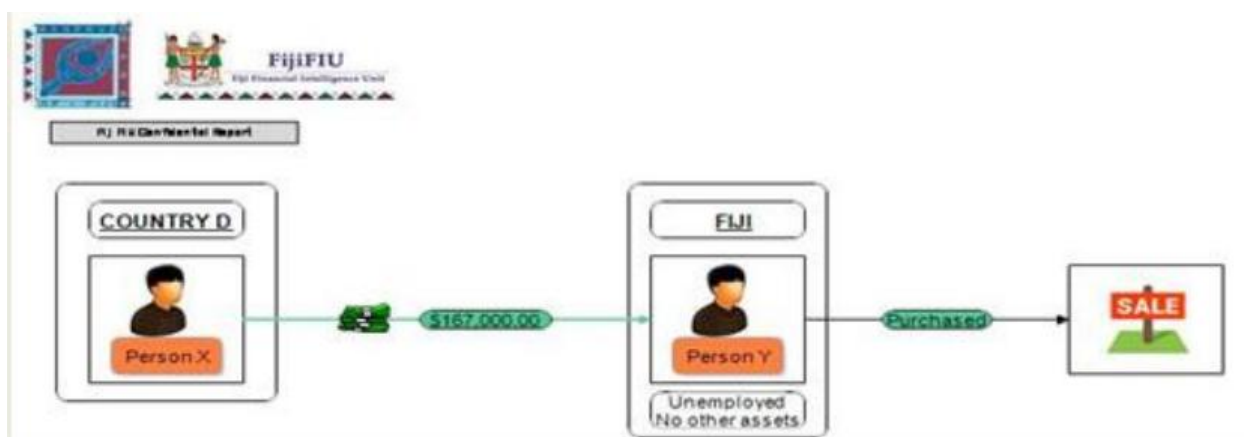
324 Một báo cáo đã được gửi đến Cục Tình báo Cảnh sát Fiji và Cơ quan tình báo FIJI tại nước D để tiếp tục thu thập hồ sơ.

Tội có thể vi phạm:

- Tội rửa tiền.
- Trốn thuế.

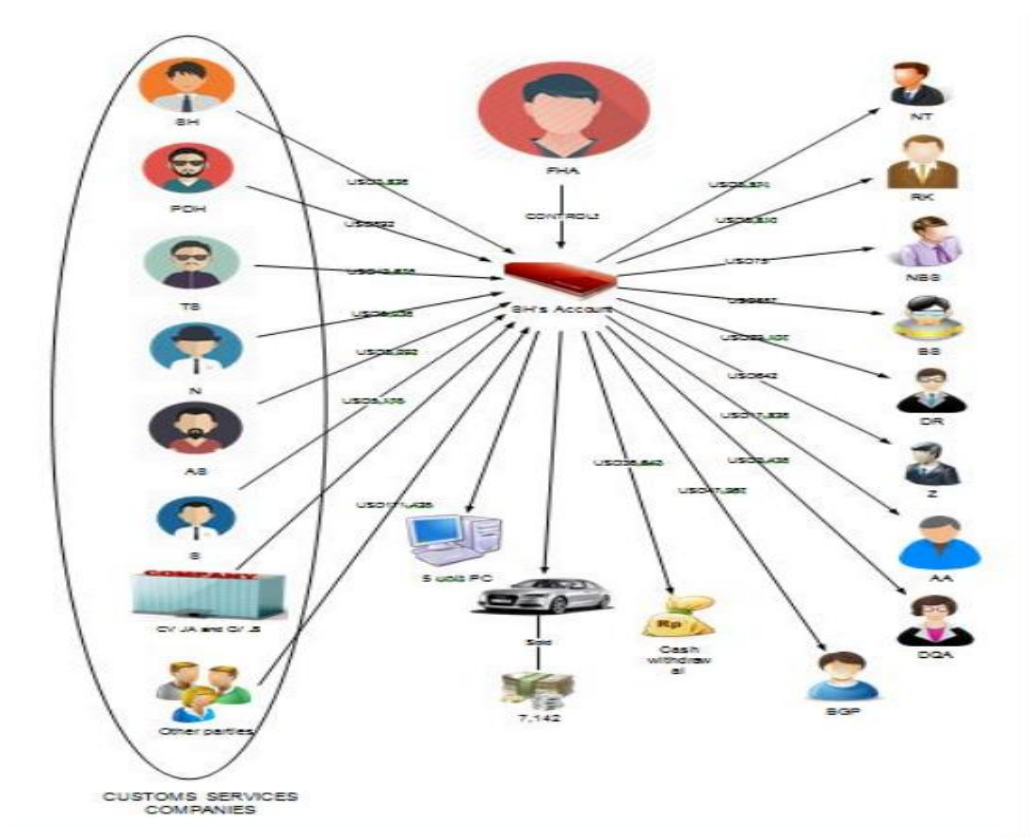
Các dấu hiệu:

- Chuyển tiền lớn giữa các cá nhân trong và ngoài nước không có mối quan hệ rõ ràng.



INDONESIA

325 FHA là một chuyên gia phân tích tại Tổng cục Hải quan và Thuế. Anh ta mượn tài khoản của SH - chủ sở hữu của AMJ Co để cất giấu tiền hối lộ nhận được từ các công ty dịch vụ hải quan mà anh ta phân tích. AMJ Co. cũng là một trong những công ty được phân tích. Tiền từ các tài khoản của SH đã được rửa bằng cách chuyển vào các tài khoản khác nhau và sau đó được sử dụng để mua tài sản như xe hơi và máy tính.



NHẬT BẢN

326 Một người đàn ông làm việc cho một công ty thương mại đã giấu một chiếc xe bị đánh cắp trong một nhà kho ở bãi container theo hợp đồng được thực hiện dưới tên của một cá nhân khác – cá nhân này biết rằng đây là chiếc xe bị đánh cắp. Anh ta bị bắt vì che giấu tài sản bị đánh cắp và vi phạm Luật trừng phạt tội phạm có tổ chức (che giấu tài sản có được từ phạm tội).

327 Nghi phạm cố tình nhận số tiền bất hợp pháp có nguồn gốc từ mại dâm khi những kẻ bảo kê gửi vào tài khoản ngân hàng được mở dưới tên con gái của một thành viên nhóm Boryokudan (nhóm tội phạm có tổ chức của Nhật Bản).

MA CAO, TRUNG QUỐC

328 Theo một STR, ông A - Phó giám đốc bộ phận quản lý tài khoản của một công ty hàng hải ở nước H đã nhận được nhiều khoản tiền với tổng giá trị khoảng sáu triệu từ tài khoản ngân hàng của mình tại nước H từ tháng 9-10/2015. Sau đó, Ông A đã mua hàng tại các cửa hàng trang sức ở Macao, Trung Quốc bằng thẻ ghi nợ của mình và chuyển tiền cho bạn gái cũ – bà B. Sau khi xem xét, cơ quan chức năng phát hiện tài khoản ngân hàng của bà B có một số lượng lớn tiền mặt được gửi thông qua các máy chuyển tiền và Bà B đã nhận được các khoản tiền từ bạn trai kể từ năm 2015.

329 Tháng 03/2016, công ty hàng hải nêu trên đã phát hiện ra rằng ông A bị nghi ngờ biển thủ khoảng 380 triệu HKD từ năm 2010 - 2016. Công ty đã báo cáo thông tin trên cho các cơ quan thực thi pháp luật của nước H. Sau khi biết các khoản tiền bất hợp pháp đã được chuyển đến Ma Cao, Trung Quốc, công ty hàng hải đã cử một đại diện đến Macao, Trung Quốc để báo cáo vụ việc với Cảnh sát tư pháp Ma Cao. Tháng 01/2018, tin tức cho biết Cảnh sát Tư pháp đã bắt giữ bà B. Các thành viên trong gia

đình bà B bị buộc tội rửa tiền thông qua hành vi mua bất động sản, xe hơi và các tài sản có giá trị. Tài sản trị giá khoảng 40 triệu HKD bao gồm tiền mặt đã bị thu giữ.

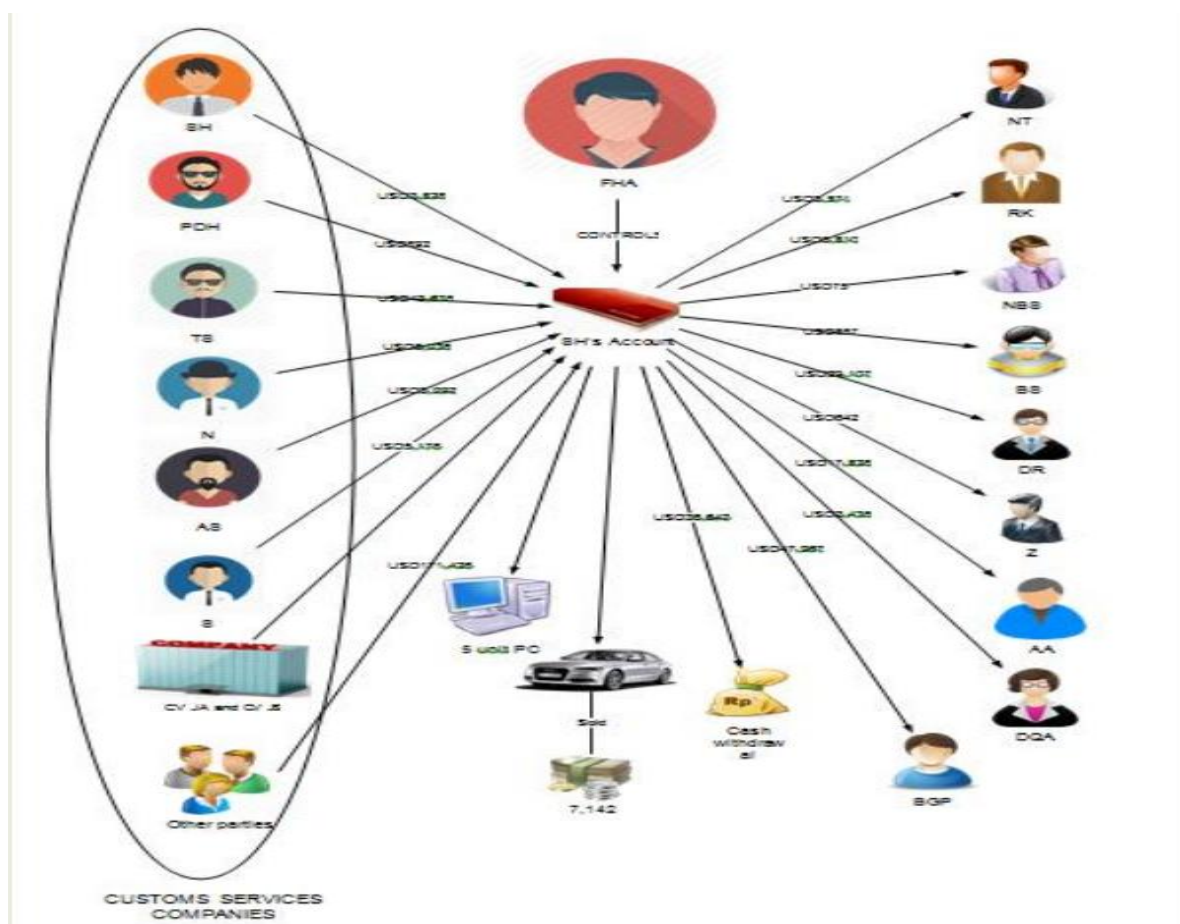
330 Qua điều tra, xem xét, Cơ quan tình báo tài chính nhận thấy tài khoản ngân hàng của bà B nhận được các khoản tiền không thường xuyên và tăng đột biến đến hơn 21 triệu HKD vào năm 2015. Sau đó, các khoản tiền này được sử dụng để mua bất động sản và tài sản có giá trị nhằm mục đích bán lại. Bà B đã chuyển lại số tiền bán hàng cho ông A. Điều rất đáng ngờ là ông A đã sử dụng bạn gái cũ - bà B và gia đình bà B để tẩu tán các tài sản phạm tội ở Ma Cao, Trung Quốc sau khi hành vi sai trái của ông A bị phát hiện ở khu vực tài phán H. Cảnh sát Tư pháp cuối cùng đã chuyển vụ việc cho Văn phòng Công tố.

SINGAPORE

Sử dụng người đại diện – Liên minh các công ty vỏ bọc để nhận các khoản thanh toán hối lộ từ nước ngoài

331 Với tư cách là đầu mối tiếp nhận thông tin, thông qua phân tích tình báo tài chính, CPIB nhận thấy có một mạng lưới các công ty Singapore có thể bị kiểm soát bởi người nước ngoài được sử dụng để nhận hoặc rửa các khoản tiền lớn có nguồn gốc đáng ngờ ở nước ngoài. Hai trong số các công ty Singapore có thể đã nhận được các khoản tiền liên quan đến hối lộ cho các cá nhân có ảnh hưởng chính trị ở nước ngoài.

332 Một cuộc điều tra đã được tiến hành đối với hai công ty Singapore và các giám đốc có liên quan đến mạng lưới các công ty Singapore. Điều tra sơ bộ cho thấy các giám đốc này đã cung cấp tên của họ để thành lập các công ty và mở tài khoản ngân hàng cho các công ty để hưởng phí. Sau đó họ đã chuyển cho các chủ sở hữu toàn quyền kiểm soát các tài khoản ngân hàng của công ty. Các công ty Singapore dường như là các công ty bình phong. Địa chỉ đã đăng ký của họ thuộc về một đại lý đã đăng ký (RFA) – đơn vị hỗ trợ cho việc thành lập các công ty. CPIB hợp tác với bộ phận điều hành của RFA để kiểm tra RFA. Yêu cầu cũng được gửi đến các cơ quan nước ngoài vì mục đích thu thập thông tin tình báo tài chính đối với các cá nhân và tổ chức. Các cuộc điều tra hiện đang diễn ra.



4.13 Các hoạt động đánh bạc (sòng bạc, đua ngựa, đánh bạc qua mạng ...)

TRUNG QUỐC

Vụ việc điển hình thứ nhất

333 Bốn nghi phạm đã mở tài khoản ngân hàng và chuyển tiền cho nhiều khách hàng thông qua ngân hàng trực tuyến và tiến hành chuyển tiền thử trước mỗi giao dịch. Tiền vào và ra từ tài khoản nhanh chóng, số dư rất thấp và địa chỉ IP thay đổi thường xuyên ở nhiều nơi. Các đối tác bao gồm các khách hàng đã bị các cơ quan chức năng điều tra do bị nghi ngờ tham gia đánh bạc trực tuyến. Số tiền liên quan đến vụ án đã lên tới hàng triệu nhân dân tệ và thông tin tình báo đã được cung cấp cho lực lượng cảnh sát.

Vụ việc điển hình thứ 2

334 Mười bốn công ty liên quan đến vụ việc này đã mở tài khoản tại cùng một thời điểm và địa điểm. Tất cả các tài khoản chia sẻ các ký tự giống nhau và tất cả các số liên lạc đều là thuê bao mới được đăng ký. Nội dung giao dịch bao gồm các từ như “top up” và “similar 6-digit membership number”. Giao dịch có thể được thực hiện vào mọi thời điểm trong ngày và một số giao dịch vào khoảng nửa đêm và đầu giờ trong ngày. Địa chỉ IP được tập trung vào các khu vực có rủi ro cao về đánh bạc. Tổng số tiền liên quan đến vụ việc này lên tới hàng triệu nhân dân tệ và các thông tin/thông tin tình báo đã được cung cấp cho lực lượng cảnh sát.

ĐÀI LOAN

335 Cơ quan điều tra thứ 4 của CIB đã đột kích các trang web cá cược. Sau khi theo dõi trang web cá cược trực tuyến của Bắc Kinh PK10 do nghi phạm Hsu dẫn đầu vào

ngày 5/9/2018, Cơ quan điều tra đã theo dõi để tìm ra một nghi phạm khác - Yao (quản trị ngầm và nhà cái). Sau khi sàng lọc các cảnh quay camera quan sát và theo dõi các nghi phạm bằng các phương tiện đi lại, Cơ quan điều tra nhận thấy các nghi phạm sống trong cùng một cộng đồng. Để ngăn chặn các nghi phạm di chuyển đến khu vực khác, Cơ quan điều tra ngay lập tức nộp đơn xin lệnh khám xét tại Tòa án quận. Khi thực hiện cuộc khám xét thứ hai vào ngày 17/9/2018, Cơ quan điều tra đã bắt giữ Peng - một nghi phạm khác tại ga ra. Các nghi phạm thú nhận đã điều hành một trang web cá cược trực tuyến. Trong quá trình khám xét nơi ở của nghi phạm, Cơ quan điều tra phát hiện Peng đã sử dụng máy đếm tiền mặt của mình để kiểm tra số tiền đặt cược hàng tuần. Số tiền đặt cược hàng tuần lên tới khoảng 10 triệu NT\$ mỗi tuần cho mỗi trong sáu đại lý độc quyền, số tiền đặt cược của trang web đã vượt quá 1 tỷ NT\$ trong sáu tháng. Cơ quan điều tra thứ 4 đã thu giữ bằng chứng bao gồm 1.982.000NT\$, hai điện thoại di động, sách và máy đếm tiền. Vụ việc bị kết tội đánh bạc.

HỒNG KÔNG, TRUNG QUỐC

336 Vào tháng 9/2017, cơ quan tình báo HKP đã xác định ông A là chủ mưu của một tổ chức cá cược có liên quan đến các hoạt động đánh bạc trực tuyến, đua ngựa và cá cược bóng đá ở Hồng Kông, Trung Quốc. Ông A cũng có thể đã mở rộng hoạt động sang các khu vực lân cận. Do đó, điều tra tài chính song song đã được tiến hành.

337 Vào tháng 6/2018, sau khi thực hiện các hành động, cơ quan thực thi đã bắt giữ 45 người vì tội cá cược và 05 người vì tội cá cược và rửa tiền với tổng số giá trị 02 triệu HKD tiền mặt bị tịch thu và 1,68 triệu HKD trong tài khoản bị giữ lại. Cuộc điều tra đang tiếp tục được tiến hành.

NHẬT BẢN

338 Các cựu thành viên của Boryokudan (nhóm tội phạm có tổ chức của Nhật Bản) đã cố tình nhận các khoản tiền tội phạm (950.000 JPY) có nguồn gốc từ một cửa hàng trò chơi đánh bạc bất hợp pháp. Họ đã bị bắt vì vi phạm Luật trừng phạt tội phạm có tổ chức (nhận tiền tội phạm).

HÀN QUỐC

339 Cá nhân J và 64 người khác là những người điều hành và thành viên của một đường dây vận hành các trang web đánh bạc trực tuyến bất hợp pháp. Từ năm 2011 – tháng 9/2018, họ đã ra mắt và vận hành các trang web cá cược thể thao như “Cola”, “Pasta” và “Y” ở Trung Quốc, Thái Lan và một số nơi khác. Họ bị cáo buộc che giấu số tiền thu được từ việc điều hành các trang web cờ bạc bất hợp pháp thông qua việc chuyển tiền vào các tài khoản được nắm giữ bởi dưới các tên mượn hoặc giả mạo hoặc thông qua hành vi mua bất động sản bằng tiền mặt và sau đó chuyển quyền sở hữu.

340 Vào ngày 24/5/2017, một cuộc điều tra sơ bộ đã được tiến hành sau khi nhận được báo cáo về các hoạt động tội phạm. Trong quá trình điều tra, tổng cộng 82 lệnh và giấy phép đã được thực hiện: 25 lệnh khám xét và thu giữ (đối với tài khoản tài chính), 27 lệnh khám xét và thu giữ (đối với cơ sở dân cư, v.v.) và 30 lệnh cho phép truy cập nhật ký liên lạc. Khoảng 15.000 con bạc và 109,2 tỷ KRW tiền đánh bạc đã bị phát hiện có liên quan. Số tiền tội phạm được xác định (rút tiền mặt) là 8,9 tỷ KRW và khoảng 13,1 tỷ KRW đã được tịch thu. Chi tiết như sau:

Nội dung (Bất động sản, tiền mặt, ...)	Tổng số tiền tịch thu
---	------------------------------

4 căn hộ (112 m2 , 188 m2 , etc.)	5,475 triệu KRW
Đất (1,150 m2), thiết bị chơi gôn trong nhà (tiền cho thuê), 3 cửa hàng cà phê internet	1,850 triệu KRW
8 xe hơi nhập khẩu (Mercedes Benz, Audi, etc.), 3 xe hơi sản xuất ở Hàn Quốc, 6 xe 02 bánh nhập khẩu	1,054.7 triệu KRW
Tiền mặt	3,3458.6 triệu KRW
229 tài khoản che dấu tài sản phạm tội	1,883.8 triệu KRW
Thiết bị tập gôn trong nhà (câu lạc bộ gôn, máy tính, ...)	187 triệu KRW
Tổng số	13.1 tỷ KRW (Thu giữ: 4,017.8 triệu KRW; Số tiền tịch thu trước truy tố: 9,083 triệu KRW)

341 Như đã trình bày ở trên, cảnh sát đã xác định 109,2 tỷ KRW tiền đánh bạc và thu giữ hoặc tịch thu các tài sản sau: i) bốn căn hộ, ii) tài sản bất động sản bao gồm đất đai, iii) xe hơi xa xỉ nhập khẩu và iv) tài khoản tiền mặt và tiền phạm tội bị che dấu. Các nhà chức trách đã thu hồi tổng cộng 13,1 tỷ KRW tiền phạm tội và trả lại cho Kho bạc nhà nước, đồng thời bắt giữ 140 người (11 người đang bị giam giữ) và giao nộp cho văn phòng công tố.

NEW ZEALAND

OCGs rửa tiền thông qua các sòng bạc ở New Zealand

342 Trong 18 tháng, ít nhất sáu cuộc điều tra tội phạm có tổ chức của New Zealand đã được tiến hành liên quan đến hành vi rửa các khoản tiền phạm tội thông qua các sòng bạc ở New Zealand. Các thủ đoạn rửa tiền cơ bản bao gồm sử dụng tiền có được từ phạm tội được để đánh bạc, nạp tiền mặt bất hợp pháp vào các máy chơi game trước khi hoàn trả tiền bằng séc sòng bạc và chuyển tiền bất hợp pháp vào tài khoản sòng bạc và sau đó chuyển chúng vào tài khoản ngân hàng thông thường. Các công ty chuyển tiền mặt làm việc cho các tổ chức rửa tiền đáng ngờ cũng đang gửi tiền cho các ông chủ sòng bạc. Một lượng tiền mặt bị tiêu tốn tại các sòng bạc bị nghi ngờ có nguồn gốc từ giao dịch ma túy trong nước. Liệu các ông chủ sòng bạc nhận được các khoản tiền này có liên quan đến rửa tiền hay không hay họ là những người thụ hưởng “trong sáng” của một hệ thống chuyển giá trị không chính thức.

VIỆT NAM

343 Năm 2017, thông qua việc truy tố và điều tra các đối tượng sử dụng internet để chiếm đoạt tài sản, Cảnh sát Việt Nam đã khởi tố một vụ án liên quan đến đánh bạc và tiến hành điều tra nhiều đối tượng và nhiều người tham gia bao gồm các cơ quan thực thi pháp luật ở nhiều tỉnh, thành phố ở Việt Nam. Trong vụ việc này, các đối tượng thành lập một doanh nghiệp CNTT và lợi dụng CNTT để tổ chức đánh bạc trực tuyến

như cá cược hoặc thẻ game. Các đối tượng này đã sử dụng nhiều thủ đoạn để thực hiện các hoạt động tội phạm như thẻ viễn thông, thẻ trò chơi để nạp tiền vào trò chơi đánh bạc, kết nối với cổng thanh toán của các công ty khác, thành lập đại lý để thu lợi nhuận từ đánh bạc, v.v.

344 Mạng lưới đánh bạc này có quy mô lớn nhằm che giấu và hợp lý hóa các khoản thu bất hợp pháp. Các đối tượng sử dụng các thủ đoạn khác nhau như đầu tư vào các dự án, góp vốn vào kinh doanh, mua bất động sản, gửi tiền, chuyển đổi thành vàng, ngoại tệ và chuyển tiền ra nước ngoài. Các nhà điều tra cho biết tổng số tiền được rửa là khoảng 38.000 USD.

345 Vào tháng 11/2018, Tòa án Nhân dân Tối cao Việt Nam đã kết án 92 người với các tội danh: “Tổ chức đánh bạc”, “Đánh bạc”, “Rửa tiền”, “Mua hóa đơn bất hợp pháp”, “Lạm dụng vị trí/quyền hạn”, “Sử dụng internet, viễn thông, thiết bị điện tử để chiếm đoạt tài sản”. Có 04 cá nhân bị kết án tội danh “Rửa tiền”. Cơ quan có thẩm quyền đã thu hồi khoảng 90% số tiền phạm tội từ những đối tượng bị kết án rửa tiền.

THÁI LAN

346 Đánh bạc qua mạng được tổ chức bất hợp pháp. Tài khoản ngân hàng được sử dụng để nhận tiền để mua điểm chơi và thường xuyên được thay đổi để tránh bị phát hiện các giao dịch lớn, do đó các tài khoản này bị đóng băng. Nhà cái đã sử dụng số tiền thu được để mua tài sản. Năm 2019, có 28 vụ việc với tổng tài sản bị thu giữ hoặc đóng băng lên tới hơn 20 triệu baht (660.000 USD).

4.14 Mingling (Đầu tư kinh doanh) và gian lận đầu tư

MALAYSIA

Vụ việc điển hình thứ 1: Kế hoạch đầu tư bất hợp pháp và lừa đảo

347 Chính quyền Malaysia đã triệt phá hoạt động của các tổ chức bị nghi ngờ lên kế hoạch đầu tư bất hợp pháp và lừa đảo. Cuộc điều tra có sự tham gia của Ngân hàng Trung ương Malaysia (BNM), Cảnh sát Hoàng gia Malaysia (RMP), Sở thuế vụ trong nước (IRB), Ủy ban các công ty Malaysia (CCM) và Ủy ban hợp tác xã Malaysia.

348 Các tổ chức đã thu hút người dân trong nước và quốc tế vào chương trình tài chính của họ bằng cách chào mời lợi nhuận cao trong một khoảng thời gian ngắn.

349 Phương thức, thủ đoạn của chương trình bất hợp pháp gồm:

- Người dân bị dụ dỗ tham gia một hợp đồng ngắn hạn để mua tiền điện tử của các tổ chức nói trên và sau đó được trả bằng vàng.
- Theo các chương trình, vàng được giữ lại bởi các tổ chức này nhằm mục đích giao dịch.
- Các chương trình cũng nhằm mục đích mang lại lợi nhuận hàng tháng cao tới 15% mỗi tháng.

350 Cuộc điều tra của các cơ quan có thẩm quyền tập trung vào việc vi phạm các điều khoản liên quan đến các chương trình đầu tư bất hợp pháp và lừa đảo. Các cuộc điều tra vẫn đang được tiến hành. Các tổ chức này cũng đã bị điều tra bởi cơ quan có thẩm quyền của nước láng giềng A về hành vi phạm tội gửi tiền bất hợp pháp xuyên nước – tới nước A.

351 Tài khoản ngân hàng lên tới hơn 4 triệu USD và các tài sản khác như xe hơi sang trọng đã bị thu giữ như một phần của quá trình điều tra

352 Phương thức rửa tiền gồm:

- Mua tài sản có giá trị;
- Chuyển tiền điện tử/Sử dụng tài khoản ngân hàng nước ngoài;
- Sử dụng tiền ảo; và
- Trộn lẫn các khoản tiền (đầu tư kinh doanh).

4.15 Sử dụng công ty/tổ chức bình phong

ÚC

Sử dụng trang web của các công ty lao động

353 Một đối tượng bị chú ý đã rút tiền mặt hơn 15 triệu AUD từ năm 2015 - 2018 liên quan đến bảy công ty hoạt động trong ngành công nghiệp vệ sinh, an ninh và xây dựng.

354 Hoạt động tài chính của đối tượng này có đặc trưng là khối lượng lớn các giao dịch tiền mặt vào tài khoản công ty và cá nhân và biểu hiện các chỉ số rủi ro rửa tiền sau:

- Tài khoản của nhiều ngân hàng được nắm giữ bởi một tổ chức;
- Thiếu đăng ký thuế hàng hóa và dịch vụ (GST); và
- Thiếu thông tin chi trả cho các khoản thuế cho nhân viên (PAYG).

355 Ngoài ra, đối tượng nêu trên có thể đã cố gắng làm xáo trộn các vấn đề của các công ty: với việc thiếu các hồ sơ lưu trữ minh bạch (ví dụ: hồ sơ tối thiểu được cung cấp cho người thanh lý các công ty phá sản); việc thành lập các công ty mới có tên tương tự với các công ty phá sản ngay sau khi thanh lý; điều chỉnh lùi ngày và có thể sử dụng các giám đốc giả.

356 Các hoạt động trên cho thấy đối tượng đã sử dụng các công ty này để tạo điều kiện cho việc rửa tiền, thành lập phi pháp các công ty thay thế công ty cổ tình bị thanh lý để trốn nợ tồn đọng và trốn thuế.

TRUNG QUỐC

357 Nghi phạm D thường xuyên chuyển tiền cho một số công ty và cá nhân. Trong một thời gian ngắn, số tiền liên quan đến các giao dịch một chiều đã tăng thêm hàng triệu nhân dân tệ. Tiền được chuyển ra và vào các tài khoản một cách nhanh chóng và độc lập, hầu hết các giao dịch đều ở các tỉnh và số tiền được chuyển có nhiều mối quan hệ. Giao dịch luôn xảy ra vào đầu giờ và thông qua ngân hàng trực tuyến. Địa chỉ IP tập trung vào các khu vực nguy cơ cao về ma túy. Tất cả các đối tác tài chính là các ngân hàng địa phương và hầu hết đã được đăng ký vào giữa năm 2018 và một số tổ chức đã bị thu hồi. Cơ quan có thẩm quyền nghi ngờ rằng thông qua một công ty vỏ bọc, Nghi phạm D và đồng bọn đã chuyển tiền bán ma túy thông qua các tổ chức tài chính được quản lý kém.

ĐÀI LOAN

358 Công ty A - một tập đoàn đóng tàu đã trúng thầu đóng 06 tàu trị giá khoảng 34,9 tỷ NT\$ vào tháng 10/2014 và các hợp đồng được ký vào tháng 11 năm 2014. Tuy nhiên, Công ty A đã thiếu vốn nghiêm trọng do chỉ có 530 triệu NT\$ tiền vốn và công ty đã mua các khoản đầu tư lớn ở Trung Quốc. Ông E - chủ tịch của Công ty A nhận thấy sự thiếu hụt nguồn vốn lớn của Công ty A có thể không qua mắt được các cuộc điều tra tín dụng của các ngân hàng cung cấp khoản vay. Vì vậy, ông E và các đồng phạm khác đã giả mạo các tài liệu liên quan để tăng không vốn của Công ty A từ 530 triệu NT\$ lên đến 4 tỷ NT\$. Chính ngân hàng cung cấp khoản vay đã bị mắc bẫy khi phê duyệt các hạn mức tín dụng với tổng số 20,5 tỷ NT\$ vào tháng 2/2016.

359 Để được vay bắc cầu, v.v., ông E và đồng phạm đã giả mạo chứng từ kinh doanh, bao gồm hợp đồng mua bán, hóa đơn thương mại, yêu cầu thanh toán, v.v., để giả vờ rằng Công ty A mua thiết bị cần thiết cho việc đóng tàu từ các công ty vỏ bọc nước ngoài AZ, OK, L3, HS và QY, tất cả các công ty này đều do con trai của ông E làm chủ tịch. Trong năm 2015, ông E và các đồng phạm khác đã năm lần gian lận để xin vay bắc cầu với tổng số tiền khoảng 68 triệu USD. Năm 2016, ông E và đồng bọn đã gian lận trong việc xin quay vòng vốn nhiều lần với tổng số tiền khoảng 134 triệu USD.

360 Để tránh bị điều tra, ông E đã chuyển một phần tiền trong tài khoản ngân hàng nước ngoài của các công ty vỏ bọc nước ngoài nói trên sang tài khoản cá nhân hoặc pháp nhân do ông E kiểm soát tại Đài Loan. Các khoản tiền sau đó đã được chuyển vào tài khoản của Công ty A. Số tiền còn lại trong tài khoản của các công ty vỏ bọc nước ngoài được sử dụng để đầu tư hoặc sử dụng cho các mục đích khác.

361 Vào tháng 2/2018, Văn phòng Công tố đã truy tố ông E và các đồng phạm vì vi phạm Luật Công ty, Luật Kế toán tổ chức kinh doanh, Bộ luật Hình sự và Luật Kiểm soát Rửa tiền

JAPAN

362. Một nghi phạm đã lừa đảo một tổ chức tài chính và khiến cho tổ chức tài chính đó đặt một khoản tiền dưới dạng một khoản vay tài chính vào tài khoản của một công ty giả mạo.

NEW ZEALAND (NZ)

Một công ty giả mạo của NEW ZEALAND đã bị sử dụng vào một mưu đồ rửa tiền có liên quan đến Bulgaria, UK, quần đảo Marshall và Belize

363 FIU NZ nhận được thông tin từ một FIU đối tác về một công ty đăng ký kinh doanh tại New Zealand đã gây chú ý cho cơ quan thực thi pháp luật ở nước ngoài do nghi ngờ có liên quan đến hoạt động rửa tiền xuyên nước. Công ty NZ là cổ đông duy nhất của một công ty ở Anh có tài khoản ngân hàng đã nhận những khoản chuyển tiền bị nghi là khoản thu phạm tội từ một công ty có trụ sở tại Bulgaria. Các giám đốc và cổ đông của Công ty NZ là một nhóm các công dân Nga được FIU NZ biết đến trong việc câu kết với các công ty NZ mà những công ty này đã tham gia vào các mưu đồ rửa tiền ở các nước nước ngoài, chủ yếu ở Đông Âu. Gần như chắc chắn rằng Công ty NZ là một công ty vỏ bọc, và là một phần của một loạt các cấu trúc công ty phức tạp được thiết kế để che giấu quyền sở hữu tài sản và giao dịch tài chính ở các nước nước ngoài.

Các công ty vỏ bọc NZ bị nghi ngờ hoạt động như một phần của mạng lưới buôn lậu vũ khí của Bắc Triều Tiên và Iran.

364 Báo cáo của FIU đối tác đã xác định một công ty vỏ bọc NZ tạo điều kiện cho các giao dịch ra nước ngoài thay mặt cho các bên thứ ba có trụ sở ở nước ngoài. Họ cáo buộc công ty vỏ bọc của NZ có liên quan đến một mạng lưới buôn lậu vũ khí của Triều Tiên và Iran. Các đối tác của các giao dịch là các công ty vỏ bọc khác có trụ sở tại những thiên đường thuế. Công ty NZ được thành lập bởi một nhóm nhỏ các công dân Nga ở tại New Zealand tiến hành cung cấp dịch vụ liên kết công ty và tín thác chủ yếu cho các khách hàng giàu có ở nước ngoài. Nhiều công ty NZ do các cá nhân này thành lập sau đó đã thu hút sự chú ý của các cơ quan thực thi pháp luật ở nước ngoài và nằm trong của các cuộc điều tra rửa tiền, trốn thuế xuyên nước.

PHILIPIN

365 Ủy ban A (AC) đã yêu cầu hỗ trợ trong việc lấy chứng từ là các tài khoản ngân hàng được sử dụng bởi một số cá nhân và tổ chức hiện đang phải đối mặt với thủ tục xét xử tại nước A. Yêu cầu hỗ trợ của AC được đưa ra theo Bản ghi nhớ đa phương về tư vấn và hợp tác và trao đổi thông tin (MMoU), mà Cơ quan đăng ký công ty của Philippines là một bên ký kết.

366 Theo cáo buộc, các tài khoản bị nêu tên trong yêu cầu đã được sử dụng để tạo điều kiện cho việc thực hiện các hoạt động bất hợp pháp, đặc biệt là các hoạt động kinh doanh dịch vụ tài chính mà không có giấy phép dịch vụ tài chính cần thiết, các hành vi lừa dối hoặc lừa đảo và hành vi tán tăn lương tâm.

367 Qua những cuộc điều tra của mình, AC đã phát hiện ra một mạng lưới nơi các nhà đầu tư - bao gồm cư dân địa phương - đã bị dụ dỗ đưa tiền vào sản phẩm đa cấp được mời chào. Các nhà đầu tư được chỉ thị gửi tiền vào một ngân hàng trong nước A dưới tên của AMPL. Trong vòng 48 giờ, tiền đã được chuyển, thông qua các điện chuyển tiền quốc tế, đến các nước khác nhau trên khắp thế giới. Trên thực tế, AMPL chịu trách nhiệm tạo điều kiện chuyển những khoản đầu tư này cho các tổ chức quốc tế khác nhau. Ước tính cho thấy khoảng 2,8 triệu USD đã được gửi vào tài khoản ngân hàng AMPL trong nửa đầu năm 2016 và khoảng 2,1 triệu USD đã bị phân tán trên toàn thế giới. AC hiểu rằng tiền đã được chuyển ra nước ngoài cho các thực thể và tài khoản ngân hàng được kiểm soát bởi EAS, SS, CDS và YI.

368 AMLI dường như là đối tượng nhận chuyển tiền từ AMPL. Do đó, AC hiểu rằng AMLI có thể liên quan tới, được sở hữu và vận hành bởi cùng những đối tượng như AMPL. Do đó, họ đã yêu cầu các tài liệu ngân hàng của AMLI và các cá nhân hoặc tổ chức có liên quan khác trong giai đoạn từ tháng 7/2014 đến nay.

369 Kiểm tra các tài liệu ngân hàng của ST, AMLI và DTI cho thấy họ có giao dịch với các cá nhân và tổ chức được AC nhắc đến là đã tham gia vào các hoạt động bất hợp pháp bị cáo buộc. Các giao dịch có đặc trưng chủ yếu là có những khoản chuyển tiền ra nước ngoài từ tài khoản ngân hàng trong nước.

370 Không kém phần quan trọng, có những giao dịch chuyển tiền từ nước A đến các ngân hàng trong nước từ các cá nhân có thể là nạn nhân của mạng lưới lừa đảo. Những việc này sẽ được nhắc đến chi tiết trong các phần thảo luận dưới đây. Thông tin được chia sẻ bởi AC không đề cập đến tập đoàn nước ngoài W. Tuy nhiên, các cuộc điều tra đã mang lại thông tin rằng YI đã chuyển số tiền đáng kể cho tập đoàn nói trên

371 Các điều khoản kinh doanh của AMLI cho thấy ST, một công dân của nước I, là một trong những thành viên hợp thành AMLI. AMLI, theo AC, là một trong những tổ

chức nhận được tiền từ AMPL. Hơn nữa, các tìm kiếm trên internet cho thấy ST là Giám đốc điều hành của TGL, một công ty khác được cho là đã nhận được tiền từ AMPL. Các cuộc điều tra cho thấy ST là người thụ hưởng của nhiều khoản tiền chuyển từ các công ty- một số trong đó được kiểm soát bởi chính ST - và một cá nhân, theo như tuyên bố của AC, là có gắn với AMPL.

372 ST cũng là đối tượng hưởng lợi từ các giao dịch chuyển tiền từ TGPL, một trong những công ty bị đưa ra trước Tòa án của nước A. Những khoản tiền này được phát hiện trong quá trình kiểm tra các giao dịch ngân hàng của họ với ngân hàng địa phương. IMC, một trong những công ty bị đưa ra trước Tòa án Liên bang của nước A, cũng đã chuyển tiền cho ST vào tài khoản của anh tại ngân hàng địa phương.

373 Phải nhắc lại rằng ES bị cáo buộc là một trong những người nhận tiền từ tài khoản công ty WB của AMPL, và là một trong các bị cáo mà AC đã khởi kiện. Người ta cũng đã xác định được rằng ES đã hai lần chuyển tiền cho ST vào tài khoản ngân hàng địa phương của ST.

374 ST cũng là chủ tịch của ALALI. ALALI đã được cấp Giấy chứng nhận hoạt động vào ngày 18 tháng 12 năm 2014. Trụ sở kinh doanh chính của công ty đặt tại XX, Chung cư, thành phố M. Phần vốn được ủy quyền thấp bất thường ở mức USD190, được chia thành năm cổ phiếu với mệnh giá là 38 USD mỗi cổ phiếu. Số tiền này không đủ để hỗ trợ cho mục đích hoạt động hay thực hiện công việc kinh doanh nào được thực hiện theo khả năng hoạt động của công ty loại đó.

375 Giấy chứng nhận hoạt động đã được cấp cho AMLI vào ngày 30 tháng 9 năm 2014. Địa điểm kinh doanh chính của công ty được đặt tại Chung cư XX, thành phố M. Cần nhấn mạnh rằng, đây cũng chính là địa chỉ văn phòng chính của ALALI như được nêu trong các Điều khoản hoạt động của công ty này. Phần vốn được ủy quyền, tương tự như AMLI, ở mức tối thiểu bất thường USD190, được chia thành năm cổ phiếu với mệnh giá là 38 USD mỗi cổ phiếu. Mặc dù có nguồn vốn tối thiểu được ủy quyền, AMLI vẫn duy trì nhiều tài khoản ngân hàng dưới tên của mình.

376 Cũng cần nhấn mạnh rằng, theo AC, những khách hàng từ nước A được yêu cầu gửi tiền vào một số tài khoản ngân hàng địa phương ở Philippines. Kiểm tra sao kê của tài khoản cho thấy sáu khoản chuyển tiền, tất cả đều có số lượng đáng kể, có nguồn gốc từ nước A và được ghi có vào tài khoản ngân hàng địa phương đã đề cập ở trên. Đáng chú ý, tất cả điều này đã xảy ra vào tháng 6/2015.

377 Điều tra tiếp tục cho thấy AMLI đã giao dịch với hàng loạt cá nhân và công ty được AC xác định là thực hiện kinh doanh dịch vụ tài chính không có giấy phép tại nước A và họ đã bị tổng đạt lệnh của tòa án. AMLI đã thực hiện chín lần chuyển tiền ra ngoài cho AMPL. Ngoài các hoạt động đáng ngờ đã nói ở trên, những khoản chuyển tiền quốc tế giữa AMLI và TGL cũng đã bị phát hiện trong quá trình điều tra.

378 IMC, với một địa chỉ trong nước A, là một trong những công ty mà AC có được lệnh của tòa án cấm kinh doanh dịch vụ tài chính không có giấy phép tại nước A. Một tài khoản ngân hàng địa phương khác của AMLI được phát hiện đã thực hiện chuyển tiền, trong đó IMC là đối tượng thụ hưởng.

379 US là một trong những công ty bị Tòa án liên bang của nước A cấm kinh doanh dịch vụ tài chính không phép. Kiểm tra tài khoản ngân hàng địa phương của AMLI cho thấy có những khoản tiền được chuyển cho US với mục đích trả phí hành chính.

380 Giấy chứng nhận hoạt động đã được Cơ quan đăng ký công ty Philippines cấp cho DTI vào ngày 29 tháng 7 năm 2011. Điều thú vị là ST đã xuất trình Giấy chứng nhận việc làm khi mở một tài khoản tại ngân hàng địa phương, có thông tin DTI là một trong những công ty con của IMC. Điều tra các tài khoản của DTI tại các ngân hàng địa phương cho thấy họ đã nhận được những khoản chuyển tiền quốc tế từ IMC.

381 YI là một trong những bị cáo trong vụ kiện mà ASIC đã khởi kiện trước Tòa án Liên bang nước A. Theo ASIC, số tiền được gửi vào tài khoản ngân hàng của AMPL, đã được chuyển ra nước ngoài cho các công ty và tài khoản ngân hàng do YI và những người khác kiểm soát. Các cuộc điều tra cho thấy YI đã bốn lần chuyển tiền cho một ngân hàng địa phương, số tiền trong các lần chuyển là rất lớn.

382 Sau khi kiểm tra kỹ các tài liệu ngân hàng và các giao dịch gắn với nhau của những cá nhân nói trên, sự liên kết và tham gia của họ trong mạng lưới rửa tiền rõ ràng đã được lên kế hoạch hết sức chu toàn. Các cá nhân từ nước A rõ ràng đã chuyển tiền số lượng lớn vào tài khoản ngân hàng địa phương của AMLI. Tiếp đó, các giao dịch tài khoản của AMLI lại cho thấy những khoản tiền được chuyển tới AMPL, TGL, IMC, US và ST.

383. ST là đối tượng liên kết với AMLI và ALALI, là người thụ hưởng trong hàng loạt giao dịch chuyển tiền từ AMLI, TGL, IMC và ES. IMC và YI, mặt khác, lại chuyển tiền quốc tế tương ứng cho công ty DTI và W.

384 Các cuộc điều tra tiếp theo cũng cho thấy AMLI và ALALI có những dấu hiệu của một tập đoàn giả mạo. Hai công ty có những điểm tương đồng rõ ràng đáng chú ý khi đặt cạnh nhau. Ví dụ (BẢNG)

	AM LI	ALA L
Ngày thành lập	30/9/2014	18/12/2014
Mục tiêu ban đầu	Nhằm phát triển những giải pháp phần mềm ứng dụng cho khách hàng của chúng tôi; giúp quá trình kinh doanh của họ, bao gồm cả việc tích hợp các hệ thống nhưng với điều kiện không thực hiện như một nhà cung cấp dịch vụ internet .	Nhằm phát triển những giải pháp phần mềm ứng dụng cho khách hàng của chúng tôi; giúp quá trình kinh doanh của họ, bao gồm cả việc tích hợp các hệ thống nhưng với điều kiện không thực hiện như một nhà cung cấp dịch vụ internet .
Địa điểm kinh doanh chính	XX Condominium, M City	XX Condominium, M City
Các công ty liên kết	1. ADR 2. AH 3. AP 4. ST	1. ADR 2. AH 3. AP 4. ST

	5. DWR	5. GC
Phần vốn được ủy quyền	Một trăm chín mươi USD (USD190.00), được chia làm 5 cổ phiếu có giá ba mươi tám USD (USD38.00) mỗi cổ phiếu	Một trăm chín mươi USD (USD190.00), được chia làm 5 cổ phiếu có giá ba mươi tám USD (USD38.00) mỗi cổ phiếu

385. Thực tế là các công ty này rõ ràng đang tham gia vào các cam kết có tính nghi vấn cao, điều này trở nên rõ ràng hơn khi các giao dịch tài chính của họ được kiểm tra. Mặc dù có nguồn vốn thấp bất thường nhưng các tập đoàn này đã giao dịch với số lượng đáng kể. Đáng nói nữa là hầu hết các giao dịch là giao dịch chuyển tiền quốc tế.

386. Trong khi sự thật là yêu cầu của ASIC chỉ đề cập đến các tài liệu liên quan đến các tài khoản ngân hàng địa phương, mà không ngờ tới mức độ mà các tổ chức tài chính Philippines đã bị sử dụng trong mạng lưới rửa tiền. Do đó, cần phải chia sẻ thông tin có được trong quá trình điều tra và các tài liệu liên quan ngay lập tức. Điều này phù hợp với chính sách đã tuyên bố của chúng tôi, như được ghi nhận trong Mục.2 Đạo luật Cộng hòa (R.A.) số 9160, còn được gọi là Đạo luật chống rửa tiền Đạo luật năm 2001, được sửa đổi, nhằm mở rộng hợp tác trong các cuộc điều tra xuyên nước và truy tố những người liên quan đến hoạt động rửa tiền ở bất cứ nơi nào như đã cam kết.

387. Hơn nữa, theo quan điểm về việc các pháp nhân Philippines bị khai thác trong hoạt động tội phạm, cũng nhấn mạnh sự cần thiết phải chia sẻ kết quả của cuộc điều tra hiện tại đến Cơ quan đăng ký công ty theo Thỏa thuận ghi nhớ đã ký với FIU.

4.16 Đổi tiền/ chuyển đổi tiền mặt

TRUNG QUỐC

Vụ việc điển hình 1

388. Nghi phạm E là người thực tế kiểm soát bốn tài khoản liên quan thuộc sở hữu của anh ta và ba cá nhân khác. Tiền mặt bằng đô-la Úc, đô-la Canada, đô-la Mỹ và ngoại tệ khác được gửi vào các tài khoản đó. Nghi phạm E sau đó đổi tiền sang đô la HK thông qua hoạt động ngân hàng trực tuyến và rút tiền mặt tại nhiều chi nhánh. Số tiền của mỗi lần rút ít hơn năm ngàn đô la Hồng Kông để tránh bị phát hiện. Nghi phạm E bị nghi buôn bán ngoại hối bất hợp pháp. Số tiền liên quan đến vụ án này là hàng triệu đô-la Hồng Kông. Nghi phạm E đã bị bắt vào tháng 7 năm 2018.

Vụ việc điển hình 2

389. Vào tháng 1 năm 2018, các nhà chức trách phát hiện thấy các tài khoản ngân hàng của nghi phạm F và G có liên quan đến giao dịch ngoại hối. Một số giao dịch bất thường đã được thực hiện vào giữa tháng 9/2011 và tháng 12/2017 và hàng triệu nhân dân tệ đã được chuyển bằng tiền mặt và qua ATM. Điều này không phù hợp với thông tin có sẵn cho thấy Nghi phạm F và G là những đối tượng thất nghiệp.

390. Trong một cuộc điều tra, các nhà chức trách phát hiện ra rằng một lượng tiền lớn đã được chuyển vào và ra khỏi tài khoản của nghi phạm F và G, bất kể những tổn thất về tỷ giá hối đoái. Ngoại tệ được gửi thường xuyên và sau đó rút bằng tiền mặt đô-la Hồng Kông. Số tiền gửi ít hơn năm ngàn đô-la mỗi ngày để tránh bị phát hiện. Nghi phạm F và G bị nghi ngờ là đối tượng thực hiện kinh doanh ngoại tệ bất hợp pháp. Nghi phạm F đã bị bắt vào tháng 12 năm 2018.

FIJI

Đổi tiền không khai báo

391. FIU đã nhận được một STR từ một đại lý thu đổi ngoại tệ liên quan đến đối tượng M, một công dân Fijian nhập tịch, là khách du lịch thường xuyên đến nước Z. Đối tượng M đã thực hiện ba giao dịch ngoại hối với tổng trị giá khoảng 30.000 đô-la FJ thay cho đối tượng X và đối tượng Y.

392. FIU Fiji đã tiến hành lập hồ sơ tài chính và xác định rằng 30.000\$ FJ không có nguồn gốc từ các tài khoản ngân hàng của đối tượng M, X và Y. Người ta nghi ngờ rằng các cá nhân này đã giữ tiền mặt tại nhà và rửa tiền ngoài nước này. Một báo cáo chuyển giao vụ việc đã được cung cấp cho FRCS để thu thập chứng cứ và điều tra. Hành vi phạm tội có thể xảy ra:

- Không khai báo tiền mặt mang qua biên giới (BCR).
- Rửa tiền
- Tội phạm liên quan thuế /trốn thuế

Các dấu hiệu:

- Mẫu BCR không được điền bởi cá nhân.
- Cá nhân đổi tiền dưới tên của người khác, đặc biệt là trẻ vị thành niên.

HỒNG KÔNG, TRUNG QUỐC

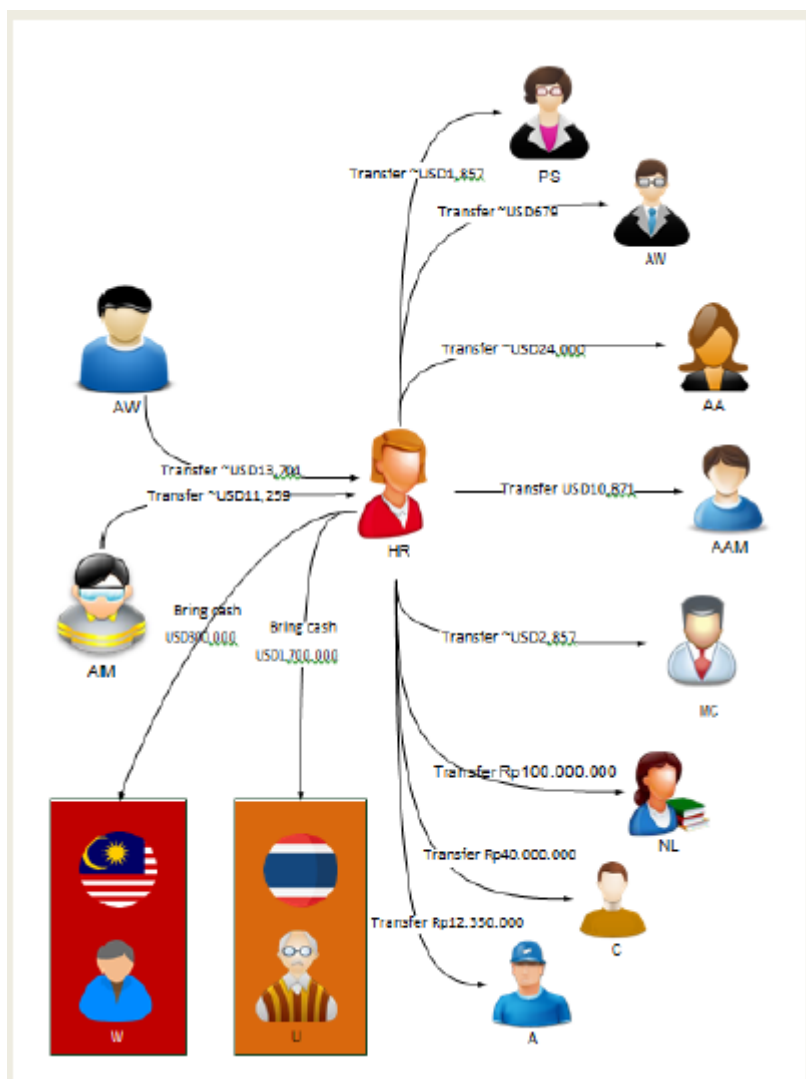
393. Một quản lý bán hàng của một công ty trong ngành kinh doanh quà tặng đã nói dối chủ của mình rằng anh ta đã nhận được 50 đơn đặt hàng từ các khách hàng ở các nước khác nhau. Người quản lý bán hàng này đã nộp phiếu tạm ứng 2,77 triệu RMB (hơn 3,4 triệu đô-la Hồng Kông) cho chủ của mình để trả vào những tài khoản được chỉ định của hai nhà cung cấp ở Trung Quốc. Tin rằng những thanh toán này là có thật, chủ nhân của anh ta đã gửi 2,77 triệu RMB vào những tài khoản được chỉ định của hai nhà cung cấp ở Trung Quốc, do hai đại diện của một nhà cung cấp dịch vụ tiền tệ được cấp phép (MSO) tại Hồng Kông, Trung Quốc. Từ ngày 23/11/2012 đến ngày 26/11/2014, đại diện của MSO đã sắp xếp việc chuyển khoản tiền tương ứng 3,1 triệu đô-la Hồng Kông và 310.000 đô-la Hồng Kông từ tài khoản ngân hàng của họ sang tài khoản ngân hàng của người quản lý bán hàng tại Hồng Kông, Trung Quốc.

394. Vào tháng 2/2018, người quản lý bán hàng đã bị kết án về hai tội giao dịch với tài sản được biết hoặc tin rằng là khoản thu từ một tội phạm có thể bị truy tố và bị kết án bốn năm tù.

INDONESIA

395. HR là vợ của KM a.k.a PR. HR, làm việc cho một dịch vụ chuyển tiền thuộc sở hữu của PR. Tài khoản HR đã được sử dụng để giữ tiền từ việc bán ma túy. HR cũng rút

tiền ra nước ngoài để đổi thành các loại tiền tệ khác. HR nhận bằng tiền mặt hoặc bằng chuyển khoản, sau đó đổi sang USD và được lấy ở Thái Lan và Malaysia. HR đã mang theo 250.000 đến 350.000 USD cho mỗi chuyến đi, tổng cộng khoảng 2.000.000 USD.



4.17 Buôn lậu tiền tệ

AFGANISTAN

Vụ việc điển hình 1

396 Túi ông X, đã được khám xét cẩn trọng với sự có mặt của các quan chức chính phủ từ các bộ phận liên quan tại một sân bay quốc tế của một nước. Cuộc khám xét cho thấy nghi phạm đã giấu hơn 1,7 triệu Rupee Ấn Độ bên trong tã trẻ em trong túi xách tay của ông này. Vì nghi phạm không thể cung cấp bất kỳ thông tin, bằng chứng nào cho số tiền mặt được phát hiện, ông ta đã bị bắt.

Vụ việc điển hình 2

397 Sau khi bị bắt vì tội buôn lậu tiền phát hiện trong túi xách tay tại một sân bay quốc tế, ông X và ông Y khai rằng họ sẽ được một số quan chức tại sân bay hỗ trợ chuyển tiền mặt ra nước ngoài. Dựa trên lời khai này của các nghi phạm, các cuộc điều tra tiếp theo đã được thực hiện và người ta phát hiện ra rằng các đối tượng đã mua chuộc các quan chức sân bay để hỗ trợ họ buôn lậu một số lượng nhất định USD và

KSA Riyals ra khỏi nước. Cuối cùng, bốn quan chức sân bay đã bị bắt cùng với các nghi phạm.

Vụ việc điển hình 3

398. Đối tượng A đến từ nước Avà đã qua kiểm tra an ninh tại sân bay, tuy nhiên những nghi ngờ đã xuất hiện ngay sau khi người này bước vào cầu dẫn ra máy bay. Theo nghi vấn của cảnh sát biên phòng, hành lý của người này đã bị lục khám, qua đó người ta phát hiện ra rằng người này đã đóng gói một số lượng lớn USD và KSA Riyals trong các vật liệu mỹ phẩm. Kiểm tra an ninh tại nhà ga, bao gồm quét tia X, không thể phát hiện ngoại tệ được đóng gói dưới dạng mỹ phẩm. Vụ việc đã được chuyển đến các cơ quan thực thi pháp luật để điều tra thêm.

Vụ việc điển hình 4

399. Cảnh sát biên giới tại một sân bay quốc tế nghi ngờ đối tượng X và Y, khi hành lý của ông X bị nghi ngờ tại một trạm kiểm tra tại quầy hàng không. Dựa trên sự nghi ngờ này, hành lý của ông X đã được khám và người ta phát hiện ra các thỏi vàng nặng hơn 11 kg được chứa trong hành lý của ông này.

400. Ông X khai nhận đã mang những thỏi vàng này vào sân bay bên trong đôi giày của mình và sau đó đặt chúng vào hành lý sau khi vượt qua các lần quét tia X. Tuy nhiên, đoạn phim CCTV dưới chân cho thấy ông X và Y vào nhà vệ sinh cùng một lúc, mỗi người mang theo một cái túi. Khi ra khỏi phòng vệ sinh, ông X được chiếu trong đoạn phim mang theo hai chiếc túi, trong khi ông Y ra khỏi phòng vệ sinh tay không. Hơn nữa, đoạn phim cũng cho thấy ông Y rời khỏi nhà ga ngay khi ông X nộp hành lý tại quầy hàng không. Trong trường hợp này, các thỏi vàng đã được ông Y mang vào sân bay, có thể do sự hỗ trợ của các quan chức sân bay.

401. Sau khi các nhà chức trách đã điều tra kỹ lưỡng vụ án, ông X đã bị phạt 4,9 triệu AFN (tương đương 72.558 USD) theo luật pháp và quy định hiện hành.

VƯƠNG QUỐC BRU-NÊ

Vụ việc điển hình 1

404 Vào tháng 2/2018, phát hiện ba người nước ngoài đi qua Sân bay Quốc tế Brunei với nhiều loại tiền tệ vượt ngưỡng khai báo mà không khai báo. Các loại tiền tệ bao gồm Ringgit Malaysia, Đồng Việt Nam, Baht Thái và Đô-la Singapore. Tiền mặt được giấu trong hành lý của họ. Hành vi này được phát hiện thông qua kiểm tra định kỳ và quét tia X bởi các nhân viên hải quan. Sau đó, người ta phát hiện ra rằng các đối tượng này có ý định vận chuyển tiền qua biên giới khu vực đất liền đến nước lân cận. Các cá nhân này đã bị truy tố và sau đó bị phạt vì phạm tội theo Mục 37 (2) của Lệnh Thu hồi Tài sản Hình sự, năm 2012 (không khai báo) với hình phạt 5.000 BND hoặc năm tháng tù cho mỗi người.

Vụ việc điển hình 2

403 Vào tháng 3/2018, một người nước ngoài bị phát hiện khi đi qua biên giới đất liền đến Brunei mang theo Đô-la Brunei và Đô-la Singapore trên ngưỡng khai báo mà không khai báo. Tiền mặt được giấu trong gói kín sau ghế hành khách phía trước của xe ô tô. Hành vi này được nhân viên hải quan phát hiện thông qua việc dừng kiểm tra ngẫu nhiên và khám xét tại một trạm kiểm soát. Cá nhân này đã bị truy tố và sau đó bị phạt vì

phạm tội theo Mục 37 (2) của Lệnh Thu hồi tài sản hình sự năm 2012 (không khai báo) với hình phạt 5.000 BND hoặc năm tháng tù giam.

NHẬT BẢN

404 Bốn nghi phạm Hàn Quốc đã nhập sáu thỏi vàng (tổng cộng 06kg, trị giá 27.500.000 yên Nhật) từ sân bay quốc tế Incheon ở Hàn Quốc đến sân bay Fukuoka ở Nhật Bản vào ngày 13/4/2017. Các nghi phạm cũng đã cố gắng đưa tiền mặt (735.220.000 JPY) ra nước ngoài mà không khai báo hoặc xin phép. Tòa án quận Fukuoka đã kết án họ hai năm sáu tháng tù giam, đình chỉ nhập khẩu bốn năm.

NEW ZEALAND

Những người đàn ông Trung Quốc đã toan tính chuyển lậu khoảng \$65.000 tiền mặt từ một nước Nam Thái Bình Dương đến New Zealand.

405 Hai người đàn ông Trung Quốc đã bị chặn tại một sân bay quốc tế tại một hòn đảo Nam Thái Bình Dương khi đang cố chuyển lậu khoảng 65.000 đô la tiền mặt vào New Zealand. Số tiền bao gồm khoảng 50.000 USD và 15.000 NZD và được giấu trên người của họ. Hai cá nhân thường xuyên đi lại giữa New Zealand và Trung Quốc, và một trong số họ thường xuyên lui tới sòng bạc ở New Zealand, nơi anh ta đã mất nhiều hơn 20.000 kể từ năm 2015. Người ta nghi ngờ rằng những cá nhân này đã cố gắng hồi hương số tiền thu được từ việc nhập ma túy trở lại New Zealand và Trung Quốc

PAKISTAN

406 Theo thông tin nhận được, một băng đảng có tổ chức liên quan đến buôn lậu ngoại tệ cố chuyển lậu ngoại tệ từ sân bay quốc tế Islamabad trên một chuyến bay quốc tế. Một chiến dịch đã được thực hiện dẫn đến việc thu hồi các loại ngoại tệ khác nhau với tổng trị giá 38,69 triệu PKR (tương đương khoảng 276.168 USD). Hai người bị buộc tội là ông AK và ông GD cũng bị bắt tại chỗ. Một trong những người bị buộc tội là ông AK đã lên máy bay cùng số ngoại tệ, sẵn sàng cất cánh, tại thời điểm bị bắt giữ.

SINGAPORE

Một người buôn lậu tiền – vận chuyển tiền mặt đã bị cầm tù 36 tháng vì buôn lậu hàng triệu đô vào Singapore

407 Người A làm công việc chuyển tiền cho một tổ chức đổi tiền ở nước láng giềng. Từ năm 2013 đến 2014, trong 100 lần, anh này đã mang vào Singapore số tiền tệ vật chất ước tính 12 triệu đô-la Singapore mà không cung cấp các báo cáo vận chuyển động tiền mặt xuyên biên giới một cách đầy đủ và chính xác. Đối tượng A cố tình cung cấp các lời khai sai lệch rằng anh ta không biết về các nguồn cung cấp và người nhận thực tế của số tiền mặt đó. Đây là lượng tiền mặt lớn nhất được mang vào Singapore bất hợp pháp.

408 Vào tháng 2/2018, đối tượng A đã bị xử và bị kết án 36 tháng tù.

THÁI LAN

409 Năm 2019, một người quốc tịch Lào mang theo tiền Thái Lan qua biên giới mà không khai báo. Hành động này là vi phạm luật hải quan với mục đích rửa tiền, và là tội phạm nguồn. Tài sản ước tính khoảng 100 triệu baht (3.300.000 USD) đã bị truy tìm, niêm phong và phong tỏa.

4.18 Sử dụng thẻ tín dụng, séc, kỳ phiếu, v.v.

FIJI

Rửa séc

410 FIU đã nhận được một STR từ một ngân hàng địa phương liên quan đến một hoạt động nghi toan lừa đảo tình vi đối với một tổ chức niêm yết công khai- công ty E. FIU đã phát hiện cá nhân F đã đổi/ rửa 14 tờ séc do Công ty E phát hành để trả cho cá nhân F.

411 Quá trình xác minh của ngân hàng địa phương xác định rằng những người được trả tiền trên séc đã bị thay đổi và đến rút tiền mặt.

412 FIU tiếp tục xác lập rằng cá nhân F có liên quan đến một trong những quan chức cấp cao của Công ty E.

413 Một báo cáo chuyên giao vụ việc đã được cung cấp cho FPF, Đơn vị điều tra tội phạm mạng để điều tra. Vụ việc hiện đang được đưa ra trước Tòa án sơ thẩm Suva.

Hành vi phạm tội có thể xảy ra:

- Có được lợi thế tài chính thông qua lừa đảo.
- Lừa đảo.

Các dấu hiệu:

- Dấu vết hoặc đổi màu trên séc có thể do tẩy xóa hoặc thay đổi

NHẬT BẢN

Vụ việc điển hình 1

414 Một người buôn bán đồ cũ, cũng là người quản lý các khoản vay bất hợp pháp, đã lên kế hoạch kiếm lợi nhuận bất hợp pháp bằng cách lừa một công ty thẻ tín dụng, bằng cách sử dụng thẻ tín dụng khách hàng của mình. Người này cung cấp cho công ty thẻ tín dụng dữ liệu bán hàng giả, chi tiết doanh số được thanh toán bằng thẻ tín dụng mà thực tế không có. Công ty thẻ tín dụng sau đó gửi tiền vào một tài khoản được mở dưới tên của người khác nhưng thực tế được kiểm soát bởi chính cá nhân này.

Vụ việc điển hình 2

415 Một người liên quan đến Boryokudan (nhóm tội phạm có tổ chức của Nhật Bản) đã nhận được thẻ tín dụng mà người quen của anh ta đã kiếm được bất hợp pháp và miễn phí. Anh ta dùng thẻ để rút tiền mặt và trả tiền chi phí sinh hoạt và chi phí giải trí.\

MA-CAO, TRUNG QUỐC

416 Một doanh nghiệp chấp nhận thanh toán thẻ ngân hàng nhận thấy rằng khách hàng A đã sử dụng 11 thẻ được phát hành bên ngoài Macao, Trung Quốc để thực hiện một số lượng lớn giao dịch tại ba cửa hàng trang sức kể từ tháng 1/2018. Tổng cộng hơn 1,8 triệu MOP đã được giao dịch trong ba tháng. Điều này đã làm ngân hàng nghi ngờ rằng Khách hàng A đã rút tiền từ thẻ để mua các vật có giá trị trong các cửa hàng trang sức này.

417 Ngay sau khi các giao dịch trên được thực hiện, thông tin tình báo đã cho thấy khách hàng A tham gia lừa đảo và đã bị Cảnh sát Tư pháp bắt giữ. Sau một cuộc điều tra chuyên sâu, khách hàng A đã bị nghi là thông đồng với nhân viên của các cửa hàng trang sức để thực hiện các giao dịch thẻ nói trên và rửa những khoản thu bất hợp pháp

từ mạng lưới tại các nước khác nhau. Một số tiền bất hợp pháp đã được chuyển đến Macao, Trung Quốc thông qua các giao dịch thẻ ghi nợ để che giấu nguồn tiền. Vụ việc cũng đã được trình lên Văn phòng Công tố để điều tra thêm.

4.19 Cơ cấu (lẩn giấu)

ÚC

Buôn lậu tiền mặt xuyên biên giới

418 Đơn vị tội phạm tài chính liên quan đến biên giới Úc (BRFCU) thuộc Lực lượng biên giới Úc (ABF) đã nghiên cứu các khía cạnh của hành vi cơ cấu trong các mô hình rửa tiền khác nhau. Đặc biệt, việc xác định hoạt động buôn lậu tiền mặt số lượng lớn như một rủi ro đáng kể ở khu vực biên giới đối với các khách du lịch/ phi hành đoàn hàng không.

419 Phi hành đoàn quá cảnh qua các sân bay trên đất liền đã được sử dụng để mang theo số lượng tiền tệ ngay dưới ngưỡng báo cáo 10.000 AUD. Hoạt động này được điều phối bởi một người kiểm soát, người này sẽ sử dụng mạng lưới của mình để cung cấp tiền trước khi khởi hành và sẽ thu lại số tiền khi đến nơi.

420 Mô hình này đã được theo dõi và liên kết với các chuyến bay đến thủ đô từ các thị trường được coi là nhiều biến động hơn so với nơi đến cũng như những nơi tài trợ cho hoạt động cung ứng ma túy.

TRUNG QUỐC

Vụ việc điển hình 1

421 Lừa đảo viễn thông do một băng đảng ở nước ngoài dẫn đầu dẫn đến tổn thất hàng triệu nhân dân tệ. Với sự hỗ trợ của FIU, cảnh sát đã tiến hành điều tra và thu thập bằng chứng từ hơn 20 thành phố. Một số nghi phạm, bao gồm cả người nước ngoài đã bị bắt và các loại thẻ ngân hàng liên quan đã bị đóng băng. Các băng đảng nước ngoài đã rửa tiền bất hợp pháp thông qua các chân rết (cơ cấu). Chỉ trong vài ngày, tiền từ hai tài khoản ngân hàng đã được chuyển đến hàng loạt tài khoản cấp một, hàng trăm tài khoản cấp hai, cấp năm và hàng ngàn tài khoản cấp ba, cấp bốn thông qua hoạt động ngân hàng trực tuyến. Tất cả số tiền đã được chuyển và rút ra ở nước ngoài.

Vụ việc điển hình 2

422 A và B sống như một cặp vợ chồng. A cố ý giúp B chuyển tiền thu được bất hợp pháp theo các cách sau:

- ☐ Sử dụng tài khoản cá nhân. A đã mở hai tài khoản ngân hàng để chuyển tiền bất hợp pháp và cả hai tài khoản luôn có số dư thấp.
- ☐ Mua tài sản và phương tiện giao thông.
- ☐ Rửa tiền thông qua sử dụng tiền mặt.
- ☐ ML thông qua đầu tư.

423 Vào tháng 9/2018, tòa án đã kết án A về tội rửa tiền và kết án A mười tháng tù giam cùng với 1 mức xử phạt kèm theo.

MALAYSIA

424 Vụ việc này liên quan đến một PEP (Nghị phạm B) cũng là một quan chức chính phủ cấp cao đã lạm dụng chức vụ của mình với tư cách là Chủ tịch của NPO, cụ thể là Quỹ ABC. Thẻ tín dụng của vợ nghị phạm B được sử dụng tiêu dùng cho các mặt hàng xa xỉ đã được ABC Foundation thanh toán. Các khoản thanh toán của NPO cho những chi tiêu cá nhân chỉ ra rằng chủ thể đã phạm tội vi phạm hình sự vi phạm tín thác.

425 ABC Foundation duy trì một tài khoản thanh toán tại một ngân hàng địa phương, với nghị phạm B là người ký duy nhất.

426 Tài khoản đã bị phát hiện nhận tiền gửi vào bằng tiền mặt thường xuyên từ nhiều địa điểm khác nhau dưới giá trị phải báo cáo giao dịch tiền mặt, có thể để tránh những biện pháp theo dõi, cập nhật thông tin khách hàng (CDD) và những yêu cầu báo cáo. Ngoài ra, nhiều tờ séc có giá trị lớn cũng được nộp vào tài khoản từ các tổ chức khác nhau mà không có lý do hợp lý cũng bị theo dõi. Số tiền séc dao động trong khoảng từ 16.000 đến 1.000.000 RM.

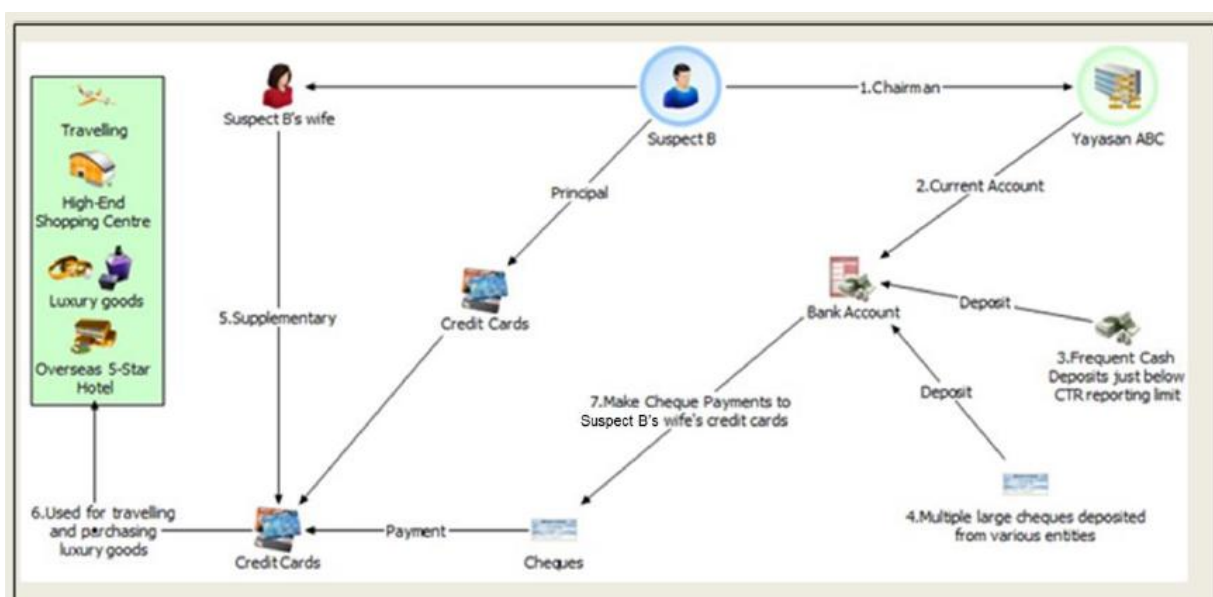
427 Đồng thời, vợ của nghị phạm B cũng giữ số tiền bổ sung của nhiều thẻ tín dụng dưới tổng hạn mức được cấp cho chủ thẻ chính. Những thẻ này đã được sử dụng một cách tích cực để đi du lịch, mua hàng hóa xa xỉ và ở tại các khách sạn xa xỉ ở nước ngoài.

428 Thẻ được thanh toán qua séc của bên thứ ba do ABC Foundation phát hành. Nhiều khoản thanh toán séc lớn đã được thực hiện và người ký séc là nghị phạm B cũng là Chủ tịch của ABC Foundation.

429 Nghị phạm B đã bị buộc tội vì nhiều tội phạm hình sự vi phạm tín thác, rửa tiền và lạm quyền. Vụ án hiện vẫn đang tiếp tục diễn ra.

Các phương thức rửa tiền được sử dụng bao gồm:

- ☐ Mua tài sản có giá trị;
- ☐ Sử dụng tài khoản ngân hàng / thẻ tín dụng / séc;
- ☐ Sử dụng tiền mặt; và
- ☐ Có sự tham gia của NPO.



New Zealand

Mạng lưới nhập khẩu ma túy sử dụng tài khoản ngân hàng được cơ cấu/phân tán và tài khoản ngân hàng của bên thứ 3

430. Mạng lưới nhập khẩu ma túy tham gia vào việc cơ cấu và sử dụng tài khoản của bên thứ 3 để tạo quỹ cho hoạt động nhập khẩu này. Các bên thứ 3 nộp 27,5 nghìn đô-la tiền mặt vào tài khoản cá nhân trong thời gian 2 tuần – mỗi lần nộp từ 9-9,5 nghìn đô-la. Những khoản ghi có này được nộp từ nhiều nơi ở khu vực Auckland. Những khoản tiền này sau đó được chuyển vào tài khoản của một bên thứ 3 khác, rồi lại hợp vào với những khoản tiền được chuyển bằng điện tử vào với giá trị khoảng 60 nghìn đô-la từ các tài khoản khác nhau của các bên thứ ba khác, trước khi chuyển đi cho tài khoản của 1 bên thứ ba khác nữa với hình thức thanh toán nợ vay.

4.20 Chuyển tiền điện tử/ sử dụng các tài khoản ngân hàng ở nước ngoài

FIJI

Công ty luật, nạn nhân của mạng lưới lừa đảo qua thư thương mại điện tử

431. FIU nhận được một STR liên quan đến tài khoản được giữ tại ngân hàng Z trong nước A. Tài khoản này được sử dụng để chiếm hữu một cách lừa đảo các quỹ của một công ty luật trong nước.

432. Công ty luật này được thuê để thay mặt 4 cá nhân bán tài sản. Địa chỉ email của 1 trong 4 người này là V bị xâm nhập và đã có 1 thư điện tử lừa đảo được gửi cho công ty luật thông báo rằng tiền cần phải được gửi vào tài khoản mở tại ngân hàng Z. Tháng 10/2018, công ty luật trong nước đã thực hiện 2 giao dịch chuyển khoảng 845 nghìn đô-la Fiji đến tài khoản tại ngân hàng Z.

433. Công ty luật này không biết rằng mình là nạn nhân của “mạng lưới lừa đảo qua thư thương mại điện tử” cho tới khi ông V kiểm tra khoản thanh toán. Ngân hàng chuyển tiền tại Fiji đã cố gắng thu hồi lại số tiền này nhưng không được.

434. Người ta tin rằng người đứng tên tài khoản tại ngân hàng Z tại nước X có thể bị liên quan đến tội phạm máy tính và là một bên trong mạng lưới lừa đảo qua thư thương mại điện tử.

435. FIU đã liên hệ với các đối tác nước ngoài để thu hồi tài sản. Vụ việc này đang được điều tra.

Tội phạm có thể:

- Xâm nhập địa chỉ thư thương mại điện tử/ tài khoản thư điện tử

Các dấu hiệu:

- Bỗng dưng thay đổi thông tin tài khoản đối với khoản chuyển tiền thanh toán.
- Sử dụng đầy đủ họ tên thay vì biệt danh và cách thức sử dụng ngôn ngữ không giống như người gửi thường dùng.

PAKISTAN

436. Một báo cáo STR liên quan đến nghi phạm XYZ của công ty ngoại hối ABC dựa trên thông tin đại chúng về việc nghi phạm này có thể bị cáo buộc liên quan đến việc lạm dụng trẻ em thông qua việc làm và bán băng qua mạng. Nghi phạm XYZ đã bị Cục

điều tra liên bang bắt giữ. Cảnh sát tư pháp nước ngoài đã bắt giữ một người đàn ông bị cáo buộc liên quan đến các hoạt động lạm dụng trẻ em. Trong quá trình điều tra, kẻ bị cáo buộc đã tiết lộ rằng công dân Pakistan, nghi phạm XYZ cũng có liên quan đến hoạt động bất hợp pháp. Thông tin này đã được đại sứ quán nước ngoài chia sẻ với cơ quan có thẩm quyền của Pakistan và trên cơ sở đó, nghi phạm XYZ đã bị cơ quan thực thi pháp luật (LEA) bắt giữ.

437. Nghi phạm XYZ đã nhận những khoản chuyển tiền nhỏ từ các cá nhân khác nhau ở 6 vùng, lãnh thổ. Người ta nghi ngờ rằng nghi phạm XYZ đã nhận những khoản tiền bất hợp pháp từ việc bán những băng hình. Kẻ bị cáo buộc cũng thừa nhận rằng hẳn ta nhận những khoản tiền nhỏ từ việc bán 1 băng video.

438. FMU đã chia sẻ thông tin tình báo tài chính với LEA. Nghi phạm đã bị buộc tội và kết án 7 năm tù giam và nộp phạt 1,2 triệu Rs bởi tòa án chuyên về tội phạm mạng.

4.21. Trao đổi hàng hóa (trao đổi – ví dụ: tái đầu tư vào thuốc phiện bất hợp pháp)

New Zealand

Một mạng lưới trao đổi hàng hóa rửa tiền trên cơ sở thương mại (TBML) bị nghi ngờ liên quan đến việc xuất khẩu các bộ phận xe như là khoản thanh toán cho việc nhập khẩu chất kích thích (methamphetamine)

439. Một nhà xuất khẩu các bộ phận xe có trụ sở tại New Zealand đã bị NZPFIU đề mắt đến với nghi ngờ liên quan đến mạng lưới trao đổi hàng hóa rửa tiền trên cơ sở thương mại do tham gia vào việc chở bằng tàu biển những bộ phận xe bị đánh cắp ở nước ngoài như là khoản thanh toán cho việc nhập khẩu chất kích thích methamphetamine từ Tây Phi. Cá nhân này có liên quan đến một tổ chức nhập khẩu ma túy quốc tế rộng khắp New Zealand, Australia và Tây Phi và bị nghi ngờ sử dụng việc kinh doanh vận tải có cơ sở ở New Zealand vào việc tạo điều kiện thanh toán (dưới hình thức các bộ phận xe cũng như chuyển tiền mặt thực tế bằng điện tín) đến Tây Phi để đổi lấy việc chuyển methamphetamine vào New Zealand qua đường bưu phẩm.

4.22 Sử dụng nhận dạng, tài liệu giả mạo

AFGHANISTAN

Vụ việc điển hình 1

440. Đối tượng MSP đã sử dụng giấy tờ nhận dạng giả để có được giấy phép nhằm tránh việc nhận dạng và bỏ qua trách nhiệm trong tương lai. Khi xem xét việc không thực hiện trách nhiệm của MSP, cơ quan nhà nước có thẩm quyền không thể thu thập được thông tin nhận dạng chính xác của nghi phạm.

441. Kết quả là FIU đã thu hồi giấy phép và thông báo cho cơ quan cấp phép để kiểm tra xác thực chứng từ nhận dạng trước khi cấp phép.

Vụ việc điển hình 2

442. Việc kiểm tra hồ sơ đấu thầu của công ty kỹ thuật X tại Cục mua sắm nước cho thấy rằng sao kê ngân hàng của công ty này là giả mạo. Việc kiểm tra chỉ ra rằng số dư cuối kỳ hiện tại của công ty hiện là 155.486 AFN. Tuy nhiên, công ty này đã làm giả một sao kê có số dư cuối kỳ là 2 triệu AFN. Điều này đã làm cho công ty đủ điều kiện để tham dự đấu thầu. Kết quả là công ty này bị đưa vào danh sách đen không được tham gia đấu thầu của Cục mua sắm nước.

NHẬT BẢN

443. Một thành viên cao cấp của Boryokudan đã có được điện thoại di động một cách bất hợp pháp từ một nhà cung cấp điện thoại di động và bán chúng bằng cách sử dụng giấy tờ tùy thân của người khác. Sau đó ông ta chuyển số tiền bất hợp pháp này vào các tài khoản ngân hàng được mở dưới tên những người khác và do ông ta kiểm soát. Ông ta đã bị bắt do vi phạm Luật trừng phạt tội phạm có tổ chức (che dấu tài sản phạm pháp).

4.23 Kim loại quý, đá quý

ÚC

Rửa tiền trên cơ sở thương mại – thị trường kim loại quý

444. Do tính ẩn danh và giá trị nội tại của nó, thị trường kim loại quý đã được xác định như một sự thay thế hấp dẫn cho thị trường tài chính đối với hoạt động rửa tiền. Đơn vị tội phạm tài chính liên quan đến biên giới ABF (BRFCU) vừa làm việc với Cơ quan điều tra an ninh nội địa Mỹ (US HIS) để tham gia vào một sáng kiến chung về minh bạch thương mại bằng cách sử dụng phần mềm phân tích “phân tích dữ liệu để nghiên cứu và hệ thống minh bạch thương mại” (DARTTS).

445. Việc này cho phép phân tích thông tin xuất nhập khẩu để xác định sự khác biệt về dữ liệu thương mại. Kết quả này xác định các công ty của Úc bị nghi sử dụng phương pháp rửa tiền trên cơ sở thương mại (TBML) bằng cách sử dụng vàng thỏi và hóa đơn giả như một phương tiện để dịch chuyển các khoản tiền bất hợp pháp ở nước ngoài dưới chiêu bài kinh doanh bán buôn vàng thỏi. Nỗ lực điều tra bao gồm cả việc kiểm tra hàng hóa và độ tinh khiết đang được tiến hành.

446. ABF BRFCU đã thực hiện một dự án khám phá những rủi ro từ vàng và sản phẩm từ vàng. Ở đây người ta quan sát thấy buôn bán kim loại quý, đá quý ngày càng được chấp nhận bởi những đối tượng tìm cách che dấu việc chuyển giao giá trị.

447. Đặc biệt dự án này cho thấy, kim loại quý và kim cương được sử dụng hàng ngày để chuyển những khoản thu phạm tội và để tạo vỏ bọc, che dấu nguồn gốc thực, địa điểm và mục đích của các giao dịch tài chính. Hoạt động ngăn chặn tại biên giới nhằm vào việc xác định việc buôn bán vàng bất hợp pháp hoặc không khai báo đã cho thấy số lượng lớn giao dịch xuất nhập khẩu mặt hàng này và việc rò rỉ đáng kể doanh thu do sử dụng hóa đơn giả, buôn lậu và hoạt động thương mại bất hợp pháp khác.

TRUNG QUỐC

Vụ việc điển hình 1

448. Hải quan và cảnh sát thành phố N đã lập một nhóm và điều tra 14 trường hợp buôn lậu kim loại quý. Nhóm này đã phá được 5 băng nhóm tội phạm. Các thành viên của các nhóm này tiếp tục buôn lậu vàng bằng cách giấu trong người. Nhiều kg vàng bị thu giữ và 22 nghi phạm bị bắt. Vụ việc đang được tiếp tục điều tra.

Vụ việc điển hình 2

449. Tháng 11/2018, hải quan và chi nhánh tại thành phố M đã điều tra vụ buôn lậu kim loại quý. Băng nhóm tội phạm đã buôn lậu hàng trăm kg kim loại quý bằng cách giấu vàng vào trong người hơn 40 lần. 5 nghi phạm đã bị bắt và vụ việc đang được tiếp tục điều tra.

Vụ việc điển hình 3

450. Tháng 7/2018, hải quan thành phố L đã tìm thấy hàng tá thỏi vàng ở trong hộp dụng cụ của 1 xe cá nhân. Nghi phạm đã bị bắt và vụ việc đang được tiếp tục điều tra.

New Zealand

Kẻ lừa đảo sáng tạo mua bán vàng/ kim loại quý

451. Kẻ lừa đảo đã sử dụng những tờ séc trộm cắp để thực hiện việc mua hàng hóa có giá trị cao ở New Zealand, bao gồm cả mua hơn 100 nghìn đô-la vàng và trang sức. Hắn ta đã đưa những tờ séc này vào các tài khoản ngân hàng của người bán lẻ và đặt hàng trước khi ngân hàng xác định được những tờ séc này không có hiệu lực. Hắn sử dụng cách thức này để mua hơn 100 nghìn đô la vàng và trang sức. Số hàng này được chuyển đến địa chỉ của hắn và đồng bọn. Khi khám nhà, cảnh sát đã không thể tìm thấy vàng/trang sức – điều này dẫn đến việc nghi ngờ hắn ta đã chuyển số vàng/trang sức này cho các nhóm tội phạm ở địa phương như việc thanh toán khoản nợ mua ma túy.

4.24 Mua tài sản có giá trị (sản phẩm nghệ thuật, đồ cổ, ngựa đua...)

Úc

Mua tác phẩm nghệ thuật bởi các tổ chức tội phạm

452. ABF BRFCU xác định một số trường hợp mua hàng hóa có giá trị để dễ dàng chuyển bất hợp pháp.

453. Năm 2018, ABF xác định một người mang quốc tịch Úc có quan hệ mật thiết với tổ chức tội phạm trong nước đi du lịch để thu xếp việc mua một tác phẩm của một nghệ sĩ rất nổi tiếng.

454. Trong quá trình điều tra, đối tượng bị theo dõi sở hữu nhiều tài liệu, bao gồm cả thỏa thuận mua bán và giấy đòi vật có giá trị. Có thể là việc mua bán hàng hóa có giá trị lớn đã được sử dụng như một cơ chế để hợp pháp hóa những dòng tiền có giá trị lớn này. Cũng có thể những giấy tờ đó được làm ra cho mục đích này.

TRUNG QUỐC

Vụ việc điển hình 1

455. Nghi phạm A là nhân viên của một công ty vận tải đa phương tiện. Tài khoản của anh ta thường xuyên nhận được tiền mặt từ vùng có rủi ro cao. Sau đó số tiền này được chuyển đến nhiều tài khoản cá nhân. Nghi phạm A cũng mua xe hơi rẻ tiền đã qua sử dụng ở nhiều thành phố. Nghi phạm A bị nghi ngờ tài trợ khủng bố và các giao dịch bất thường không thể giải thích được theo nghề nghiệp của anh ta. Giá trị các khoản tiền liên quan đến vụ việc này lên tới hàng triệu nhân dân tệ. Thông tin này đã được báo cáo lên cơ quan nhà nước có thẩm quyền.

Vụ việc điển hình 2

456. Nghi phạm B sản xuất và bán ma túy nhiều lần trong suốt năm 2010-2011 và nguồn gốc thu nhập không rõ ràng. Bà chủ của anh ta, nghi phạm C và bố mẹ bà ta, có rất nhiều tiền ra vào tài khoản. Cảnh sát đã lập hồ sơ về nghi phạm C và bố mẹ bà ta nghi ngờ rửa tiền. Theo chứng cứ có được, tòa án đã khẳng định nghi phạm C không có thu nhập và số tiền dùng để mua các sản phẩm tài chính, nhà và xe cũng như tiền mặt là

từ tiền bán ma túy của nghi phạm B. Tháng 9/2018, nghi phạm C bị kết tội rửa tiền và phạt 5 năm tù giam cùng với khoản tiền phạt.

FII

457. Ông Z, một thương nhân ở Fiji đã làm ăn với ông Y, một nhà đầu tư nước ngoài. Như một phần của thương vụ, ông Z được ông Y đề nghị tìm một bất động sản để có thể đầu tư ví dụ như một siêu thị. Ông Z giới thiệu bất động sản B và gửi một thỏa thuận mua bán trị giá 5,5 triệu đô-la FJ (2,75 triệu đô-la Mỹ). Ông Y đã chuyển xấp xỉ 5,3 triệu đô-la FJ (2,7 triệu đô-la Mỹ) vào hai tài khoản ngân hàng khác nhau để mua. Sau đó, ông Y bắt đầu nghi ngờ ông Z nên đã yêu cầu vợ mình là bà X đến Fiji để điều tra việc mua bán này. Bà X phát hiện ra rằng thỏa thuận mua bán gốc chỉ có 3,3 triệu đô-la FJ (1,6 triệu đô-la Mỹ). Khi ông Y chất vấn ông Z về sự chênh lệch này thì ông Z giải thích rằng bất động sản đó được bán 5,5 triệu đô-la FJ nhưng giấy tờ mua bán ghi là 3,3 triệu đô-la FJ nhằm trốn thuế.

458. Điều đó cho thấy ông Z đã thổi phồng giá trị của bất động sản B nhằm chiếm đoạt 1,2 triệu đô-la FJ của ông Y. Sau đó số tiền này được sử dụng như là một phần thanh toán cho 2 chiếc xe, 2 căn và lập một khoản tiền gửi có kỳ hạn. Ông Z đã bị bắt và chờ xét xử. Tài sản cũng bị niêm phong.

4.25 Đầu tư vào thị trường vốn, sử dụng môi giới

Australia

Chuyển giao chứng khoán ngoài thị trường trên các thị trường giao dịch nhỏ

459. Chuyển nhượng ngoài thị trường (OMT) là việc chuyển quyền sở hữu chứng khoán (bao gồm cả quyền lợi trong các phương án đầu tư) song phương giữa các bên ở ngoài thị trường trao đổi.

460. Năm 2018, Ủy ban Chứng khoán và Đầu tư Úc (ASIC) đã bắt đầu giám sát các rủi ro về rửa tiền/ tài trợ khủng bố liên quan đến OMT trên các thị trường nhỏ.

461. Thông qua công việc này, ASIC xác định rằng Công ty A ở Úc có hoạt động giao dịch không cân xứng với các chứng khoán khác trên sàn giao dịch.

462. Công ty A hoạt động trong lĩnh vực bán lẻ với hàng loạt thị trường nước ngoài và cổ đông nắm quyền kiểm soát của công ty này đã chuyển hơn 1 triệu AUD cho một sòng bạc Úc.

463. ASIC lưu ý rằng các sàn giao dịch nhỏ có thể bị lợi dụng rửa tiền thông qua OMT, mà nó được coi là phương tiện hấp dẫn tiềm năng để chuyển tài sản cho các doanh nghiệp tội phạm. Các yếu tố rủi ro bao gồm cả việc họ có thể hoạt động ngoài ngành ngân hàng Úc và bị ảnh hưởng chủ yếu bởi những danh mục cổ phiếu không được quản lý mà không có yêu cầu buộc phải báo cáo bất đối với việc chuyển nhượng quyền sở hữu ngoài thị trường hoặc nghĩa vụ theo dõi cập nhật thông tin.

NHẬT BẢN

464. Một nghi phạm đã gửi tài sản bất hợp pháp có được từ việc lừa đảo trong tài khoản chứng khoán được mở dưới tên giả và chuyển tiền mua cổ phiếu.

4.26 Các trường hợp được phát hiện trực tiếp từ các báo cáo giao dịch đáng ngờ hoặc giao dịch vượt ngưỡng

AFGANISTAN

465. Dựa trên các STR mà FIU nhận được từ các đối tượng báo cáo, sự nghi ngờ đã xuất hiện dựa trên hoạt động của một số công ty thương mại. Các STR này được ưu tiên dựa trên phân loại ma trận rủi ro. Các STR về Công ty thương mại A và Công ty thương mại B được áp dụng phân tích tài chính.

466. FIU bắt đầu phân tích tài chính đối với các công ty này và chuyển dữ liệu thông tin tình báo tài chính cho LEA.

467. Trong năm 2018, FinTRACA đã chuyển giao (47) trường hợp chủ động và phản ứng cho các cơ quan thực thi pháp luật trong nước để điều tra hoặc tiếp tục hành động.

Úc

468. Chiến dịch Astatine tập trung vào một tập đoàn tội phạm có trụ sở tại New south wales (NSW) liên quan đến buôn bán ma túy và buôn lậu thuốc lá. Tổ chức này đã tham gia nhập khẩu 50 triệu liều thuốc lá và âm mưu nhập 200 kg methylenedioxymethamphetamine (MDMA) qua đường biển.

469. Ủy ban thống nhất thực thi pháp luật của Úc và Nhóm điều tra chung tội phạm có tổ chức chung (JOCG) của NSW đã tiến hành một cuộc điều tra song song đối với một nhân viên của Bộ Di trú và Bảo vệ Biên giới (nay là Bộ Nội vụ), người bị buộc tội lạm dụng chức vụ của mình để hỗ trợ tổ chức này.

470. Vào tháng 8/2017, JOCG tại NSW đã thực hiện 13 lệnh khám xét các đối tượng liên quan tới tổ chức này trên toàn NSW. Khoảng 80 kg cocaine và tổng cộng 740.000 AUD tiền mặt đã bị thu giữ trong bốn nhà. Trong quá trình điều tra, JOCG đã thu giữ thêm 2 triệu AUD. JOCG đã bắt giữ chín người trong đó có tám người ở Sydney. Người được cho là lãnh đạo tổ chức đã bị bắt tại Dubai và bị dẫn độ về NSW liên quan đến cáo buộc nhập khẩu ma túy.

471. AUSTRAC đã hỗ trợ thông tin tình báo tại chỗ trong suốt quá trình điều tra. Thông tin tình báo tài chính đã xác định được các liên kết chính giữa các đối tượng trong nước và nước ngoài chưa biết trước đây và phát hiện các khoản tiền mặt được nhiều thành viên tổ chức này thường xuyên gửi vào có giá trị rất lớn.

Trung Quốc

Vụ việc điển hình 1

472. Các tổ chức tài chính nhận thấy rằng hơn 100 khách hàng đã mở tài khoản trong một khoảng thời gian ngắn. Mỗi tài khoản đã mua khoảng 50 nghìn đô-la Mỹ thông qua ngân hàng trực tuyến và chuyển số tiền đó sang tài khoản cá nhân ở những nơi khác. Tổng số tiền đã đạt tới hàng triệu đô-la. Người kiểm soát những tài khoản này bị nghi ngờ hoạt động ngân hàng ngầm bất hợp pháp.

473. Bắt đầu từ các STR, cơ quan chức năng đã phân tích hơn một triệu giao dịch lớn và mười tầng lớp những bên liên quan. Cơ quan chức năng đã phân loại các phương thức giao dịch, đặc điểm nhận dạng và các loại tội phạm và phát hiện hàng trăm bên liên quan.

474. Tháng 7/2018, các cơ quan thực thi pháp luật đã bắt giữ thành công 26 nghi phạm liên quan đến vụ án này, triệt phá sáu băng đảng ngân hàng ngầm lớn, 21 tụ điểm và thu giữ các công cụ gây án như máy tính và thẻ ngân hàng bị đóng băng.

Vụ việc điển hình 2

475. Tháng 10/2018, các tổ chức tài chính đã báo cáo với cơ quan có thẩm quyền rằng người đại diện hợp pháp của Công ty A đã xin chuyển nhượng 80 triệu nhân dân tệ. Cơ quan chức năng ngay lập tức đã cung cấp thông tin liên quan cho cảnh sát. Sau khi điều tra, cơ quan có thẩm quyền phát hiện ra các giao dịch của Công ty A có các đặc điểm sau:

- a) Công ty A có các kênh đầu tư và có kênh gây quỹ riêng.
- b) Giám đốc tài chính của Công ty A cũng là đại diện theo pháp luật của bốn công ty liên quan. Anh ta có 27 tài khoản ngân hàng chung và các đối tác đến từ khắp nơi trong nước này.
- c) Thanh toán vào các tài khoản cá nhân để tránh giám sát hoặc trốn thuế.
- d) Các đối tác chủ yếu là những người trẻ tuổi và trung niên biết sử dụng Internet và họ chủ yếu là bạn bè hoặc người quen.
- e) Đặc trưng dễ nhận thấy của các giao dịch là có khoản tiền nhỏ được triết khấu.

476. Sau đó, cảnh sát đã lập hồ sơ vụ án, và niêm phong hàng trăm triệu nhân dân tệ và bắt giữ 6 nghi phạm.

ĐÀI LOAN, TRUNG QUỐC

477. Tháng 7/2015, Bộ phận phòng chống rửa tiền (AMLD) đã nghiên cứu thông tin tình báo tài chính do một ngân hàng báo cáo về tài khoản của ông S gần đây đã nhận được một số tiền mặt lớn được gửi vào. Hoạt động tài chính này không phù hợp với khả năng tài chính và lịch sử giao dịch của ông S. AMLD đã quyết định tiến hành phân tích sâu hơn. Sau khi phân tích các tài liệu liên quan do các tổ chức tài chính cung cấp, AMLD đã nhận thấy các giao dịch này có thể liên quan đến các hoạt động bất hợp pháp.

478. Tháng 11/2015, AMLD đã chuyển giao vụ việc này cho MJIB. MJIB đã mở một cuộc điều tra và tìm ra chân tướng sự việc như sau: Ông T và ông W là chủ tịch tiền nhiệm và kế nhiệm của Công ty T, một công ty niêm yết tại Đài Loan Trung Quốc. Ông L là giám đốc của Công ty T. Vào tháng 5/2015, ông T và những người khác đã thành lập Công ty F ở nước ngoài và chỉ định ông S làm chủ tịch và sử dụng Công ty F để mua các khoản phải thu của Công ty T và vốn các công ty con của Công ty T. Tuy nhiên, quá trình thẩm định và ký kết thỏa thuận không được tiến hành theo các thủ tục thông thường và các tài liệu liên quan đã không được xem xét hoặc phê duyệt bởi Hội đồng quản trị. Vào tháng 7, Công ty T đã tiết lộ thông tin quan trọng cho biết Công ty F đã mua các tài sản nói trên của Công ty T với tổng số tiền khoảng 204 triệu Đài tệ và Công ty F sẽ thanh toán theo kế hoạch trả góp. Sau nhiều lần thanh toán, Công ty F đã không thể tiếp tục trả tiền vì một số lý do. Ông T và cộng sự đã không tích cực yêu cầu Công ty F thực hiện hợp đồng. Điều đó đã khiến Công ty T nhận khoản lỗ khoảng 33,3 triệu Đài tệ.

479. Sau khi MJIB hoàn tất cuộc điều tra, vụ việc liên quan đến vi phạm Đạo luật Chứng khoán và ngoại hối đã được chuyển đến Văn phòng Công tố vào tháng 4/2018 để truy tố.

FIJI

480. Năm 2018, FIU Fiji đã cấp 321 CDR cho Lực lượng cảnh sát Fiji, Cơ quan hải quan và thuế, các FIU nước ngoài và các cơ quan thực thi pháp luật khác có liên quan. CDR được xây dựng từ việc phân tích các STR. Đối tượng chính nhận CDR của FIU Fiji là Cục Hải quan & thuế (FRCS) cảnh báo về những vi phạm Đạo luật Thuế thu nhập và thuế giá trị gia tăng (VAT). Trong năm 2018, đã có 207 báo cáo như vậy được chuyển cho FRCS, 62 CDR cho Lực lượng cảnh sát Fiji, bao gồm cả Đơn vị chống rửa tiền và tài sản do phạm tội mà có, Đơn vị chống tội phạm xuyên nước và Cục tình báo của cảnh sát.

481. Là một phần của phân tích STR, việc kiểm tra cũng được thực hiện trên cơ sở dữ liệu trực tuyến của FIU Fiji bao gồm báo cáo giao dịch tiền mặt, báo cáo chuyển tiền điện tử (EFTR) và báo cáo chuyển tiền qua biên giới (BCR).

482. Cơ sở dữ liệu của FIU Fiji cũng có thể được truy cập bởi các cơ quan đối tác chính thông qua cơ chế truy cập dữ liệu trực tiếp (DDA).

MALAYSIA

Vụ việc về tài trợ khủng bố

483. Là một phần của sáng kiến khu vực về CFT, FIU đã tham gia chương trình trao đổi cán bộ phân tích trong khu vực để phân tích các giao dịch đáng ngờ liên quan đến nhóm vũ trang Maute liên kết với ISIL được đặt tại miền Nam Philippines. Chương trình này được diễn ra từ tháng 5 đến tháng 8/2018 có sự tham gia của các cán bộ phân tích đến từ Trung tâm phân tích và báo cáo giao dịch Úc (AUSTRAC), Cơ quan tình báo tài chính Indonesia - MaPusat Pelaporan dan Analisis Tansaksi Keuangan (PPATK), BNM và Hội đồng chống rửa tiền (AMLC). Chương trình trao đổi này đã đưa ra một báo cáo tình báo tài chính toàn diện về nhóm Maute dựa trên các giao dịch ở các nước có liên quan. Báo cáo đã được phổ biến đến các cơ quan thực thi pháp luật có liên quan ở tất cả các nước để tiếp tục xử lý.

Lừa đảo – Lừa qua thư điện tử của doanh nghiệp

484. FIU đã nhận được cảnh báo từ cơ quan thực thi pháp luật của nước Y về một khoản tiền 1,5 triệu USD (5,8 triệu MYR) đã được chuyển qua năm giao dịch từ nạn nhân A tại nước Y đến tài khoản ngân hàng thuộc sở hữu của đối tượng X ở Malaysia từ tháng 1 đến tháng 3/2018. Nạn nhân A đã nhận được một lá thư được viết một cách có chủ đích bởi đối tác thương mại của mình. Đối tượng Y đã chỉ đạo nhân viên của mình chuyển tiền cho đối tượng X ở Malaysia. Từ tháng 1 đến tháng 3/2018, những kẻ mạo danh sử dụng địa chỉ email giả mạo để lừa nhân viên của Nạn nhân A thực hiện năm giao dịch chuyển tiền với tổng trị giá 1,5 triệu USD vào tài khoản ngân hàng của Đối tượng X tại Ngân hàng C ở Malaysia.

485. Từ cảnh báo của cơ quan thực thi pháp luật ở nước Y, FIU đã ngay lập tức liên hệ với Ngân hàng C phong tỏa tài khoản không cho thực hiện bất kỳ giao dịch rút tiền nào. Tuy nhiên, tại thời điểm đó, cần lưu ý rằng đối tượng X đã rút một phần tiền thông qua séc ngân hàng và tiền đã được chuyển đến ba đối tác tại địa phương với số dư còn lại trên tài khoản vào khoảng 3,15 triệu RM.

486. Phân tích sơ bộ vụ việc đã có những phát hiện sau:

- Tên đối tượng X gần giống với tên của đối tác thương mại của nạn nhân A;

- Đối tượng X và các đối tác địa phương mới được thành lập vào cùng thời điểm cuối năm 2017 và đầu năm 2018. Sau khi đăng ký kinh doanh, các đối tượng này ngay lập tức mở tài khoản ngân hàng để tạo điều kiện thuận lợi cho việc nhận và chuyển tiền lừa đảo;

- Hầu hết số tiền nhận được từ nạn nhân A đã được rút ngay lập tức trong cùng ngày hoặc ngày làm việc tiếp theo thông qua séc ngân hàng, rút tiền tại ATM và chuyển tiền trực tuyến cho các đối tác, đây là những dấu hiệu phổ biến được ghi nhận trong các vụ lừa đảo; và

- Theo quan sát trên tài khoản của đối tượng X và các đối tác thì thấy, tất cả các khoản tiền cuối cùng đã được rút bằng tiền mặt, điều này đã khiến cho việc lần theo dấu vết người thụ hưởng cuối cùng rất khó khăn.

487. Vụ việc đã được chuyển cho các cơ quan thực thi pháp luật có liên quan và kết quả là tài khoản của đối tượng X bị đóng băng và các đối tượng bị điều tra.

NEW ZEALAND

Vụ việc điển hình 1

488. FIU New Zealand (NZFIU) đã nhận được một SAR liên quan đến một thành viên của NZ OCG gửi một lượng tiền mặt cực lớn tại một sông bạc ở New Zealand. Một cán bộ phân tích của NZFIU đã kiểm tra hồ sơ tài chính và xác định giá trị tài sản và tiền vượt quá những gì mà thông tin từ hồ sơ tài chính này đem lại. NZFIU đã thông tin cho Cơ quan điều tra tội phạm của New Zealand và cơ quan bắt đầu tiến hành hoạt động điều tra về những hành vi của cá nhân này. Sau đó, cá nhân này đã bị bắt vì liên quan đến việc sản xuất và cung cấp methamphetamine, và tài sản trị giá khoảng 770 nghìn USD đã bị thu giữ theo Luật tố tụng hình sự của New Zealand.

Vụ việc điển hình 2

489. NZFIU đã nhận được SAR liên quan đến một cá nhân không xác định được đã thanh toán các hóa đơn tiền điện của hộ gia đình có giá trị cực kỳ cao bằng cách sử dụng một lượng lớn tiền mặt. NZFIU đã yêu cầu công ty điện lực xác định chủ sở hữu của tài khoản mà các khoản tiền được thanh toán. NZFIU đã chuyển giao 1 báo cáo cho NZP quận nơi mà cá nhân này cư trú, trong đó có nêu nhận định rằng cá nhân này có khả năng đang thực hiện hoạt động trồng cần sa trong nhà. NZP Quận đã tiến hành điều tra đối với cá nhân này và xác định cá nhân này thực sự đang tiến hành hoạt động trồng cần sa trong nhà từ nhà của mình; anh ta đã bị bắt và bị buộc tội liên quan đến cần sa.

Vụ việc điển hình 3

490. NZFIU nhận được một SAR liên quan đến công ty xuất nhập khẩu hàng điện tử có hoạt động tài chính đáng ngờ xảy ra trong tài khoản của công ty tại New Zealand, bao gồm các khoản tiền gửi không giải thích được, thanh toán vượt hạn mức thẻ tín dụng và các giao dịch đến/đi các nước, vùng lãnh thổ có rủi ro cao. NZFIU đã tìm hiểu thông tin từ các cơ quan đối tác và đưa ra nhận định rằng công ty này có thể tham gia vào hoạt động rửa tiền trên cơ sở thương mại. NZFIU đã có một báo cáo tình báo chi tiết về vụ việc và chuyển báo cáo cho đơn vị điều tra đặc biệt và đơn vị này đã bắt đầu cuộc điều tra hình sự chính thức về các hoạt động của công ty.

SINGAPORE

Thu hồi 2,9 triệu đô-la Singapore trong vụ việc vi phạm về tín thác được phát hiện từ các báo cáo giao dịch đáng ngờ

491. Văn phòng báo cáo giao dịch đáng ngờ Singapore (STRO) đã nhận được một số STR về cá nhân A, là kế toán của Công ty B- công ty đăng ký tại Singapore. Kết quả phân tích của STRO cho thấy có nhiều khoản tiền gửi bằng séc từ các công ty hải ngoại vào tài khoản của cá nhân A tại Singapore. Điều này là bất thường vì các công ty hải ngoại được Công ty B quan tâm và cá nhân A không có quyền sở hữu trong các công ty này. Cần lưu ý rằng các khoản tiền sau đó đã được rút bằng tiền mặt, séc và không được chuyển cho các doanh nghiệp khác.

492. STRO đã chuyển giao thông tin từ các STR này và kết quả phân tích của mình cho cơ quan thực thi pháp luật có liên quan ở Singapore. Các cuộc điều tra cho thấy cá nhân A đã chiếm đoạt số tiền tương đương 46,2 triệu đô-la Singapore từ Công ty B và các công ty nước ngoài của họ bằng cách chuẩn bị các chứng từ thanh toán giả mạo và sử dụng séc ký không có chữ ký của người được ủy quyền. Số tiền thu được từ hành vi phạm tội này chủ yếu được sử dụng để tài trợ cho các hoạt động đánh bạc của cá nhân A. Cơ quan thực thi pháp luật có liên quan đã thu hồi số tiền là 2,9 triệu đô-la Singapore từ cá nhân A.

493. Cá nhân A đã bị kết án 18 năm tù vì các tội của mình bao gồm cả tội vi phạm về tín thác và rửa tiền.

5. ẢNH HƯỞNG CỦA CÁC BIỆN PHÁP ĐỐI KHÁNG VỀ AML/CFT

494. Phần này của báo cáo cung cấp một cái nhìn tổng quan về các kết quả gần đây liên quan đến biện pháp đối kháng về pháp luật, quản lý và thực thi pháp luật.

5.1 Tác động của việc cải thiện khuôn khổ pháp luật hoặc quản lý đến việc phát hiện và / hoặc ngăn ngừa các phương thức cụ thể

AFGHANISTAN

495. FinTRACA đã xây dựng Danh sách theo dõi, cho phép các đối tượng báo cáo truy cập, tra soát khi họ thực hiện các giao dịch với khách hàng. Danh sách chỉ định này rất hữu ích trong việc cảnh báo các đối tượng báo cáo về các mối đe dọa hiện có.

ÚC

Quy định của AUSTRAC về chuyển đổi tiền kỹ thuật số

496. Các Luật mới quy định về các đại lý chuyển đổi tiền tệ kỹ thuật số (DCE) ở Úc đã được AUSTRAC, cơ quan tình báo tài chính và quản lý về chống rửa tiền, tài trợ khủng bố (AML/CFT) của Úc áp dụng vào năm 2018.

497. Các luật AML/ CTF mới đã bổ sung các quy định đối với các nhà cung cấp dịch vụ về tiền điện tử, bao gồm bitcoin, việc tuân thủ và năng lực tình báo nhằm giúp các DCE vận hành, kiểm soát hệ thống nhằm giảm thiểu rủi ro tội phạm sử dụng DCE để rửa tiền, tài trợ khủng bố và tội phạm mạng.

498. Các DCE có hoạt động kinh doanh tại Úc bắt buộc phải đăng ký với AUSTRAC và tuân thủ các nghĩa vụ báo cáo và quy định về AML/ CTF của Chính phủ, cho phép họ bảo vệ hoạt động của mình khỏi hoạt động rửa tiền và tài trợ khủng bố, đồng thời giúp củng cố niềm tin của công chúng và người tiêu dùng trong lĩnh vực này.

499. Những thay đổi này cũng đã tạo điều kiện thuận lợi cho việc chia sẻ thông tin tình báo tài chính và thông tin liên quan đến việc sử dụng các loại tiền kỹ thuật số, chẳng hạn như bitcoin và các loại tiền điện tử khác, giữa các tổ chức trong lĩnh vực và chính phủ. Điều này đã mang lại cho Úc những lợi ích ngay lập tức trong cuộc chiến chống lại tội phạm nghiêm trọng và tội phạm tài trợ khủng bố.

TRUNG QUỐC

500. Theo các yêu cầu trong *Thông báo về quy định liên quan đến các giao dịch rút tiền mặt lớn ở nước ngoài bằng thẻ ngân hàng của Cục quản lý ngoại hối*, từ năm 2018, giá trị giao dịch rút tiền mặt từ thẻ ngân hàng ở nước ngoài của một cá nhân không được vượt quá 100 nghìn nhân dân tệ mỗi năm. Sau khi thực hiện chính sách này, việc rút một lượng lớn tiền mặt ở nước ngoài đã được kiểm chế một cách hiệu quả. Số tiền tối đa cho một lần rút tiền mặt ở nước ngoài, đối với một cá nhân, đã giảm từ một triệu xuống còn 20 hoặc 30 nghìn nhân dân tệ. Năm 2018, tổng số tiền tích được rút bằng tiền mặt ở nước ngoài bằng thẻ của ngân hàng trong nước đã giảm 44% so với năm 2017.

ĐÀI LOAN, TRUNG QUỐC

501. Phù hợp với phạm vi của doanh nghiệp cho thuê tài chính được đưa ra ngày 5/3/2018, Ủy ban giám sát tài chính (FSC) đã ban hành “Quy chế về quản lý phòng, chống rửa tiền của các doanh nghiệp cho thuê tài chính” vào ngày 20/6/2018. Ngày 9/11, FSC đã ban hành các quy định kiểm toán nội bộ và hệ thống kiểm soát nội bộ về

phòng, chống rửa tiền và chống tài trợ khủng bố của doanh nghiệp cho thuê tài chính, ngành ngân hàng, chứng khoán và hợp đồng tương lai và các công ty bảo hiểm. Cũng ngày này, FSC đã sửa đổi đối với “Quy định về phòng, chống rửa tiền và chống tài trợ khủng bố dành cho các kế toán viên công khai được chứng nhận”.

502. Nhằm tăng cường cơ chế AML/CFT của Đài Loan Trung Quốc, ngày 14/11/2018, FSC đã sửa đổi “Quy định về phòng, chống rửa tiền của các tổ chức tài chính” và “Quy định báo cáo về tài sản hoặc lợi ích từ tài sản và vị trí của các cá nhân hoặc đối tượng bị chỉ định xử phạt bởi các tổ chức tài chính”.

503. FSC sẽ tiếp tục giám sát các ngành công nghiệp tài chính để tuân thủ các quy định liên quan đến AML và triển khai công tác AML/CFT và tiếp tục xem xét các quy định liên quan đảm bảo việc phù hợp với các quy tắc quốc tế.

504. Ngày 07/11/2018, Đài Loan Trung Quốc đã sửa đổi Đạo luật chống rửa tiền (MLCA) và Đạo luật chống tài trợ khủng bố (Đạo luật CTF). Những sửa đổi đối với MLCA chủ yếu là việc đưa các doanh nghiệp xử lý các nền tảng hoặc giao dịch tiền ảo vào cơ chế AML/CFT. Ngoài ra, dựa trên các sửa đổi mới được ban hành này, các tổ chức tài chính và các doanh nghiệp, ngành nghề phi tài chính chỉ định (DNFBP) phải xây dựng hệ thống kiểm toán và kiểm soát nội bộ về AML/CTF dựa trên rủi ro rửa tiền, tài trợ khủng bố cũng như quy mô kinh doanh của tổ chức mình. Đạo luật CTF sửa đổi quy định rằng phạm vi của các biện pháp trừng phạt tài chính mục tiêu (TFS) áp dụng đối với các tài sản thuộc sở hữu toàn bộ hoặc một phần hoặc được kiểm soát, trực tiếp hoặc gián tiếp, hoặc đối với các quỹ hoặc tài sản khác của cá nhân và tổ chức thay mặt cho hoặc theo chỉ đạo của cá nhân và tổ chức bị chỉ định.

FIJI

505. Fiji hiện đang rà soát lại Đạo luật về trật tự công cộng nhằm tăng cường hơn nữa các quy định pháp lý về các biện pháp trừng phạt tài chính mục tiêu (TFS) đối với tài trợ khủng bố (Khuyến nghị số 6) và tài trợ phổ biến vũ khí (Khuyến nghị số 7). Việc rà soát các điều khoản này đã được bắt đầu từ tháng 2/2018. Việc rà soát hiện đang trong giai đoạn tham vấn. APG và CTED cũng đã được tham vấn ý kiến về các điều khoản dự thảo này.

506. Ngân hàng Dự trữ của Fiji (RBF) đã tăng cường thanh tra tại chỗ về AML/CFT đối với các nhà cung cấp dịch vụ chuyển tiền, các tổ chức đổi tiền và đang sửa đổi Chính sách giám sát về AML đối với lĩnh vực này.

507. FIU Fiji đã tăng cường thanh tra tại chỗ về AML/CFT đối với các DNFBP. Năm 2018, FIU đã tiến hành thanh tra tại chỗ về AML/CFT đối với 05 công ty bất động sản và 08 công ty luật.

508. Hiện nay, việc rà soát Đạo luật và các Quy định về doanh nghiệp nhằm giải quyết các lỗ hổng pháp lý quan trọng về tính minh bạch của các chủ sở hữu hưởng lợi của các pháp nhân đang được tiến hành.

INDONESIA

509. BAPPEBTI (Ủy ban giám sát giao dịch tương lai) đã ban hành 04 quy chế về Tài sản mã hóa và Vàng kỹ thuật số. Qua Ngân hàng Trung ương (BI), Indonesia cấm việc sử dụng tất cả các loại tiền ảo trong thanh toán và hệ thống thanh toán. Tuy nhiên, Tiền ảo / Tài sản mã hóa vẫn được cho phép sử dụng đối với mục đích đầu tư và/hoặc kinh

doanh. Các quy định này yêu cầu những nhà kinh doanh tài sản mã hóa và vàng kỹ thuật số trong thị trường giao dịch tương lai phải tuân thủ các quy định về AML/CFT.

MALAYSIA

Giảm ngưỡng Báo cáo giao dịch tiền mặt (viết tắt “CTR” trong các đoạn sau)

510. Có hiệu lực từ ngày 01/1/2019, BNM, với tư cách là cơ quan có thẩm quyền theo Đạo luật chống rửa tiền, tài trợ chống khủng bố và các khoản tiền thu được từ hoạt động bất hợp pháp năm 2001 (AMLA) đã giảm ngưỡng báo cáo giao dịch tiền mặt từ 50.000 RM (khoảng 12.000 USD) xuống còn 25.000 RM (khoảng 6.000 USD).

511. Quyết định này được đưa ra xuất phát từ những phát hiện trong báo cáo NRA năm 2017, theo đó, tham nhũng là tội phạm có rủi ro cao thứ hai đối với nước. Căn cứ vào kết quả phân tích các vụ việc điển hình và STR, số tiền thu được từ tham nhũng được đưa vào các tổ chức tài chính và các tổ chức tài chính phi ngân hàng là rất khác nhau nhưng thường dưới ngưỡng báo cáo giao dịch tiền mặt được quy định. Điều này ngày càng gây khó khăn cho các cơ quan thực thi trong việc phát hiện hành vi rửa các khoản tiền thu được từ tham nhũng trừ khi có báo cáo STR. Thêm vào đó, ngưỡng báo cáo trước đó là 50.000 RM là tương đối cao so với ngưỡng báo cáo của các nước, vùng lãnh thổ khác và không phản ánh chính xác quy mô và mức độ sử dụng tiền mặt trong nền kinh tế Malaysia.

512. Việc giảm ngưỡng báo cáo sẽ khiến tội phạm khó khăn hơn trong việc rửa tiền thu được từ tội phạm qua các tổ chức báo cáo. Việc tội phạm sử dụng một lượng lớn tiền mặt lưu trữ, di chuyển và phân bổ số tiền bất hợp pháp cho thấy tầm quan trọng của việc thực hiện báo cáo CTR như là một biện pháp phòng ngừa rủi ro rửa tiền và tài trợ khủng bố. Bằng cách hạ thấp ngưỡng báo cáo, hành vi rửa tiền có thể được phát hiện dễ dàng hơn thông qua việc giám sát tăng cường và dễ dàng nhận biết hơn những dấu hiệu của một giao dịch đáng ngờ.

NEW ZEALAND

513. Cơ chế báo cáo giao dịch được miêu tả trước (PTR) đã tăng cường chất lượng hỗ trợ của FIU New Zealand cho các đối tác trong nước và quốc tế.

514. Theo các quy định về AML/CFT đã được cập nhật, hiện nay, các đối tượng báo cáo phải báo cáo các giao dịch tiền mặt có giá trị lớn (LCT) từ 10.000 đô-la trở lên và giao dịch chuyển tiền điện tử quốc tế (IFT) từ 1.000 đô-la trở lên cho FIU New Zealand (NZFIU). Các ví dụ dưới đây minh họa cho các giá trị gia tăng mà báo cáo PTR mang lại khi hỗ trợ NZFIU trong việc dựng nên bức tranh tình báo trong toàn bộ hệ thống tài chính nhằm hỗ trợ cho các cuộc điều tra tội phạm nghiêm trọng và có tổ chức:

- Đơn vị điều tra đặc biệt của cảnh sát New Zealand (NZP) đã gửi yêu cầu cho NZFIU về các cá nhân bị nghi ngờ tham gia vào việc nhập khẩu methamphetamine vào nước. Những cá nhân này trước đây không có trong hồ sơ của NZP và cũng không liên quan đến bất kỳ giao dịch đáng ngờ nào. Trong các tuần tiếp theo, NZFIU đã nhận được các PTRs về các nghi phạm liên quan đến các khoản tiền được gửi vào tài khoản ngân hàng của bên thứ ba. NZFIU đã đưa ra một báo cáo hỗ trợ hướng điều tra của nhóm và các yêu cầu đang được tiếp tục thực hiện. Nếu theo cơ chế trước đây thì các giao dịch này vẫn sẽ không được báo cáo do không có các yếu tố nghi ngờ đối với các giao dịch này ở các đối tượng báo cáo.

- Một FIU đối tác ở nước A đã gửi yêu cầu cho NZFIU liên quan đến các khoản tiền bị nghi ngờ do phạm tội mà có gửi vào tài khoản ngân hàng của một công dân NZ có tên MR (cũng là người chuyển tiền) được giữ ở nước A. FIU đối tác đã yêu cầu cung cấp chi tiết về việc di chuyển của dòng tiền khi tiền vào tài khoản ngân hàng của người gửi tiền ở nước A và ai là người thụ hưởng của giao dịch này. Chỉ dựa trên thông tin PTR, NZFIU đã có thể theo dõi các khoản tiền nghi ngờ thu được từ tội phạm được chuyển đến một tài khoản ở nước B và xác định được ai là người thụ hưởng của giao dịch. NZFIU đã gửi báo cáo cho FIU đối tác để hỗ trợ.

SINGAPORE

Tăng cường truy cập thông tin về chủ sở hữu hưởng lợi

515. Theo cơ chế mới về chủ sở hữu hưởng lợi, các công ty nước ngoài phải nắm được thông tin về chủ sở hữu hưởng lợi của mình thông qua yêu cầu bắt buộc cung cấp đăng ký người kiểm soát cho Cơ quan đăng ký kinh doanh. Theo quy định sửa đổi Mục 386A của Đạo luật về Doanh nghiệp năm 2017, các thông tin đăng ký về người kiểm soát phải được cung cấp cho Cơ quan đăng ký và các cơ quan công quyền để quản lý hoặc thực thi bất kỳ quy định pháp luật nào (bao gồm CAD, CPIB và IRAS) theo yêu cầu. Trên thực tế, những thay đổi này đã giúp nâng cao khả năng tiếp cận các thông tin cơ bản do các cơ quan có thẩm quyền trong nước nắm giữ, trong khi các thông tin này có thể có được từ các tổ chức tài chính và các nhà cung cấp dịch vụ doanh nghiệp (CSP) và cả các DNFBP khác (ví dụ: luật sư và kế toán viên).

516. Với cải thiện nêu trên, các cơ quan thực thi pháp luật có thể tiếp cận thông tin về chủ sở hữu hưởng lợi từ các đại lý được đăng ký. Và, vì lý do này, CPIB đã phối hợp với ACRA để tiến hành các cuộc thanh tra chung các CSP để có cách tiếp cận toàn diện hơn hướng đến việc phòng, chống tội phạm rửa tiền.

6. CÁC TỪ VIẾT TẮT VÀ THUẬT NGỮ

ABF - Lực lượng biên phòng Úc
AFP - Cảnh sát Liên bang Úc
AML - Chống rửa tiền
AMLA - Đạo luật chống rửa tiền
AMLC - Ủy ban chống rửa tiền
AMLD – Bộ phận chống rửa tiền
ANF - Lực lượng chống ma túy (Pakistan)
APG – Nhóm châu Á / Thái Bình Dương về chống rửa tiền
ATM - Máy rút tiền tự động
AUSTRAC - Trung tâm phân tích và báo cáo giao dịch Úc
BCR - Báo cáo tiền tệ qua biên giới
C & ED - Cục Hải quan và Tiêu thụ đặc biệt (Hong Kông, Trung Quốc)
CDD – Cập nhật thông tin khách hàng
CDR - Báo cáo chuyển giao về tiền mặt
CFT - Chống tài trợ khủng bố
CIB - Cục điều tra hình sự
CIPB - Cục điều tra hành vi tham nhũng
CTR - Báo cáo giao dịch tiền mặt/tiền tệ
DGCE - Tổng cục trưởng Hải quan và Tiêu thụ đặc biệt (Indonesia)
DNFBP - Các tổ chức và ngành nghề phi tài chính chỉ định
EAG - Nhóm Á-Âu
ECOFEL – Trung tâm điều hành và lãnh đạo FIU của Nhóm Egmont
EFT - Chuyển tiền điện tử
ESW – Trang web được bảo mật của Egmont
FATF - Lực lượng đặc nhiệm tài chính về chống rửa tiền
FINTRAC - Trung tâm phân tích báo cáo giao dịch tài chính (Canada)
FIU - Đơn vị tình báo tài chính
FMU - Đơn vị giám sát tài chính (Pakistan)
FRCS – Cơ quan hải quan và sở thuế vụ Fiji
FSRB - Các tổ chức khu vực dạng FATF
GIF - Văn phòng tình báo tài chính (Macao, Trung Quốc)
HT - Buôn người
IDR – Đồng rupia Indonesia

ICRG - Nhóm rà soát các vấn đề hợp tác quốc tế

IFTI – Chỉ dẫn giao dịch chuyển tiền quốc tế

INTERPOL - Tổ chức cảnh sát hình sự quốc tế

JAFIC - Trung tâm tình báo tài chính Nhật Bản

KYC – Nhận biết khách hàng

LEA - Cơ quan thực thi pháp luật

MIT – Nhóm khủng bố hoạt động ở Indonesia (Mujahidin Indonesia Timur)

MJIB - Cục Điều tra Bộ Tư pháp

MG - Tập đoàn Maute (Philippines)

ML - Rửa tiền

MR - Chuyển tiền

MSP - Nhà cung cấp dịch vụ tiền tệ

NAB – Ban Nước thực thi giải trình (National Accountability Bureau) (Pakistan)

NCC - Ủy ban điều phối nước về phòng chống rửa tiền (Malaysia)

NGO - Tổ chức phi chính phủ

NNB - Ủy ban chống ma túy nước (Indonesia)

NPO - Tổ chức phi lợi nhuận

NRA - Đánh giá rủi ro nước

NZP - Cảnh sát New Zealand

NZFIU - Đơn vị tình báo tài chính New Zealand

OCG - Các nhóm tội phạm có tổ chức

PPATK – Đơn vị tình báo tài chính Indonesia

PS - Buôn người

PEP – Cá nhân có ảnh hưởng chính trị

PKR – Đồng Rupee Pakistan

PML – Rửa tiền chuyên nghiệp

POI – Cá nhân bị truy tìm

PTR - Báo cáo giao dịch được miêu tả trước

RI – Các tổ chức báo cáo

RMP - Cảnh sát Hoàng gia Malaysia

SAR - Báo cáo hoạt động đáng ngờ

SEA CTFWG - Nhóm công tác chống tài trợ khủng bố ở Đông Nam Á

SEC - Ủy ban Ngoại hối và Chứng khoán (Philippines)

STR - Báo cáo giao dịch đáng ngờ

SVF – Các công cụ lưu trữ giá trị

TF - Tài trợ khủng bố

TRACFIN – Cơ quan tình báo tài chính của Pháp (France FIU)

TTP – Sự dịch chuyển Taliban của Pakistan

VAT - Thuế giá trị gia tăng

VC - Tiền ảo