NGÂN HÀNG NHÀ NƯỚC VIỆT NAM
CỤC PHÒNG, CHỐNG RỬA TIỀN

BÁO CÁO HỘI NGHỊ MÔ HÌNH THƯỜNG NIÊN NĂM 2024
Từ ngày 11-13/11/2024 tại Malaysia

Hội nghị được chủ trì bởi ông Marzunisham Omar - Phó Thống đốc Ngân hàng Trung ương Malaysia và Ban Thư ký APG cùng với sự tham dự của gần 200 đại biểu đến từ các nước thành viên APG. Trong đó, phiên họp đầu tiên của Hội nghị là phiên họp toàn thể, sau đó Hội nghị được chia thành 02 phiên song song với 02 chủ đề là: *Lợi dụng pháp nhân để rửa tiền, tài trợ khủng bố* và *Gian lận, lừa đảo thông qua phương thức điện tử*. Hội nghị đã trao đổi, thảo luận các vấn đề cụ thể sau:

1. Nội dung phiên họp toàn thể

Tại phiên họp toàn thể sáng ngày 11/11/2024, Hội nghị thông qua dự thảo Báo cáo mô hình thường niên năm 2024 của APG. Chủ trì phiên họp là ông Mohd Fuad Arshad, Giám đốc Đơn vị tình báo tài chính (FIU) Malaysia; các diễn giả tham gia thảo luận, chia sẻ gồm: Ông Vipin Kumar Ashok, Phó Giám đốc FIU Ấn Độ; ông Mohamad Nahar Bin Haris, Chuyên gia Ủy ban phòng chống tham nhũng Malaysia; bà Hsun-Yi Wang, Chuyên gia, Cục Điều tra Bộ Tư pháp, Đài Loan, Trung Quốc; ông Abdulla Ashraf, Giám đốc FIU Maldives.

Báo cáo cung cấp **141** nghiên cứu điển hình mô tả các phương pháp và xu hướng rửa tiền, tài trợ khủng bố, tài trợ phổ biến vũ khí hủy diệt hàng loạt (RT, TTKB, TTPBVKHDHL) mới nhất, gồm các nghiên cứu điển hình lạm dụng pháp nhân.

2. Nội dung phiên họp song song

2.1. Phiên họp Lợi dụng pháp nhân để rửa tiền, tài trợ khủng bố

a) Khuyến nghị 24[1]

Vào tháng 3 năm 2022, FATF đã tăng cường Khuyến nghị 24 (R.24) và Lưu ý thực hiện (Interpretive Note) đối với các Khuyến nghị của FATF liên quan đến tính minh bạch và chủ sở hữu hưởng lợi (BO) của pháp nhân. FATF cũng đã công bố

[1] Các diễn giả tham gia: Bà Caroline Bicheno, Ban Thư ký APG; Bà Pei Yu Su, Thư ký điều hành Văn phòng chống rửa tiền Đài Loan, Trung Quốc; Ông Andrey Frolov, Tư vấn cấp cao Ban thư ký EAG

hướng dẫn cập nhật về chủ sở hữu hưởng lợi của pháp nhân để hỗ trợ các nước thực hiện các yêu cầu R.24 tăng cường.

R.24 hiện yêu cầu các nước đánh giá và kiểm soát rủi ro do pháp nhân, không chỉ đối với các rủi ro do được tạo ra trong một nước/một khu vực pháp lý mà cả người nước ngoài có quyền sở hữu hưởng lợi có mối liên hệ với khu vực pháp lý đó. Đáng chú ý là, R.24 yêu cầu các khu vực pháp lý phải có cách tiếp cận đa chiều, tức là sử dụng kết hợp các cơ chế khác nhau để thu thập thông tin về BO và đảm bảo thông tin luôn sẵn sàng phục vụ các cơ quan có thẩm quyền một cách kịp thời.

b) Hiểu biết của các nước thành viên về rủi ro RT/TTKB do lạm dụng pháp nhân

Theo Khuyến nghị của FATF, các khu vực pháp lý phải đánh giá rủi ro RT/TTKB/TTPBVKHDHL theo Khuyến nghị 1 và rủi ro RT/TTKB liên quan đến pháp nhân theo Khuyến nghị 24. Khuyến nghị 24 yêu cầu các quốc gia đánh giá rủi ro RT/TTKB của các cấu trúc pháp lý được hình thành và quản lý ở quốc gia mình cũng như các cơ cấu pháp lý nước ngoài nhưng có liên kết với quốc gia. Theo thống kê, có 38/42 thành viên của APG (chiếm 90%) đã thực hiện đánh giá chéo theo Phương pháp FATF cập nhật. Kết quả:

- 06 thành viên (14%) đã đánh giá rủi ro RT/TTKB liên quan đến pháp nhân tại thời điểm đánh giá chéo[2];

- 20 thành viên (48%) đã đánh giá rủi ro RT/TTKB liên quan đến pháp nhân tại thời điểm đánh giá chéo. Tuy nhiên, nhóm đánh giá cho rằng việc đánh giá rủi ro của các nước này ở cấp độ quá cơ bản, chung chung, không toàn diện theo yêu cầu cần làm, không bao gồm đầy đủ các loại hình pháp nhân, không đánh giá đầy đủ cả pháp nhân trong nước và/hoặc quốc tế, hoặc không đánh giá đồng thời cả rủi ro RT/TTKB[3] (Việt Nam nằm trong nhóm 20 nước thành viên này).

- 06 thành viên (14%) chưa đánh giá rủi ro RT/TTKB liên quan đến pháp nhân tại thời điểm đánh giá chéo. Sau đó, đã tiến hành đánh giá rủi ro[4].

- 06 thành viên (14%) chưa thực hiện đánh giá rủi ro RT/TTKB liên quan đến pháp nhân tại thời điểm đánh giá chéo.[5]

---

[2] Canada, Ấn Độ, Indonesia, Hàn Quốc, New Zealand and Mỹ.
[3] Bangladesh, Đài Loan Trung Quốc, Cook Islands, Hong Kong, Trung Quốc, Nhật Bản, Macao, Malaysia, Marshall Islands, Mongolia, Myanmar, Nauru, Pakistan, Palau, Samoa, Solomon Islands, Timor-Leste, Thái Lan, Tonga, Vanuatu and Việt Nam.
[4] Úc, Bhutan, Brunei, Philippines, Singapore và Sri Lanka.
[5] Campuchia, Trung Quốc, Fiji, Lào, Nepal và Papua New Guinea.

Trên cơ sở kết quả đánh giá rủi ro RT/TTKB, các quốc gia cần xác định các lỗ hổng cụ thể trong hệ thống phòng, chống rửa tiền, chống tài trợ khủng bố của quốc gia mình để phát triển các biện pháp quản lý và giảm thiểu ro. Điều này bao gồm tăng cường khung pháp lý, cải thiện việc thu thập và chia sẻ dữ liệu, tăng cường giám sát và thúc đẩy hợp tác quốc tế.

c) Các mối đe dọa lạm dụng pháp nhân để RT/TTKB/TTPBVKHDHL

- Báo cáo Tài trợ phổ biến hóa học, sinh học, phóng xạ hoặc hạt nhân (CBRN) của Viện nghiên cứu tư pháp và tội phạm liên khu vực Liên Hợp quốc (UNICRI)[6]:

Tháng 10/2023, UNICRI công bố Báo cáo "Tài trợ phổ biến CBRN: Góc nhìn từ Đông Nam Á". Báo cáo tập trung vào sự phức tạp của tài trợ tài chính cho hoạt động phổ biến vũ khí hạt nhân, thông tin chi tiết về các mối đe dọa tài trợ phổ biến vũ khí hạt nhân ở Đông Nam Á, giải quyết các mối quan tâm như kế hoạch mua vũ khí hủy diệt hàng loạt (WMD), mạng lưới phổ biến WMD và các hoạt động tạo doanh thu được thiết kế để trốn tránh các chương trình trừng phạt. Báo cáo cũng đưa ra các biện pháp để giảm thiểu rủi ro tài trợ tài chính phổ biến vũ khí hạt nhân; trong đó, hợp tác và chia sẻ kiến thức được coi là rất quan trọng để củng cố các khuôn khổ khu vực và toàn cầu nhằm ngăn chặn việc lạm dụng các hệ thống tài chính cho các hoạt động phổ biến vũ khí hạt nhân.

- Công ước Liên hợp quốc về chống tham nhũng (UNCAC)[7]: Công cụ chống tham nhũng phổ quát ràng buộc pháp lý duy nhất. Công ước đã được soạn thảo và đàm phán tại Vienna, Áo vào năm 2002-2003 và sau đó được Đại hội đồng Liên Hợp Quốc thông qua vào ngày 31/10/2003. UNCAC (Điều 12) yêu cầu mỗi quốc gia cần thực hiện các biện pháp phù hợp với các nguyên tắc của luật pháp quốc gia mình để ngăn chặn tham nhũng liên quan đến khu vực tư nhân và đưa ra các hình phạt hình sự hay hành chính cho việc không tuân thủ các biện pháp này khi cần thiết. Các biện pháp này có thể bao gồm việc thúc đẩy sự minh bạch giữa các tổ chức tư nhân, bao gồm biện pháp xác định người đại diện pháp lý thật sự trong việc thành lập và quản lý doanh nghiệp.

- Tháng 5/2024, UNODC công bố báo cáo về việc thực hiện minh bạch BO của các nước ASEAN và Timo-Leste. Về khuôn khổ pháp lý có 04 quốc gia thành viên (Campuchia, Lào, Thái Lan, Việt Nam) đưa định nghĩa về BO và minh bạch thông tin BO vào nghĩa vụ PCRT/TTKB; 07 quốc gia còn lại (Brunei, Indonesia, Malaysia, Myanmar, Philipine, Singapore, Timor-Leste) nêu định nghĩa về BO và

[6] Diễn giả Carlotta Diễn giả Carlotta Zenere, Điều phối viên, UNICRI
[7] Diễn giả Anne Lim, Tư vấn Chương trình chống tham nhũng, UNODC

minh bạch thông tin BO liên quan đến việc thu thập thông tin về pháp nhân và thỏa thuận pháp lý. Về cơ chế xác minh thông tin BO: Indonesia sử dụng công chứng khi thành lập doanh nghiệp lần đầu nhưng không bắt buộc cho các lần thay đổi chủ sỡ hữu sau đó, Philippines yêu cầu công chứng các biểu kê khai thông tin doanh nghiệp. Về cập nhật thông tin BO: 05 quốc gia yêu cầu cập nhật khi có thay đổi với thời hạn hoàn thành (Brunei, Singapore trong 02 ngày làm việc, Philippines trong 07 ngày làm việc, Timor-Leste trong 10 ngày làm việc), 04 quốc gia (Indonesia, Malaysia, Philipine, Timor-Leste) yêu cầu cập nhật ít nhất hàng năm.

d) Luật sư, kế toán, tín thác và các nhà cung cấp dịch vụ công ty (TCSP) bị lợi dụng để cấu trúc doanh nghiệp[8]

Đánh giá rủi ro quốc gia (NRA) của Anh năm 2015, 2017 và 2020 đã xác định sự không thống nhất trong phương pháp giám sát đối với các đơn vị chuyên nghiệp (lĩnh vực pháp lý và kế toán) là một trong những lỗ hổng quan trọng để rửa tiền (mức độ rủi ro Cao).

Báo cáo đánh giá đa phương năm 2018 của FATF đối với Anh cũng xác định điểm yếu đáng chú ý trong hoạt động giám sát đối với lĩnh vực pháp lý và kế toán (đặc biệt về sự sự thống nhất, áp dụng phương pháp giám sát trên cơ sở rủi ro).

e) Các chỉ dấu cờ đỏ xác định các doanh nghiệp/lĩnh vực có rủi ro cao[9]

- Giao dịch phức tạp, bất thường: Sắp xếp cấu trúc doanh nghiệp phức tạp nhằm che dấu mục đích thật sự của giao dịch và BO của giao dịch; Giao dịch được thực hiện có cấu trúc phức tạp hoặc có hoạt động kinh doanh ở các quốc gia khác nhau.

- Sử dụng công ty vỏ bọc: Thành lập doanh nghiệp không có hoạt động kinh doanh thật sự.

- Yếu tố địa lý: Cấu trúc doanh nghiệp có yếu tố nhiều quốc gia, phức tạp về chủ sở hữu, tài sản; Giao dịch liên quan tới các quốc gia tại khu vực được coi là thiên đường thuế.

- Thiếu minh bạch: Bất cập trong việc xác minh cấu trúc chủ sở hữu; Khách hàng trốn tránh nghĩa vụ khai báo thông tin về mục đích của giao dịch.

- Bất minh về tài sản: Tài sản được xử lý hoặc mua lại trong những tình huống không cần thiết; Tài sản không liên quan đến mục đích sử dụng của tài khoản.

---

[8] Diễn giả Jacqueline Griffiths, Văn phòng giám sát chống rửa tiền đối với các đơn vị chuyên nghiệp (lĩnh vực pháp lý và kế toán) (OPBAS), Anh.

[9] Diễn giả Euriica Wong (Bank of China, Malaysia)

- Sử dụng các dịch vụ chỉ định và tín thác: Sử dụng bên thứ ba để làm khó cho việc kiểm soát nguồn tiền bất hợp pháp; Sử dụng doanh nghiệp có tên gần giống nhau.

f) Các cơ quan thực thi pháp luật sử dụng thông tin đăng ký BO[10]

Cơ quan thực thi pháp luật sử dụng thông tin cho nhiều mục đích như điều tra tình báo, củng cố chứng cứ, khởi tố và xác định tài sản. Cơ sở dữ liệu về BO cung cấp thông tin về các cá nhân, các doanh nghiệp liên quan tới cá nhân đó, giúp cơ quan thực thi pháp luật đánh giá hoạt động kinh doanh hợp pháp hay liên quan tội phạm.

Philippines gần đây đã khởi xướng Chương trình cải cách đăng ký công ty để tăng cường và hợp lý hóa quyền truy cập của cơ quan thực thi pháp luật đối với thông tin quyền sở hữu có lợi. Các hành động bao gồm:

- Ủy ban Chứng khoán và Giao dịch Philippines (SEC) đã giới thiệu đăng ký tự động vào eFAST và đăng ký bắt buộc về quyền sở hữu hưởng lợi trong quá trình thành lập. SEC đã bổ sung các hướng dẫn về việc đặt các công ty vào tình trạng nợ quá hạn khi không nộp các yêu cầu báo cáo.

- Tháng 4/2024, đã có trên 500 doanh nghiệp đang hoạt động, 68% các doanh nghiệp này đã tuân thủ yêu cầu khai báo BO. SEC đã đưa 32% doanh nghiệp chưa khai báo vào tình trạng "không tuân thủ"; trong đó 97% các doanh nghiệp này là doanh nghiệp nhỏ, siêu nhỏ và trung bình.

- SEC đã đặt 117.885 doanh nghiệp vào kiểm soát và không hoạt động trong vòng 8 năm qua. Đáng chú ý là 100% các doanh nghiệp này đều không có báo cáo liên quan đến hoạt động kinh doanh trong thời gian này.

- SEC đã làm việc với khoảng 19 cơ quan, đơn vị, thực hiện 734 yêu cầu cung cấp thông tin liên quan đến thông tin doanh nghiệp, bao gồm thông tin về BO về 4.989 doanh nghiệp và 1.099 cá nhân.

g) Các hành động của cơ quan chức năng, cơ quan thực thi pháp luật[11]

Theo Luật Chống rửa tiền số 8 năm 2010, mức phạt cho tội rửa tiền tối đa là 100 tỷ IDR, các hình phạt bổ sung gồm: Thông báo vi phạm, đình chỉ hoạt động, thu hồi giấy phép, tiếp quản.

---

[10] Diễn giả Daniel Macalino, Ủy ban Chứng khoán và Giao dịch Philippines (SEC)
[11] Diễn giả Pak Jarkasih, Trưởng phòng điều tra thuế - Tổng cục Thuế (DGT), Indonesia

Tội phạm thuế và các tội phạm liên quan đến thuế bao gồm: Không kê khai thu nhập thuế, điền thông tin thuế không đúng/ không chính xác, từ chối thực hiện kiểm toán thuế, không lưu trữ chứng từ/báo cáo, sử dụng hóa đơn thuế giả mạo. BO là người nắm giữ trên 25% sở hữu của doanh nghiệp, hoặc người là kiểm soát, người hưởng lợi, chủ sở hữu thực sự của doanh nghiệp. Việc xác định BO thông qua các chứng từ pháp lý của doanh nghiệp có thể xác định chủ sở hữu nắm giữ trên 25% vốn của doanh nghiệp. Đối với các trường hợp còn lại, việc xác định BO phải dựa vào các công cụ/kỹ thuật phân tích tài chính.

h) Hợp tác quốc tế trong tịch thu tài sản (vụ việc sử dụng công ty vỏ bọc để rửa tiền)[12]

Theo thông tin trao đổi với Quốc gia A vào đầu năm 2023, Hải quan Hồng Kông đã phát hiện một chỉ dấu về giao dịch rửa tiền thông qua hoạt động thương mại liên quan đến buôn bán kim cương để rửa 500 triệu HKD (~ 64 triệu USD) trong khoảng thời gian từ tháng 1 đến tháng 12/2021. Có năm công ty được thành lập để xuất khẩu kim cương tổng hợp có giá trị thấp sang Quốc gia A dưới vỏ bọc kim cương tự nhiên có giá trị cao, cắt và đánh bóng cho mục đích rửa tiền.

Giá trị của kim cương tổng hợp đã được phóng đại rất nhiều theo như khai báo. Thông qua việc thổi phồng giá trị khai báo, tổ chức này sau đó đã chuyển số tiền thu được từ tội phạm của họ từ Quốc gia A sang Hồng Kông, Trung Quốc dưới dạng "thanh toán hợp pháp" cho kim cương. Tổ chức này đã sử dụng tài khoản ngân hàng của năm công ty để xử lý số tiền thu được từ tội phạm và giải ngân cho hơn 100 công ty địa phương để tiếp tục giao dịch. Từ tháng 12/2023 đến tháng 2/2024, Hải quan Hồng Kông đã vô hiệu hóa tổ chức này bằng cách bắt giữ năm người vì tội rửa tiền ở Hồng Kông, Trung Quốc và thu giữ 1 triệu HKD (~ 0,13 triệu USD).

Những khó khăn/thách thức trong vụ việc: Quá trình tố tụng kéo dài và phức tạp (do liên quan đến nhiều quốc gia), thông tin hạn chế liên quan những công ty vỏ bọc được đăng ký tại các thiên đường thuế, nỗ lực phối hợp/hợp tác quốc tế trong việc phá vỡ mạng lưới tội phạm quốc tế.

Đề xuất các biện pháp cần tăng cường trong thời gian tới: Hợp tác công tư (PPP), chia sẻ thông tin tình báo giữa các quốc gia, tạo kênh liên lạc chuyên biệt và sử dụng công nghệ.

---

[12] Diễn giả Alex FAN, Cục Điều tra và tình báo tài chính – Cảnh sát Hong Kong

3. Nội dung phiên họp gian lận, lừa đảo qua phương thức điện tử

a) Lừa đảo điện tử: Là hành vi gian lận sử dụng các phương tiện điện tử, chẳng hạn như thư điện tử, trang web giả mạo, tin nhắn điện thoại hoặc các nền tảng mạng xã hội nhằm đánh lừa người dùng cung cấp thông tin nhạy cảm (như thông tin tài khoản ngân hàng, mật khẩu, mã OTP) hoặc cung cấp tiền. Những kẻ lừa đảo điện tử thường khai thác sự thiếu cảnh giác của người dùng bằng các phương thức tinh vi, bao gồm:

- Giả mạo trang web: Tạo các trang web hoặc ứng dụng như trang web chính thức của ngân hàng hoặc công ty để đánh cắp thông tin đăng nhập;

- Email lừa đảo (phishing): Gửi email giả mạo từ những địa chỉ đáng tin cậy (như ngân hàng, tổ chức chính phủ) với nội dung yêu cầu người dùng cung cấp thông tin cá nhân, đăng nhập tài khoản hoặc nhấp vào đường link có chứa mã độc;

- Tin nhắn lừa đảo (smishing): Dùng tin nhắn SMS giả danh các tổ chức để dẫn dụ người dùng truy cập vào các đường link độc hại hoặc cung cấp thông tin cá nhân;

- Giả danh qua điện thoại (vishing): Giả danh nhân viên ngân hàng hoặc công an gọi điện cho người dùng với các lý do như xác minh tài khoản, điều tra lừa đảo, nhằm đánh cắp thông tin tài chính.

- Lừa đảo qua mạng xã hội: Mạo danh người thân hoặc bạn bè của nạn nhân để nhờ chuyển tiền, nhờ thanh toán, lừa nạn nhân truy cập vào đường link nguy hiểm.

Thời gian qua, các hoạt động lừa đảo trực tuyến ở Đông Nam Á đã chuyển từ các băng nhóm lừa đảo nhỏ lẻ, độc lập sang các tổ chức tội phạm lớn hơn, hoạt động theo hình thức công nghiệp hóa. Các nhóm tội phạm này thường hoạt động dưới vỏ bọc của các khu công nghiệp và công nghệ, tạo ra mạng lưới hoạt động ổn định với quy mô lớn, tinh vi và có tổ chức. Các hoạt động lừa đảo trực tuyến tập trung chủ yếu ở các khu vực có quy định yếu kém và pháp luật lỏng lẻo, bao gồm Myanmar, Campuchia, Lào và Philippines. Các Đặc khu Kinh tế (SEZ) với ưu đãi về thuế và quy định đặc biệt đã trở thành "thiên đường" cho các tổ chức tội phạm. Sự yếu kém trong quản lý và tham nhũng ở một số quốc gia đã tạo điều kiện cho các hoạt động lừa đảo trực tuyến phát triển mạnh.

b) Một số hình thức rửa tiền mới

- Rửa tiền thông qua tiền điện tử: Vai trò ngày càng tăng của tiền điện tử trong rửa tiền. Tính chất ẩn danh và phi tập trung của tiền điện tử khiến tội phạm khó theo dõi hơn. Các phương thức mà tội phạm sử dụng tiền điện tử để rửa tiền, bao gồm:

+ Sử dụng sàn giao dịch tiền điện tử không được kiểm soát: Tội phạm có thể sử dụng các sàn giao dịch hoạt động ở các khu vực pháp lý có quy định lỏng lẻo hoặc không tuân thủ các quy định PCRT/TTKB để rửa tiền.

+ Sử dụng máy trộn tiền điện tử (mixer): Mixer là dịch vụ che giấu nguồn gốc của tiền điện tử bằng cách trộn lẫn các khoản tiền từ nhiều nguồn khác nhau. Điều này gây khó khăn cho việc theo dõi dòng tiền bất hợp pháp.

+ Chuyển tiền điện tử qua nhiều ví và sàn giao dịch: Tội phạm có thể di chuyển tiền điện tử qua một loạt các ví và sàn giao dịch để che giấu dấu vết của họ.

+ Sử dụng các giao dịch OTC (ngoài sàn giao dịch): Giao dịch OTC cho phép tội phạm trao đổi tiền điện tử mà không cần thông qua các sàn giao dịch được kiểm soát, giúp tránh được sự giám sát.

- Rửa tiền thông qua các doanh nghiệp liên quan đến sòng bạc

+ Tội phạm có thể sử dụng các sòng bạc để che giấu nguồn gốc bất hợp pháp của tiền bằng cách trộn lẫn tiền bẩn với tiền hợp pháp được tạo ra thông qua hoạt động kinh doanh cờ bạc.

+ Một số sòng bạc, đặc biệt là những sòng bạc hoạt động ở các khu vực đặc biệt hoặc kém được kiểm soát, có thể tạo điều kiện thuận lợi cho rửa tiền do thiếu giám sát hiệu quả.

- Rửa tiền thông qua gian lận mạng

+ Tội phạm có thể sử dụng các khoản tiền có được từ gian lận mạng để tài trợ cho các hoạt động bất hợp pháp khác hoặc rửa tiền thông qua các phương thức truyền thống.

+ Sự gia tăng của các mô hình tội phạm như dịch vụ (CaaS) cho phép tội phạm dễ dàng tiếp cận các công cụ và dịch vụ để thực hiện gian lận mạng và rửa tiền.

- Rửa tiền thông qua buôn bán người: Tội phạm có thể khai thác nạn nhân buôn người để thực hiện các hoạt động bất hợp pháp như rửa tiền thông qua các tài khoản ngân hàng hoặc doanh nghiệp giả mạo.

c) Một số giải pháp nhằm phòng ngừa và đấu tranh chống lừa đảo trực tuyến của các quốc gia hiện nay

- Hợp tác quốc tế:

+ Hợp tác song phương và đa phương: Các quốc gia Đông Nam Á đã tăng cường hợp tác lẫn nhau và với các quốc gia khác, đặc biệt Trung Quốc, để chia sẻ thông tin tình báo, điều tra chung, truy bắt tội phạm lừa đảo trực tuyến hoạt động xuyên biên giới.

+ Tham gia các tổ chức quốc tế: Các quốc gia này cũng tích cực tham gia vào các diễn đàn và sáng kiến quốc tế như ASEAN, INTERPOL và Diễn đàn Toàn cầu về Gian lận để trao đổi kinh nghiệm, phối hợp hành động chống lừa đảo trực tuyến.

+ Hỗ trợ lẫn nhau trong việc hồi hương nạn nhân: Các quốc gia đã hỗ trợ nhau trong việc xác minh danh tính, giải cứu và hồi hương công dân bị mắc kẹt trong các đường dây lừa đảo ở nước ngoài.

- Thực thi pháp luật:

+ Tăng cường chiến dịch truy quét: Các cơ quan thực thi pháp luật đã tăng cường các chiến dịch truy quét các tụ điểm lừa đảo trực tuyến, đặc biệt là ở các khu vực biên giới và đặc khu kinh tế có quy định lỏng lẻo.

+ Bắt giữ và truy tố tội phạm: Các quốc gia đã đẩy mạnh việc bắt giữ và truy tố các cá nhân và tổ chức liên quan đến hoạt động lừa đảo trực tuyến, bao gồm cả những kẻ cầm đầu, tuyển dụng và điều hành các đường dây lừa đảo.

+ Đóng băng tài khoản và tịch thu tài sản: Các cơ quan chức năng đã áp dụng các biện pháp tài chính để phong tỏa tài khoản ngân hàng, tịch thu tiền mặt, tiền điện tử và tài sản bất hợp pháp có liên quan đến hoạt động lừa đảo.

+ Hợp tác với các ngân hàng và tổ chức tài chính: Các quốc gia đã tăng cường hợp tác với các ngân hàng và tổ chức tài chính để ngăn chặn hoạt động rửa tiền, phát hiện các giao dịch đáng ngờ và hỗ trợ nạn nhân bị lừa đảo.

- Nâng cao nhận thức cộng đồng

+ Tuyên truyền, giáo dục: Các Chính phủ đã triển khai các chiến dịch tuyên truyền, giáo dục công chúng về các hình thức lừa đảo trực tuyến phổ biến, cách thức hoạt động của tội phạm và cách thức phòng ngừa, tự bảo vệ.

+ Cảnh báo sớm: Các cơ quan chức năng đã phát đi các cảnh báo sớm về các chiêu thức lừa đảo mới, các trang web giả mạo, các số điện thoại nghi ngờ lừa đảo.

+ Hỗ trợ nạn nhân: Các quốc gia đã thiết lập các đường dây nóng, trang web và ứng dụng di động để tiếp nhận thông tin, hỗ trợ nạn nhân tố cáo tội phạm và tìm kiếm sự giúp đỡ.

- Hoàn thiện khung pháp lý

+ Bổ sung, sửa đổi luật pháp: Các quốc gia đã và đang xem xét việc sửa đổi, bổ sung luật pháp để tăng cường hiệu quả của việc phòng ngừa, điều tra và xử lý tội phạm lừa đảo trực tuyến.

+ Xây dựng chính sách, quy định cụ thể: Các quốc gia đã ban hành các chính sách, quy định cụ thể về quản lý hoạt động kinh doanh trực tuyến, dịch vụ tài chính, công nghệ thông tin và viễn thông để hạn chế rủi ro lừa đảo trực tuyến.

- Kiểm soát công nghệ

+ Phát triển công nghệ phòng chống: Các quốc gia đã đầu tư vào việc phát triển công nghệ, phần mềm để phát hiện, ngăn chặn các cuộc tấn công mạng, phần mềm độc hại và các hình thức lừa đảo trực tuyến khác.

+ Kiểm soát việc sử dụng internet và mạng xã hội: Một số quốc gia đã áp dụng các biện pháp kiểm soát việc sử dụng internet và mạng xã hội để ngăn chặn việc lan truyền thông tin giả mạo, lừa đảo và tuyển dụng người tham gia vào hoạt động phi pháp.