

Thực trạng lừa đảo chuyển tiền qua tài khoản tại một số quốc gia và một số đề xuất, khuyến nghị

 NGUYỄN HỒ PHƯƠNG THẢO *

● NGÀY NHẬN BÀI: 21/11/2024 ● NGÀY BIÊN TẬP: 8/12/2024 ● NGÀY DUYỆT ĐĂNG: 9/4/2025



ẢNH: ĐT (ST)

* TRƯỜNG ĐẠI HỌC KINH TẾ, ĐẠI HỌC HUẾ

Tóm tắt: Sự phát triển của công nghệ thanh toán đã đặt ra thách thức đối với cơ quan quản lý tại các quốc gia trong việc đối phó với loại hình tội phạm lừa đảo chuyển tiền. Trong vài năm tới, lừa đảo chuyển tiền qua tài khoản được dự đoán sẽ tiếp tục gia tăng đáng kể trên khắp thế giới với tổn thất cực lớn. Bài viết tập trung phân tích hình thức lừa đảo chuyển tiền qua tài khoản và đề xuất một số khuyến nghị đối với các cơ quan quản lý nhà nước tại Việt Nam.

Từ khóa: Lừa đảo, lừa đảo chuyển tiền, tài khoản ngân hàng

MONEY TRANSFER FRAUD IN SOME COUNTRIES AND SEVERAL SUGGESTIONS AND RECOMMENDATIONS

Abstract: The development of payment technology has raised challenges for the regulatory authorities in dealing with money transfer fraud. In the next few years, money transfer fraud is predicted to continue to increase significantly globally with huge losses. This article focuses on analyzing types of money transfer fraud through bank accounts and proposes some recommendations for regulatory authorities in Vietnam.

Keywords: Fraud, money transfer fraud, bank account

1. ĐẶT VẤN ĐỀ

Sự phát triển của công nghệ thanh toán đã đặt ra thách thức đối với cơ quan quản lý tại các quốc gia trong việc đối phó với loại hình tội phạm lừa đảo chuyển tiền. Không thể phủ nhận được đóng góp to lớn của sự phát triển công nghệ thanh toán trong việc thúc đẩy chuyển đổi kinh tế xã hội ở nhiều quốc gia. Dữ liệu hiện tại từ Capgemini và GlobalData – các công ty phân tích dữ liệu hàng đầu thế giới - cho thấy đến năm 2030, thị trường thanh toán không dùng tiền mặt toàn cầu sẽ đạt tốc độ tăng trưởng kép hàng năm khoảng 14-15%. Tuy nhiên, đây cũng trở thành mảnh đất màu mỡ cho sự phát triển của tội phạm lừa đảo, gây ra thiệt hại tài chính đáng kể cho các nền kinh tế. Hội nghị thượng đỉnh về chống lừa đảo toàn cầu được tổ chức vào tháng 10/2023 đã công bố kết quả khảo sát cho thấy, hơn 1/4 số người được hỏi trên khắp thế giới bị mất tiền vì lừa đảo hoặc đánh cắp danh tính vào năm 2022, thiệt hại tài chính lên tới 1.026 nghìn tỷ USD (khoảng 24.000 triệu tỷ đồng). Cuộc khảo sát trên cũng nhấn mạnh thực trạng chung là việc trình báo các vụ lừa đảo là khá ít với chưa tới 40% số người bị lừa đảo trình báo sự việc của mình cho cảnh sát hoặc cơ quan Chính phủ

khác. Gần 1/4 số người được khảo sát cảm thấy việc trình báo một vụ lừa đảo sẽ không tạo ra sự khác biệt. Lừa đảo chuyển tiền qua tài khoản đã và đang trở thành mối đe dọa mạng cao nhất và cấp bách nhất ở các khu vực trên toàn thế giới. Nhiều quốc gia đã công bố số liệu về số vụ lừa đảo và giá trị lừa đảo gia tăng mạnh mẽ chỉ trong thời gian ngắn. Những báo cáo từ các quốc gia phơi bày bản chất không biên giới, không ngừng nghỉ của tội phạm lừa đảo. Thiệt hại mà tội phạm này gây ra là rất lớn, nạn nhân thường bị tổn thương nghiêm trọng về mặt tinh thần. Trong vài năm tới, lừa đảo chuyển tiền qua tài khoản được dự đoán sẽ tiếp tục gia tăng đáng kể trên khắp thế giới với tổn thất cực lớn. Bài viết tập trung phân tích hình thức lừa đảo chuyển tiền qua tài khoản và đề xuất một số khuyến nghị đối với các cơ quan quản lý nhà nước tại Việt Nam.

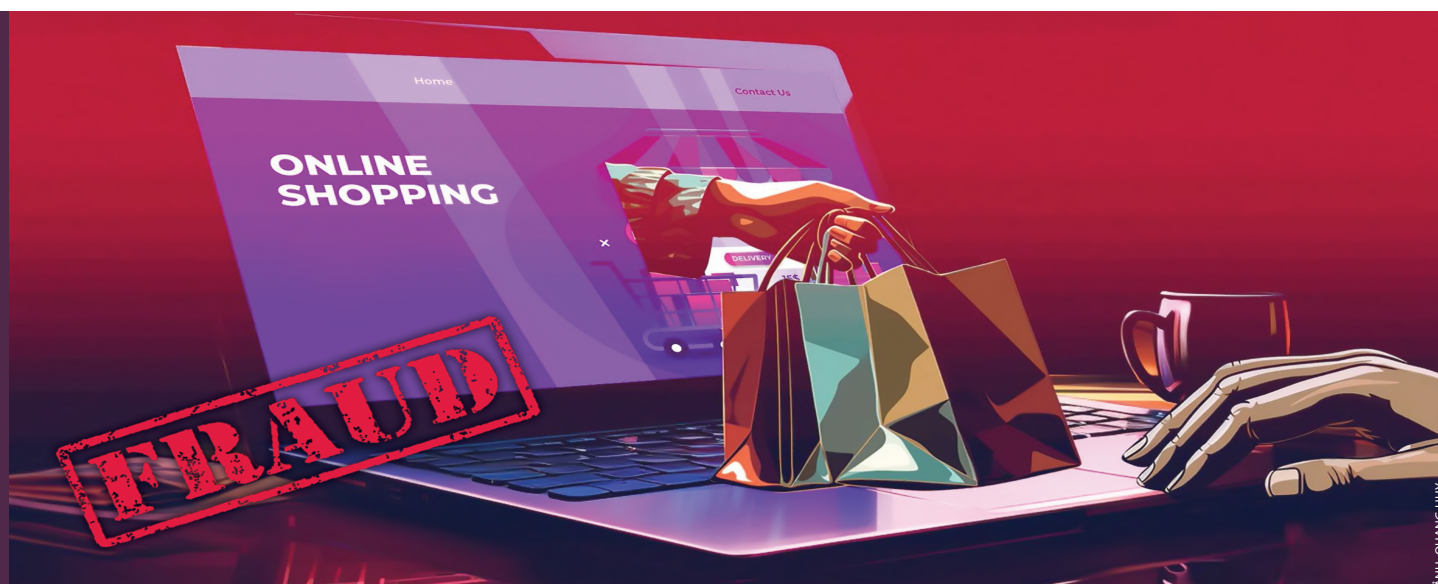
2. TỔNG QUAN VỀ LỪA ĐẢO CHUYỂN TIỀN QUA TÀI KHOẢN

Một thực tế là rất nhiều người dân vẫn chưa phân biệt rõ các trường hợp lừa đảo chuyển tiền. Hiện tại, có thể phân thành 2 hình thức lừa đảo bao gồm:

- Lừa đảo chuyển tiền không có ủy quyền (Unauthorised Fraud) là

khi ai đó đánh cắp thông tin ngân hàng hoặc thông tin cá nhân của nạn nhân và sử dụng chúng để thực hiện giao dịch từ tài khoản của nạn nhân mà họ không biết. Đó là một giao dịch mà nạn nhân không nhận ra. Các hình thức lừa đảo này bao gồm: gian lận thẻ (Card fraud) tức là kẻ lừa đảo có quyền truy cập vào thông tin cá nhân của nạn nhân hoặc đánh cắp thông tin thẻ tín dụng hoặc thẻ ghi nợ của họ; gian lận truy cập từ xa (Remote access fraud) là việc kẻ lừa đảo gọi điện thuyết phục rằng chúng đang gọi từ ngân hàng và cần trợ giúp về sự cố với tài khoản của nạn nhân và yêu cầu nạn nhân cấp quyền truy cập từ xa vào máy tính và yêu cầu đăng nhập vào ngân hàng trực tuyến; gian lận danh tính (Identity fraud) là việc kẻ lừa đảo đánh cắp thông tin cá nhân của nạn nhân để mạo danh họ. Sau đó, chúng rút các khoản vay và thẻ tín dụng đứng tên nạn nhân hoặc rút tiền mặt từ tài khoản ngân hàng của họ.

- Lừa đảo chuyển tiền có ủy quyền hay còn gọi là lừa đảo chuyển tiền qua tài khoản – (Authorised push payment – APP) - là thuật ngữ mô tả một phương thức lừa đảo trong đó tội phạm bằng nhiều thủ đoạn khiến những người dùng hợp pháp thực hiện thanh toán vào tài khoản đích dưới sự kiểm soát của tội



Hầu hết các quốc gia đều đang cho thấy tổn thất lớn từ lừa đảo chuyển tiền qua tài khoản, kể cả các quốc gia phát triển

phạm. Số tiền rời khỏi tài khoản của người dùng hợp pháp sẽ đi qua một hoặc một số tài khoản con la (mule accounts – một loại tài khoản rửa tiền), thường là ở nước ngoài, sau đó tiền sẽ được rút ra hoặc bị chúng chuyển đổi thành tài sản kỹ thuật số khó theo dõi, chẳng hạn như tiền điện tử. Các thuật ngữ khác về hình thức lừa đảo này bao gồm “PIX fraud” ở Brazil, “scams” ở Úc và Singapore, “APP fraud” ở Anh, “bank transfer scam” ở Nhật Bản.

Trong một giao dịch lừa đảo chuyển tiền qua tài khoản, chính chủ tài khoản bị lừa phải chuyển tiền cho một kẻ lừa đảo đóng giả là người nhận thanh toán. Tội phạm sẽ lừa nạn nhân chuyển tiền trực tiếp từ tài khoản của họ đến tài khoản mà chúng kiểm soát. Những kẻ lừa đảo sử dụng các chiến thuật tinh vi để lừa tiền từ các nạn nhân. Chúng lợi dụng các lỗ hổng trong hệ thống trực tuyến hoặc thao túng nạn nhân chuyển tiền cho chúng mà họ không hề nhận ra. Chúng thường yêu cầu nạn nhân chuyển tiền qua chuyển khoản ngân hàng, ứng dụng thanh toán hoặc thẻ ghi nợ trả trước để khiến việc theo dõi giao dịch trở nên khó khăn hơn.

Một số cách thức mà những kẻ lừa đảo thường sử dụng để thực hiện lừa đảo chuyển tiền qua tài khoản như sau:

- Lừa đảo thương mại điện tử/ mua sắm trực tuyến (Purchase scams): Những kẻ lừa đảo đóng giả người mua hoặc người bán trên các thị trường trực tuyến để đánh lừa nạn nhân. Những kẻ lừa đảo đóng vai là người bán hàng thường thiết lập các cửa hàng trực tuyến giả mạo hoặc đăng các mặt hàng để bán trên các thị trường tin cậy. Những kẻ lừa đảo cũng có thể giả dạng người mua giả, nhằm mục tiêu vào người bán cá nhân trên thị trường trực tuyến. Chúng thường gửi bằng chứng thanh toán giả mạo với số tiền lớn hơn so với tiền hàng, sau đó yêu cầu bên bán chuyển trả lại tiền thừa. Bên bán sau khi chuyển xong mới biết là chúng từ thanh toán là giả.

- Lừa đảo đầu tư (Investment scams): Nạn nhân của các vụ lừa đảo đầu tư thường tìm thấy “cơ hội đầu tư” thông qua tìm kiếm trên internet hoặc qua lời giới thiệu từ bạn bè trực tuyến, sau khi bị lừa hoặc bị lôi kéo bởi những kẻ lừa đảo, họ đã chuyển tiền vào các tài khoản ngân hàng được chỉ định cho “khoản đầu tư” của họ. Để thao túng tâm lý của nạn nhân, những kẻ lừa đảo có xu hướng lôi kéo nạn nhân vào các nhóm trò chuyện thông qua các nền tảng xã hội như Facebook, Instagram, WhatsApp. Trong các nhóm hoặc kênh trò chuyện này, nạn nhân đã

nhận được nhiều thành tích từ các thành viên khác nói rằng họ đã “thu lợi” từ khoản đầu tư như thế, thuyết phục nạn nhân về tính xác thực của khoản đầu tư. Bị cám dỗ bởi những khoản lợi nhuận đã hứa, các nạn nhân sẽ liên hệ với những kẻ lừa đảo. Trước khi nhận được số tiền kiếm được từ “khoản đầu tư” của mình, các nạn nhân đã được những kẻ lừa đảo hướng dẫn chuyển tiền để trả các “phí” khác nhau phát sinh cho việc thực hiện giao dịch.

- Lừa đảo hẹn hò trực tuyến (Romance scams): Những kẻ lừa đảo giả dạng đối tác tiềm năng để lừa tiền đang ngày càng gia tăng, nhằm vào những người cô đơn và dễ bị tổn thương, lợi dụng mong muốn kết nối và đồng hành của nạn nhân. Một khi đã chiếm được lòng tin của nạn nhân, chúng sẽ bày ra nhiều tình huống khẩn cấp về tài chính khác nhau, từ khủng hoảng gia đình cho đến việc kinh doanh thất bại, buộc nạn nhân phải gửi tiền theo cách của chúng.

- Lừa đảo mạo danh (Phishing scams): Đây là hình thức rất phổ biến nhưng nhiều người vẫn bị sập bẫy. Những kẻ lừa đảo mạo danh các tổ chức có uy tín hoặc thậm chí là những người mà nạn nhân tin tưởng để lừa lấy số tiền tích lũy của nạn nhân. Những kẻ lừa đảo này thường có sức thuyết phục đáng kinh ngạc.

+ Mạo danh các cơ quan uy tín như các cơ quan của Chính phủ hoặc ngân hàng, cơ quan thuế để thông báo rằng nạn nhân đang gặp vấn đề nghiêm trọng như bị cáo buộc phạt tiền hoặc những vấn đề tương tự, cần được xử lý ngay lập tức. Nạn nhân sẽ bị lừa phải chuyển tiền cho chúng để tránh các vấn đề pháp lý.

+ Mạo danh một người nào đó mà nạn nhân biết rõ, chẳng hạn như thành viên gia đình hoặc bạn bè. Trong những trường hợp này, chúng thường thêu dệt nên những câu chuyện phức tạp về việc đang gặp khó khăn và cần tiền gấp, dựa vào phản ứng cảm xúc lo lắng tự nhiên của nạn nhân để vượt qua sự hoài nghi thông thường của họ. Những tiến bộ gần đây trong trí tuệ nhân tạo thậm chí còn mang lại cho những kẻ lừa đảo khả năng tái tạo kỹ thuật số giọng nói của người thân bằng cách sử dụng các mẫu tìm thấy trên mạng, càng làm tăng thêm độ tin cậy cho những lời nói dối của chúng.

- Lừa đảo việc làm (Job scams): Đây là một loại lừa đảo đặc biệt xảo quyệt, lợi dụng hy vọng và nguyện vọng của người tìm việc. Những kẻ lừa đảo việc làm thường đóng giả là các công ty tuyển dụng cung cấp việc làm lương cao từ các thương hiệu nổi tiếng. Chúng cũng có thể tạo các tin tuyển dụng giả trên các nền tảng việc làm hợp pháp để thu hút những người đang tìm việc. Đối với những trò lừa đảo công việc phức tạp hơn, chúng thậm chí có thể trả tiền cho nạn nhân khi họ hoàn thành một số nhiệm vụ đơn giản đầu tiên. Khi đã có được sự tin tưởng của nạn nhân rằng đó không phải là một trò lừa đảo, chúng sẽ yêu cầu các khoản thanh toán trả trước lớn hơn trước khi biến mất cùng với số tiền đó. Nạn nhân chỉ phát hiện ra công việc đó là giả mạo sau khi tiền đã được chuyển khỏi tài khoản.

3. THỰC TRẠNG LỪA ĐẢO CHUYỂN TIỀN QUA TÀI KHOẢN Ở MỘT SỐ QUỐC GIA

Hầu hết các quốc gia đều đang cho thấy tổn thất lớn từ lừa đảo chuyển tiền qua tài khoản, kể cả các quốc gia phát triển. Những thiệt hại được báo cáo thực tế từ nạn nhân không thể hiện được bức tranh toàn cảnh, nghĩa là con số thiệt hại thực tế lớn hơn nhiều. Tuy vậy, những số liệu đó đã xác nhận rằng bọn tội phạm đang đạt được rất nhiều thành công khi lừa các nạn nhân rơi vào bẫy lừa đảo.

3.1. Anh

Anh từ lâu đã là điểm đến hấp dẫn của những kẻ lừa đảo chuyển tiền qua tài khoản. Sự phổ biến của ngôn ngữ tiếng Anh, tốc độ số hóa nhanh chóng và sự dễ dàng thành lập công ty, cùng như hệ thống thanh toán nhanh, cho phép chuyển khoản gần như ngay lập tức giữa các tài khoản ngân hàng đều được coi là những lý do giải thích cho điều này. Tốc độ thanh toán ở Anh làm giảm khả năng ngân hàng phát hiện và thu hồi số tiền bị đánh cắp. Lừa đảo được xem là một trong 10 mối đe dọa tội phạm có tổ chức và nghiêm trọng hàng đầu đối với Anh. Trong 10 năm qua, đây là loại tội phạm mà một cá nhân có nhiều khả năng gặp phải nhất ở Anh, chiếm hơn 40% tổng số tội phạm. Bộ Tài chính Anh lần đầu tiên công bố số liệu thống kê về hình thức lừa đảo hiện đại này vào năm 2017 và ghi nhận 43.875 trường hợp với tổng thiệt hại là 236 triệu Bảng Anh (khoảng 7.100 tỷ đồng). Sự gia tăng này có mối liên hệ chặt chẽ với quá trình số hóa ngày càng tăng và sự phổ biến của truyền thông xã hội. Theo UK Finance (Hiệp hội thương mại của Anh về dịch vụ tài chính và ngân hàng) báo cáo trong năm 2023 có đến 222.694 vụ lừa đảo chuyển tiền qua tài khoản ở Anh và xứ Wales với thiệt hại 376,4 triệu Bảng Anh (khoảng 11.000 tỷ đồng), cho thấy sự gia tăng nhanh chóng. Trong đó, lừa đảo đầu tư chiếm tỷ trọng lớn nhất trong số các loại lừa đảo chuyển tiền qua tài khoản tại Anh. Theo điều tra của tổ chức UK Finance cho thấy, 81% người dân nói rằng họ tự tin có

thể xác định được lừa đảo, mặc dù chưa đến một nửa nhận thức được ngay cả những hành vi lừa đảo phổ biến nhất. Thiệt hại ngày càng gia tăng của người dân đã thúc đẩy thị trường hướng tới các quy định pháp lý, buộc các tổ chức tài chính phải bồi thường cho các nạn nhân bị lừa đảo. Vào tháng 6/2023, Dự luật Thị trường và Dịch vụ Tài chính của Anh có hiệu lực, yêu cầu các ngân hàng bồi hoàn cho các nạn nhân của các vụ lừa đảo chuyển tiền qua tài khoản. Tổng số tiền được trả lại cho nạn nhân thông qua khoản hoàn trả trực tiếp từ ngân hàng của họ hoặc thông qua việc thu hồi tiền từ tài khoản người thụ hưởng năm 2023 là 256,4 triệu Bảng, đạt mức hơn 68%. Việc hoàn trả cho nạn nhân bị lừa đảo chuyển tiền qua tài khoản rất phức tạp vì nó liên quan đến việc nạn nhân vô tình thực hiện thanh toán. Tỷ lệ hoàn trả đã tăng ở hầu hết các loại lừa đảo này vào năm 2023 tại Anh. Năm 2023, Anh ban hành “Chiến lược chống lừa đảo” với trọng tâm là phòng ngừa và mong muốn chặn lừa đảo ngay từ nguồn, chẳng hạn như yêu cầu một số công ty truyền thông xã hội lớn phải hành động nhiều hơn để ngăn chặn gian lận bắt nguồn trên nền tảng của họ, kể cả các ngân hàng, công ty viễn thông và công ty công nghệ. UK Finance cũng chỉ ra rằng 76% lừa đảo chuyển tiền qua tài khoản bắt nguồn từ nền tảng trực tuyến và 16% nữa bắt nguồn từ viễn thông trong năm 2023. Các công ty này cũng phải đóng vai trò của mình để trấn áp dòng tiền chảy vào tay tội phạm. UK Finance cho rằng, việc ngành dịch vụ tài chính phải gánh chịu những chi phí phát sinh từ việc các ngành khác không giải quyết thỏa đáng các rủi ro lừa đảo của chính họ là không công bằng. Vào tháng 10/2024, chính sách hoàn trả bắt buộc đối với tất cả nạn nhân của vụ lừa đảo chuyển tiền qua tài khoản của Cơ quan quản lý hệ thống thanh toán của Anh được ban hành, thay vì chỉ áp dụng trong các trường hợp nạn nhân sơ suất nghiêm trọng, có thể dẫn đến sự thay đổi

trong cách thức hoạt động của những kẻ lừa đảo. Một mặt, điều này mang lại cho người dân sự yên tâm rằng, nếu họ là mục tiêu của bọn tội phạm thuộc loại lừa đảo này, cuối cùng họ sẽ không bị mất tiền. Mặt khác, sự tự mãn của người dân sẽ dẫn đến hệ quả là số vụ lừa đảo tăng lên.

Cơ quan quản lý hệ thống thanh toán (PSR) của Anh được thiết lập để xem xét lại các tiêu chuẩn về trách nhiệm pháp lý đối với tổn thất do lừa đảo. Những thay đổi này sẽ buộc cả ngân hàng chuyển và nhận đều phải chịu trách nhiệm như nhau trong việc hoàn trả cho khách hàng trong trường hợp giao dịch lừa đảo, các hướng dẫn rõ ràng hơn sẽ xác định các tình huống trong đó khách hàng không có sự quan tâm đầy đủ từ phía ngân hàng và chứng minh được sự sơ suất của ngân hàng. Anh vẫn là quốc gia duy nhất cho đến hiện tại áp dụng phương pháp hoàn trả 100% cho các trường hợp bị lừa đảo chuyển tiền qua tài khoản. Tuy nhiên, Anh sẽ không đơn độc trong nỗ lực này bởi vì Liên minh châu Âu đã công bố kế hoạch ban hành Chỉ thị dịch vụ thanh toán (PSD3) và Quy định dịch vụ thanh toán (PSR1) mới, trong đó cũng sẽ ưu tiên bảo vệ tốt hơn cho các nạn nhân bị lừa đảo và phân bổ phần trách nhiệm pháp lý lớn hơn cho các tổ chức tài chính.

3.2. Singapore

Mức thu nhập bình quân đầu người cao hơn đáng kể so với mức trung bình toàn cầu, khiến Singapore trở thành mục tiêu của những kẻ lừa đảo. Tại Singapore đã ghi nhận về số vụ lừa đảo chuyển tiền qua tài khoản là 46.563 trường hợp trong năm 2023, nhiều nhất là các vụ lừa đảo việc làm với 9.914 trường hợp; lừa đảo thương mại điện tử đứng thứ hai với 9.783 trường hợp. Xét về mặt thiệt hại thì lừa đảo đầu tư dẫn đến tổn thất tài chính cao nhất, tổng trị giá 204,5 triệu đô la Singapore (SGD) (khoảng hơn 3.600 tỷ đồng), tiếp theo là các vụ lừa đảo việc làm với số tiền thiệt hại lên tới 135,7 triệu SGD (khoảng hơn 2.400 tỷ đồng). Tổng thiệt hại được



Tại Singapore đã ghi nhận về số vụ lừa đảo chuyển tiền qua tài khoản là 46.563 trường hợp trong năm 2023

ghi nhận chính thức năm 2023 là 651,8 triệu SGD (khoảng hơn 11.500 tỷ đồng) tương đương 0,1% GDP của Singapore, trong khi năm 2019 con số này là 170,8 triệu SGD, cho thấy tốc độ gia tăng đáng kể của loại hình lừa đảo này.

Tháng 7/2023, Singapore đã thông qua Luật về an ninh trực tuyến, trong đó yêu cầu đối với nền tảng trực tuyến phải áp dụng các biện pháp để bảo vệ người dùng của họ tốt hơn. Đạo luật này cũng trao quyền cho Chính phủ trong một số trường hợp nhất định ra lệnh xóa các trang web và tài khoản trực tuyến bị nghi ngờ được sử dụng cho các mục đích lừa đảo, từ đó chủ động ngăn chặn các hành vi này và hoạt động độc hại trên mạng trước khi nó gây ra nhiều thiệt hại hơn và có thêm nhiều nạn nhân liên quan. Gần đây nhất, ngày 24/10/2024, Cơ quan quản lý tiền tệ Singapore (Monetary Authority of Singapore - MAS) công bố các tổ chức tài chính, công ty viễn thông phải chịu trách nhiệm đối với nạn nhân bị lừa đảo, các tổ chức có 6 tháng để chuẩn bị các biện pháp mới kể từ khi quy định này bắt đầu có hiệu lực vào ngày 16/12/2024. Các ngân hàng phải xác định tài khoản đáng ngờ dựa trên việc số dư giảm nhanh chóng nếu trong cùng một ngày có hơn một nửa số dư bị chuyển khỏi tài khoản (với điều kiện tài khoản đó phải có số dư ít nhất 50.000

SGD tức là khoảng hơn 918 triệu đồng). MAS cũng đưa ra Khung trách nhiệm chung (Shared Responsibility Framework - SRF), trong đó quy định các tổ chức tài chính và công ty viễn thông có thể phải chịu trách nhiệm chia sẻ những tổn thất của nạn nhân trong một số vụ lừa đảo nếu các tổ chức này không thực hiện nhiệm vụ của mình. Nạn nhân có trách nhiệm cung cấp bằng chứng cho thấy tổn thất của họ không phải do sơ suất của chính họ. Nếu các ngân hàng và các công ty viễn thông đã làm những gì cần thiết trong khuôn khổ nhiệm vụ của mình thì nạn nhân trong những trường hợp như vậy sẽ phải chịu toàn bộ tổn thất. Singapore có thể là quốc gia đầu tiên đưa các công ty viễn thông vào khuôn khổ bồi hoàn tổn thất do lừa đảo. Lý do MAS đưa ra SRF là vì họ cho rằng các ngân hàng và nhà cung cấp dịch vụ thanh toán là người giám sát quỹ của người tiêu dùng và đóng vai trò quan trọng như người gác cổng chống lại việc tiền bị kẻ lừa đảo chiếm đoạt, trong khi công ty viễn thông là nhà cung cấp cơ sở hạ tầng cho tin nhắn SMS thường được ngân hàng sử dụng để liên lạc với người dùng. Nhiệm vụ của các công ty viễn thông là giảm nguy cơ gửi SMS lừa đảo đến người tiêu dùng bằng cách chạy bộ lọc chống lừa đảo trên mạng và chặn những mạng có liên kết lừa đảo đã biết, các biện pháp

quản lý việc đăng ký thẻ SIM và cho phép các thuê bao chặn các cuộc gọi và SMS quốc tế. Ngoài ra, các công ty viễn thông chỉ có thể gửi những tin nhắn SMS đến người đăng ký thuê bao nếu chúng bắt nguồn từ một công ty tổng hợp SMS được ủy quyền, hoạt động cho một doanh nghiệp muốn gửi tin nhắn SMS số lượng lớn. Nhưng nếu các công ty viễn thông cũng thực hiện đúng nhiệm vụ của mình, họ sẽ không bị yêu cầu bồi hoàn cho các nạn nhân bị lừa đảo.

Tuy nhiên, phạm vi của SRF chỉ giới hạn ở các hành vi lừa đảo được thực hiện trên nền tảng số, chẳng hạn như một trang web giả mạo được truy cập thông qua một liên kết, trong đó nạn nhân bị lừa nhập chi tiết tài khoản của họ. Các tổ chức bị mạo danh phải có trụ sở tại Singapore hoặc đã cung cấp dịch vụ cho người dân Singapore. Đây không phải là một khuôn khổ hoàn trả toàn diện cho các hành vi lừa đảo như trong trường hợp phát sinh từ lừa đảo chuyển tiền qua tài khoản như lừa đảo đầu tư hoặc lừa đảo khác. Do đó, từ ngày 30/9/2024, Singapore đưa ra luật cho phép cảnh sát quyền tạm thời hạn chế các giao dịch ngân hàng của những đối tượng là mục tiêu của hoạt động lừa đảo, những người không biết rằng họ đang bị lừa. Bộ Nội vụ cho biết, luật được đưa ra trong bối cảnh số vụ lừa đảo liên quan đến việc nạn nhân tự nguyện chuyển tiền cho kẻ lừa đảo vẫn còn cao, bất chấp các biện pháp và nỗ lực giáo dục công chúng về cách phòng tránh. Ngoài ra, Chính phủ Singapore còn thiết lập “Cổng thông tin Chính phủ một cửa” vào tháng 2/2024, trang web này cung cấp thông tin về những gì người dân nên làm nếu cho rằng mình đã trở thành nạn nhân của lừa đảo, cách thức để người dân có thể tự bảo vệ mình cũng như các xu hướng lừa đảo mới nhất nhằm nâng cao nhận thức của người dân. Cổng này cũng cung cấp thông tin về các cơ quan hỗ trợ mà nạn nhân của các vụ lừa đảo có thể liên hệ. Bên cạnh đó, Singapore còn tăng cường các hoạt động giáo

dục cộng đồng thông qua các buổi phỏng vấn truyền thông và các buổi nói chuyện trong trường học để nâng cao nhận thức.

3.3. Úc

Úc là một trong những quốc gia có mức tăng trưởng cao nhất về số vụ lừa đảo chuyển tiền qua tài khoản. Trong năm 2023, Úc ghi nhận tất cả 236.358 trường hợp nạn nhân của lừa đảo chuyển tiền, với tổng thiệt hại lên đến 2,3 tỷ AUD (khoảng 36.400 tỷ đồng). Trong đó, số vụ lừa đảo mạo danh là lớn nhất do đặc thù của Úc có các cộng đồng đa dạng về văn hoá và ngôn ngữ. Tuy nhiên, thiệt hại về vật chất lớn nhất lại đến từ lừa đảo đầu tư, chiếm đến 1,3 tỷ AUD bởi vì giới trẻ ở Úc - đặc biệt là Gen Z - mạo hiểm và liều lĩnh cũng như quá tự tin cho rằng họ có đủ hiểu biết để có thể kiểm soát được mọi thông tin. Phần lớn tổn thất lừa đảo chuyển tiền qua tài khoản bắt nguồn từ mạng xã hội do liên hệ qua Whatsapp (47% tổn thất), Facebook (20%), trang web hẹn hò trực tuyến (9%) và Instagram (9%). Đáng quan ngại, con số thiệt hại năm 2023 đã tăng đáng kể so với năm 2019 khi Úc chỉ ghi nhận 634 triệu AUD thiệt hại trong năm này.

Vào tháng 12/2023, Cơ quan truyền thông của Úc (ACMA) đã bắt đầu giai đoạn thử nghiệm đăng ký ID người gửi SMS. Đây là một phần trong sáng kiến “Chống lừa đảo” của Chính phủ. Theo đó, cơ quan đăng ký sẽ bảo vệ các tiêu đề tin nhắn chữ-số (tên doanh nghiệp rút ngắn) của các thương hiệu và cơ quan Chính phủ, sau đó tập trung vào các thương hiệu từng là mục tiêu của các vụ lừa đảo mạo danh. Các nhà cung cấp dịch vụ viễn thông báo cáo đã chặn hơn 246,7 triệu cuộc gọi lừa đảo và hơn 106,7 triệu tin nhắn SMS lừa đảo trong khoảng thời gian từ tháng 10 – 12/2023 theo các quy tắc đã đăng ký của ACMA. Đồng thời, các công ty này cũng kiểm tra tính tuân thủ của các công ty tổng hợp SMS (nhà cung cấp dịch vụ viễn thông gửi SMS số lượng lớn) để xác định các vấn đề tiềm ẩn có thể khiến các nhà mạng của Úc

gặp nguy cơ lừa đảo.

Úc cũng đã xem xét các kế hoạch chia sẻ tổn thất do lừa đảo. Dự thảo luật đưa ra các quy định nghĩa vụ mạnh mẽ thúc đẩy hành động chống lừa đảo, bao gồm các hình phạt cứng rắn đối với việc không tuân thủ quy định về giải quyết tranh chấp để bồi thường cho nạn nhân. Bộ trưởng Bộ Tài chính chỉ định ngân hàng, công ty viễn thông, nhà cung cấp dịch vụ nền tảng kỹ thuật số phải thực hiện các bước hợp lý để ngăn chặn hoạt động lừa đảo tiếp cận hoặc ảnh hưởng đến người dùng trên các dịch vụ của họ. Bộ trưởng Tài chính có thể sử dụng cơ chế chỉ định để chỉ định thêm các lĩnh vực và cơ quan quản lý có liên quan vào khuôn khổ này theo thời gian khi hoạt động lừa đảo thay đổi, tuy nhiên họ đang cân nhắc xem xét, tính hiệu quả của các sáng kiến ngành hiện có, lợi ích của người dùng và mọi hậu quả (bao gồm cả lợi ích và rủi ro) của việc chỉ định. Cụ thể hơn là tập trung vào việc triển khai các hệ thống và quy trình mạnh mẽ nhằm ngăn chặn những kẻ lừa đảo truy cập hoặc sử dụng nền tảng của tổ chức đó để duy trì hoạt động lừa đảo. Đồng thời, các tổ chức này có nghĩa vụ thực hiện các bước hợp lý để phát hiện các hành vi lừa đảo, bao gồm việc xác định kịp thời những người dùng đang hoặc có thể bị ảnh hưởng bởi một hành vi lừa đảo. Ngoài ra, cơ quan quản lý phải thực hiện các bước hợp lý để ngăn chặn các hành vi lừa đảo bị nghi ngờ đang diễn ra nhằm ngăn chặn tổn thất hoặc tổn thất thêm cho người dùng như làm gián đoạn các hoạt động lừa đảo trước khi nó được thực hiện thành công.

3.4. Nhật Bản

Theo Cơ quan Cảnh sát Quốc gia Nhật Bản (National Police Agency - NPA), tình trạng lừa đảo chuyển tiền qua tài khoản ngân hàng gia tăng nhanh với hơn 15 tỷ JPY bị tổn thất (tương đương khoảng 2.500 tỷ đồng) chỉ trong nửa đầu năm 2023. Lừa đảo mạo danh vẫn là hình thức lừa đảo hàng đầu ở Nhật Bản, tiếp theo là lừa đảo đầu tư, trong đó những kẻ lừa

đào chủ yếu sử dụng chuyển khoản ngân hàng (bank transfer) và chuyển khoản trực tuyến (wire transfer) để chiếm đoạt tiền từ nạn nhân. Nạn nhân chủ yếu thuộc nhóm trên 65 tuổi, chiếm đến hơn 87% số vụ việc. Tình trạng già hoá dân số ở Nhật Bản là vấn đề dẫn đến hình thức lừa đảo mạo danh ngày càng nhiều, do sự di cư về đô thị, gặp gỡ ít nên việc nhiều người lớn tuổi không còn nhận ra giọng nói của cháu mình và khiến họ không thể đặt câu hỏi nghi ngờ với các đối tượng lừa đảo. Số vụ việc ngày càng gia tăng khiến NPA đã phải thành lập một đơn vị mới để trấn áp các vụ lừa đảo nhắm vào người cao tuổi ở Nhật Bản. Kế hoạch đưa ra sau khi thảo luận với các ngân hàng là sẽ khoá thẻ ATM của những người trên 65 tuổi. Vấn đề này vấp phải rất nhiều phản ứng vì 29% người Nhật trên 65 tuổi, nếu loại trừ dịch vụ đối với những người này sẽ khiến các ngân hàng cũng như nền kinh tế bị ảnh hưởng lớn. Theo báo cáo của Liên minh chống lừa đảo toàn cầu (Global Anti-Scam Alliance), tình trạng lừa đảo ở Nhật Bản năm 2024 đạt đến điểm khủng hoảng khi có 71% người Nhật được hỏi cho biết đã gặp phải các vụ lừa đảo ít nhất một lần mỗi tháng, tăng 8% so với năm 2023. Trong đó, 87% nạn nhân không báo cáo vụ việc cho các cơ quan chức năng, 37% số người được hỏi vẫn bày tỏ sự thiếu tin tưởng vào khả năng nhận diện bẫy lừa đảo của chính mình. Nhật Bản đã thông qua các biện pháp mới nhằm chống lại tình trạng này bao gồm yêu cầu nghĩa vụ của các công ty truyền thông, nhà cung cấp dịch vụ internet, công ty viễn thông và tổ chức tài chính. Để chống lại sự gia tăng ngày càng nhanh của các quảng cáo lừa đảo trên mạng xã hội, các nền tảng truyền thông xã hội sẽ phải nâng cao quy trình sàng lọc quảng cáo. Chiến lược toàn diện của Chính phủ Nhật Bản bao gồm yêu cầu các công ty truyền thông xã hội phát triển các tiêu chuẩn sàng lọc rõ ràng và tăng cường quy trình xác minh để đảm bảo quảng cáo đáp ứng

các tiêu chuẩn này. Chính phủ cũng kêu gọi các hành động nhanh chóng để loại bỏ bất kỳ quảng cáo nào bị phát hiện là lừa đảo và đang đặt ra các nguyên tắc nghiêm ngặt để ngăn chặn những quảng cáo dẫn đến các cuộc trò chuyện nhóm, vốn được xác định là một lĩnh vực rủi ro đáng kể. Nhật Bản cũng đang thúc đẩy việc sử dụng thẻ định danh cá nhân My Number để ký hợp đồng điện thoại di động, tăng cường bảo mật bằng cách sử dụng các phương pháp xác minh điện tử để đọc thông tin chip IC, mục đích là xác minh nghiêm ngặt danh tính người dùng.

3.5. Mỹ

Theo dữ liệu liên bang, các khoản thiệt hại do lừa đảo chuyển tiền qua tài khoản tăng vọt gần 150% trong khoảng thời gian chỉ 2 năm lên tới 1,9 tỷ USD vào năm 2023, trong đó lừa đảo mạo danh là phổ biến nhất. So với các nước châu Âu, thị trường thanh toán theo thời gian thực (real-time) của Mỹ chưa phát triển bằng, trong đó mạng thanh toán Zelle là lớn nhất, cho phép thanh toán ngay lập tức cho các khách hàng của các ngân hàng. Người dân thực hiện chuyển nhanh hàng tỷ đô la mỗi ngày cho nhau trên ứng dụng Zelle và các ứng dụng thanh toán khác để làm mọi việc như mua sắm và thanh toán hóa đơn. Tốc độ và sự tiện lợi

của các nền tảng thanh toán này đã đồng thời khiến chúng trở nên cực kỳ phổ biến và trở thành thời nam châm thu hút những kẻ lừa đảo mạo danh. Kẻ lừa đảo thường giả làm người chăn nuôi chó, người bán vé, các cơ quan Chính phủ hoặc các dịch vụ hợp pháp khác. Bằng việc hợp tác với các tổ chức tài chính lớn, Zelle đã tạo cho nhiều người dùng ấn tượng rằng thanh toán qua ứng dụng cũng an toàn như thanh toán được ngân hàng hỗ trợ trực tiếp. Một cuộc điều tra của Mỹ ước tính rằng, đến năm 2021, người dùng Zelle đã mất tới 440 triệu USD vì nhiều hình thức lừa đảo khác nhau. Nạn nhân thường rất khó lấy lại tiền đã chuyển cho những kẻ lừa đảo. Các ngân hàng lớn vận hành Zelle hiếm khi hoàn trả cho những khách hàng là nạn nhân bị lừa đảo. Phía ngân hàng cung cấp ứng dụng Zelle cho biết trên trang web của họ rằng: “Ngay cả khi nạn nhân bị lừa ủy quyền thanh toán cho hàng hóa hoặc dịch vụ mà ai đó nói rằng họ sẽ cung cấp nhưng họ không thực hiện điều đó, thì đây sẽ bị coi là một trò lừa đảo”, nhưng bởi vì nạn nhân đã ủy quyền thanh toán nên có thể không lấy lại được tiền của mình. Cho đến gần đây, Zelle cũng không đưa ra biện pháp bảo vệ nào trước các khoản thanh toán được ủy quyền thực hiện do lừa đảo. Chỉ sau khi số lượng nạn nhân



Một cuộc điều tra của Mỹ ước tính rằng, đến năm 2021, người dùng Zelle đã mất tới 440 triệu USD vì nhiều hình thức lừa đảo khác nhau

lừa đảo tăng lên và cùng với đó là áp lực từ các nhà lập pháp thì các ngân hàng trong mạng Zelle mới bắt đầu bồi thường cho các nạn nhân của các vụ lừa đảo mạo danh.

Trong báo cáo tháng 10/2022, Ủy ban về Lừa đảo Kỹ thuật số của Hạ viện cho rằng, việc xem nhẹ vấn đề này đã tạo ra một nền văn hóa dễ dãi trong Chính phủ và các cơ quan thực thi pháp luật đối với lừa đảo và những tên tội phạm gây ra hành vi đó, điều này được thể hiện rõ qua phản ứng mờ nhạt của các cơ quan quản lý trước mối đe dọa của hình thức lừa đảo này. Tội phạm thực hiện hành vi lừa đảo chuyển tiền qua tài khoản bằng cách lấy mã chuyển khoản hợp lệ, thường thông qua việc lừa đảo hoặc thao túng khách hàng, vì dữ liệu hợp pháp nên các ngân hàng có thể khẳng định việc chuyển tiền đã được ủy quyền và thực hiện chính xác, khiến nạn nhân không thể yêu cầu hoàn trả. Mối đe dọa từ hình thức lừa đảo này đã thúc đẩy Ủy ban Thượng viện Mỹ về ngân hàng, nhà ở và đô thị phải gửi thông báo tới người đứng đầu của các ngân hàng lớn bao gồm CEO của JPMorgan Chase, Bank of America, Wells Fargo và Citibank. Thông báo này trích dẫn số liệu của một báo cáo cho thấy, người tiêu dùng đã mất 10 tỷ USD do lừa đảo trực tuyến nói chung vào năm 2023. Trong đó, nhiều nạn nhân của lừa đảo chuyển tiền qua tài khoản không bao giờ được hoàn tiền và vấn đề ngày càng gia tăng nghiêm trọng. Chính điều này đã thúc đẩy Ủy ban Thượng viện liên hệ với các ngân hàng nói trên và nêu rõ các hành động mà họ mong đợi các ngân hàng thực hiện. Hiệp hội Ngân hàng Mỹ cho biết, đang nghiên cứu một chương trình phối hợp liên lạc theo thời gian thực giữa các ngân hàng để phát hiện tốt hơn các hoạt động đáng ngờ và giảm dòng tiền bị đánh cắp khỏi tài khoản.

Việc bồi thường cho nạn nhân của các vụ lừa đảo mạo danh gửi tiền qua Zelle đặt ra tiền lệ quan trọng ở Mỹ. Đây sẽ là một bước tiến lớn. Hiện tại, các ngân hàng, tổ chức tín

dụng và các tổ chức khác chỉ phải bồi thường cho nạn nhân bị lừa đảo nếu các khoản thanh toán không được ủy quyền. Chẳng hạn như Cash App tuyên bố không cung cấp tính năng hoàn tiền cho các khoản thanh toán được ủy quyền. Mặc dù “Quy định E” - còn được gọi là Đạo luật chuyển tiền điện tử - đã chỉ đạo các tổ chức tài chính bảo vệ khách hàng trong trường hợp giao dịch lừa đảo, nhưng điều đó không áp dụng cho chuyển tiền có ủy quyền. Các cơ quan quản lý tại Mỹ đang đề xuất đưa ra luật mới nhằm tìm cách trấn áp các hành vi lừa đảo thanh toán bằng cách thu hẹp các lỗ hổng trong luật hiện hành. Dự luật này được cho là có thể phải đối mặt với sự phản đối của ngành Ngân hàng.

3.6. Thái Lan

Bắt đầu từ tháng 5/2024, Thái Lan tiến hành một quy trình xác minh dữ liệu toàn diện để xác định và giải quyết các “SIM ma” và các tài khoản ngân hàng lừa đảo gây ra mối đe dọa đáng kể đối với an ninh tài chính nhưng vẫn đảm bảo các hoạt động giao dịch hàng ngày của người dân. Động thái này cho thấy quyết tâm của Chính phủ Thái Lan trong việc tạo ra một môi trường kỹ thuật số an toàn cho mọi công dân. Những cá nhân sở hữu từ 6 đến 100 thẻ SIM cho mỗi công ty điện thoại di động vẫn cần xác minh danh tính của mình và phải thực hiện việc này tại các trung tâm dịch vụ hoặc thông qua các phương thức do nhà mạng điện thoại di động chỉ định trước tháng 7/2024. Chỉ thị này do Ủy ban Phát thanh và Truyền hình Quốc gia thực hiện, nhằm mục đích đảm bảo tất cả các thẻ SIM đang lưu hành đều được liên kết với người dùng hợp pháp và đã được xác minh, từ đó giảm nguy cơ lạm dụng. Thiệt hại do tội phạm lừa đảo chuyển tiền qua tài khoản gây ra trong tháng 8/2024 tại Thái Lan ở mức 75 triệu THB mỗi ngày (khoảng 50 tỷ đồng), giảm 36% so với mức 116 triệu THB mỗi ngày (khoảng 75 tỷ đồng) trong khoảng thời gian từ tháng 1 đến tháng 6.

Từ tháng 11/2023 đến tháng 8/2024, trung tâm Anti Online Scam Operation Center (AOC) của Thái Lan đã nhận được 985.538 cuộc gọi, tương đương trung bình 3.231 cuộc gọi mỗi ngày. Nạn nhân của tội phạm lừa đảo chuyển tiền qua tài khoản có thể yêu cầu sự hỗ trợ hữu ích từ Trung tâm để nhanh chóng đóng băng tài khoản của họ, giảm thiểu tổn thất tài chính và ngăn chặn tội phạm thực hiện các giao dịch tiếp theo. Chỉ trong tháng 7/2024, AOC cũng đình chỉ 920.694 tài khoản con la, 16.279 trang web trái phép, thu hồi 71.122 “SIM lã” (mule SIM cards). Nạn nhân có thể gọi đến đường dây nóng AOC 1441 để báo cáo vụ lừa đảo và nhận lời khuyên về cách được bảo vệ khỏi tội phạm này và kiểm soát thiệt hại sau khi bị lừa đảo. AOC đang là giải pháp toàn diện cho người dân tại quốc gia này nhằm ngăn chặn tội phạm lừa đảo chuyển tiền qua tài khoản nói riêng và tội phạm lừa đảo trực tuyến nói chung.

Chính phủ Thái Lan cũng đã đề xuất một luật mới nhằm đối phó với sự gia tăng nhanh chóng thời gian gần đây của loại tội phạm này, đồng thời giúp nạn nhân phục hồi các tổn thất tài chính. Bộ Kinh tế và Xã hội số (Ministry of Digital Economy and Society) chịu trách nhiệm soạn thảo luật này. Dự kiến sẽ tăng án tù cho những kẻ lừa đảo từ 1 năm lên 5 năm; thực hiện các biện pháp phòng ngừa bổ sung để ngăn chặn việc chuyển tiền bất hợp pháp thông qua tài sản kỹ thuật số; tăng cường luồng thông tin giữa các cơ quan Chính phủ; khuyến nghị các biện pháp vượt qua trở ngại trong việc truy tìm số tiền bị lừa đảo và trả lại cho nạn nhân.

4. MỘT SỐ KHUYẾN NGHỊ

Làn sóng tội phạm được dự đoán sẽ trở nên tồi tệ hơn khi dân số già hóa và sự phát triển của trí tuệ nhân tạo (AI) khiến việc thực hiện lừa đảo trở nên dễ dàng và việc truy tìm dấu vết tội phạm trở nên khó khăn hơn bao giờ hết. Các kẻ lừa đảo thường nhắm

vào các quốc gia có thu nhập bình quân đầu người cao nhằm hưởng lợi trên mỗi nạn nhân cao hơn so với nhiều quốc gia khác. Tuy nhiên, gần đây hoạt động này có xu hướng mở rộng trên phạm vi toàn cầu. Lừa đảo chuyển tiền qua tài khoản thường là một sự kiện thay đổi cuộc sống vì nó có thể xóa sạch tiền tiết kiệm của người dân hoặc gây thiệt hại không thể khắc phục được về tài chính của họ, nạn nhân còn bị tác động tổn thương tinh thần nặng nề. Ngoài ra, những hậu quả từ lừa đảo chuyển tiền làm xói mòn niềm tin của người dân đối với các tổ chức tài chính và giao dịch trực tuyến, khiến tính toàn diện của toàn bộ hệ thống tài chính gặp rủi ro. Tình trạng này đòi hỏi sự quan tâm từ cả khu vực công và tư nhân để ngăn chặn các thiệt hại kinh tế và xã hội hơn nữa. Cần có nhận thức đúng về hình thức lừa đảo này để bảo đảm an toàn cho thị trường tài chính và cho cả người dân. Tại Việt Nam, chưa có báo cáo chính thức nào về con số tổn thất do lừa đảo chuyển tiền qua tài khoản. Theo khảo sát từ Statista năm 2023, trong số những người dùng mạng tại Việt Nam thì tỷ lệ người bị lừa đảo mạo danh là 18,91%. Thiệt hại tài chính do lừa đảo gây ra khá lớn, ảnh hưởng đến cả tinh thần của nạn nhân. Nhiều nạn nhân không báo cáo vụ lừa đảo cho cơ quan thực thi pháp luật với lý do như sự không chắc chắn hoặc quy trình báo cáo phức tạp. Việc xác thực mạnh đối với tài khoản và việc giới hạn số tiền chuyển chỉ có thể ngăn chặn tình trạng tài khoản của khách hàng bị xâm nhập, tuy nhiên chưa thể ngăn chặn hiệu quả đối với tình trạng lừa đảo chuyển tiền qua tài khoản khi nạn nhân trực tiếp thực hiện hành vi chuyển tiền vì bị những kẻ lừa đảo thao túng.

Phối hợp liên ngành: Những nỗ lực hiện tại của các cơ quan quản lý trong việc chống lại những kẻ lừa đảo chuyển tiền qua tài khoản đang thiếu sự đồng bộ và sự phối hợp. Những kẻ lừa đảo không thể làm điều này một mình. Chúng lợi dụng các hoạt động

kinh doanh hợp pháp, chẳng hạn như viễn thông, công nghệ, internet, truyền thông xã hội và các doanh nghiệp thương mại điện tử để thực hiện các hoạt động lừa đảo và nhắm mục tiêu vào các kênh thanh toán của nạn nhân. Chúng cũng hợp tác với những kẻ rửa tiền và sử dụng các khoản thanh toán nhanh để tăng tốc độ chuyển tiền và hoạt động ngân hàng xuyên biên giới nhằm khiến việc theo dõi và truy vết các khoản tiền lừa đảo trở nên khó khăn hơn. Sự xuất hiện của AI là một thách thức quan trọng trong các cuộc chiến chống lừa đảo. Khi các kẻ lừa đảo bắt đầu lợi dụng AI, số lượng khách hàng bị lừa sẽ tăng lên. AI có thể tạo ra hình ảnh, tập lệnh, video và giọng nói chỉ trong vài giây. Trong tương lai, cuộc chiến chống lừa đảo đòi hỏi khả năng thích ứng, hợp tác và cảnh giác thường xuyên. Do vậy, để giải quyết mối đe dọa lừa đảo đang gia tăng một cách có hiệu quả, tận gốc thì cần thiết phải có hành động phối hợp về các giải pháp, kỹ thuật và dữ liệu thông minh chia sẻ giữa các cơ quan chính phủ, các tổ chức tài chính, công ty viễn thông và nhà cung cấp công nghệ. Các ngân hàng, trang thương mại điện tử, các công ty viễn thông cần nâng cao trách nhiệm trong việc ngăn ngừa tội phạm lừa đảo chuyển tiền thông qua nền tảng mà họ cung cấp cho khách hàng. Mặc dù có thể gây ra một số bất tiện nhưng những biện pháp như vậy là cần thiết để giúp ngăn chặn lừa đảo và bảo vệ khách hàng. Các cơ quan quản lý cũng nên xem xét về nghĩa vụ đối với các công ty có liên quan khác như viễn thông, công nghệ và các hoạt động kinh doanh kỹ thuật số khác tạo điều kiện cho hoạt động lừa đảo chuyển tiền. Tội phạm sẽ luôn thích nghi và lừa đảo sẽ không bao giờ biến mất, nhưng bằng cách hợp tác giữa các ngành sẽ chủ động ngăn chặn mối đe dọa và khiến việc tiến hành lừa đảo trở nên khó khăn hơn.

Trách nhiệm pháp lý đối với các thiệt hại do lừa đảo chuyển tiền qua tài khoản: Trong lừa đảo chuyển tiền qua tài

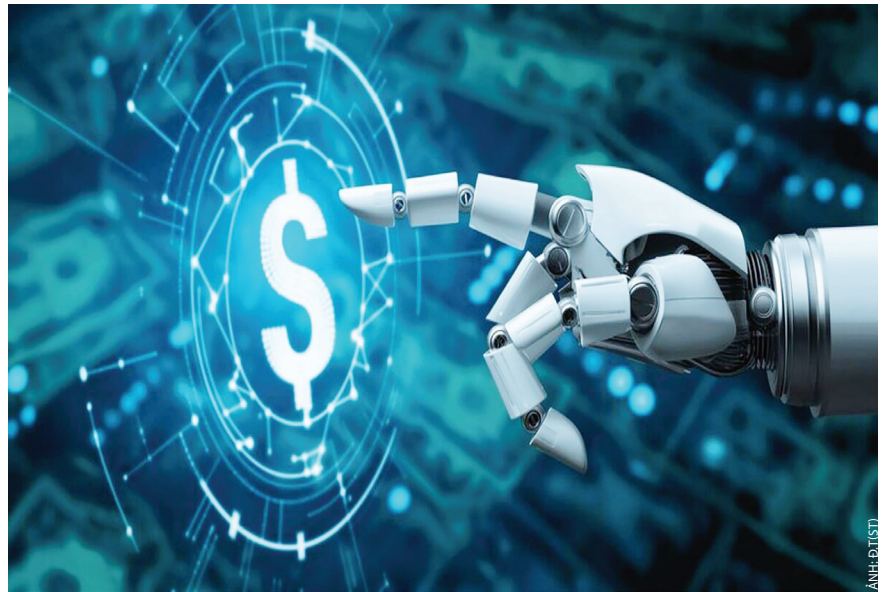
khoản, số tiền thiệt hại lớn hơn đáng kể so với hành vi trộm cắp thẻ tín dụng trong hầu hết các trường hợp. Những kẻ lừa đảo dĩ nhiên là mục tiêu đầu tiên của cơ quan thực thi pháp luật để thu hồi số tiền bị tổn thất của nạn nhân. Sau đó, tùy thuộc vào bối cảnh và hành vi đã xảy ra, nạn nhân và/hoặc người thứ 3 có thể phải chịu trách nhiệm đóng góp toàn bộ hoặc một phần vào việc bù đắp tổn thất. Tuy nhiên, có sự khác nhau giữa các khu vực, quốc gia và thậm chí cả ngân hàng và nhà cung cấp dịch vụ thanh toán vì mỗi khu vực pháp lý hoặc tổ chức có thể có các quy định và hướng dẫn riêng nhằm bảo vệ người dùng, giao dịch tài chính và trách nhiệm pháp lý về lừa đảo. Nhiều vấn đề cần cân nhắc khi đưa ra các quy định pháp lý vì nó có thể tạo ra những hậu quả không lường trước được, chẳng hạn như nếu sự đền bù tổn thất cao từ phía bên thứ 3 sẽ khiến cho việc gia tăng lừa đảo và khả năng xảy ra tương tự trong tương lai. Hoặc vì trách nhiệm bồi thường cao mà các bên cung cấp dịch vụ sẽ tìm cách để ngăn chặn và giảm tình trạng lừa đảo như hạn chế quyền truy cập vào các sản phẩm và điều này có thể ảnh hưởng xấu tới nền kinh tế. Sự thay đổi trách nhiệm pháp lý đối với hành vi lừa đảo được thực hiện thông qua các khoản thanh toán được ủy quyền là một vấn đề mang tính thời sự. Với động thái ở một số quốc gia trong thời gian gần đây, các cơ quan quản lý tại Việt Nam cũng cần xem xét cân nhắc trong việc chia sẻ trách nhiệm đối với các thiệt hại do lừa đảo chuyển tiền.

Dự báo, cảnh báo và giáo dục người dân về lừa đảo chuyển tiền qua tài khoản: Mức độ phổ biến của các mối loại lừa đảo sẽ khác nhau giữa các quốc gia, tùy thuộc vào chu kỳ kinh tế, nhận thức về rủi ro lừa đảo cũng như mức độ kiểm soát và ứng phó của những cơ quan quản lý. Các cơ quan quản lý và cơ quan thực thi pháp luật cần có những hành động khẩn cấp, quyết liệt để giải quyết những bầy lừa đảo này theo cách tiếp cận đa hướng, góp phần tạo

niềm tin chung vào hệ sinh thái thanh toán kỹ thuật số.

Chính phủ cần có tầm nhìn xa trước các mối đe dọa ngày càng tăng trong bối cảnh kỹ thuật số, giải quyết các lỗ hổng tiềm ẩn trước khi chúng có thể bị khai thác, đảm bảo rằng các rủi ro không làm lu mờ lợi ích của chuyển đổi kỹ thuật số.

Giáo dục và nâng cao nhận thức của người dân là một công cụ mạnh mẽ trong cuộc chiến chống lại tình trạng lừa đảo chuyển tiền qua tài khoản. Qua khảo sát ở nhiều quốc gia cho thấy, mức độ không chắc chắn cao về các chiến thuật lừa đảo, đặc biệt liên quan đến nội dung do AI tạo ra, đòi hỏi cần giáo dục cộng đồng toàn diện hơn. Do đó, chính phủ nên ưu tiên việc đầu tư vào chiến dịch truyền thông mạnh mẽ hơn nữa thông qua các phương tiện thông tin đại chúng chính thống và các cơ quan chính quyền địa phương nhằm nâng cao nhận thức thường xuyên để tạo điều kiện cho người dân nhận thức được mối đe dọa và các ứng phó tốt nhất để chống lại lừa đảo. Chẳng hạn, vào tháng 1/2023, Singapore đã đưa ra chiến dịch “I Can ACT Against Scams”, “ACT” trong tiêu đề chiến dịch là viết tắt của “Add-Check-Tell” có nghĩa là 3 hành động chính mà các cá nhân nên chủ động thực hiện để bảo vệ bản thân và cộng đồng trước những hành vi lừa đảo chuyển tiền qua tài khoản bao gồm: “Thêm” các tính năng bảo mật chẳng hạn như xác thực hai yếu tố cho tài khoản cá nhân; “Kiểm tra” các dấu hiệu lừa đảo tiềm ẩn bằng cách đặt câu hỏi như yêu cầu cung cấp thông tin để xác minh tính hợp pháp người nhận tiền; “Thông báo” cho chính quyền và chủ sở hữu nền tảng công nghệ về các trường hợp bị lừa đảo của cá nhân. Tương tự, UK Finance của Anh cũng đưa ra chiến dịch “TAKE FIVE TO STOP FRAUD” trong nỗ lực nhằm chống lại tình trạng lừa đảo chuyển tiền, chiến dịch này kêu gọi người dân DỪNG LẠI và XEM XÉT liệu tình huống chuyển tiền có thật sự hợp lý hay không.



Sự xuất hiện của AI là một thách thức quan trọng trong các cuộc chiến chống lừa đảo

Các tổ chức tài chính cần chung tay ngăn chặn khách hàng rơi vào những trò lừa đảo này bằng cách đẩy mạnh tuyên truyền nâng cao nhận thức về những trò lừa đảo phổ biến. Bên cạnh đó, cũng có thể đưa ra các biện pháp để đảm bảo những khách hàng là nạn nhân của lừa đảo nhận được sự trợ giúp cần thiết bất kể họ giao dịch tại ngân hàng nào như xây dựng đội ngũ các chuyên gia chống lừa đảo hoạt động 24/7 để ngăn chặn các hành vi lừa đảo trước khi chúng thành công, các chuyên gia phải đảm bảo rằng họ hiểu rõ ai đang gửi và nhận tiền qua hệ thống tài khoản của họ. Các nhân viên của tổ chức tài chính cũng phải được đào tạo liên tục, nghiêm ngặt để phát hiện và ngăn chặn các trường hợp lừa đảo tại điểm cung cấp dịch vụ chuyển tiền nhằm ngăn khách hàng trở thành nạn nhân của loại tội phạm này.

Kiểm soát các tài khoản con la: Khi tội phạm kiếm tiền bất hợp pháp, chúng cần che giấu hoặc rửa nguồn tiền. Một cách thức chúng sử dụng là tìm người chuyển số tiền đó. Chúng sẽ trả tiền cho những người này và yêu cầu mở tài khoản ngân hàng đứng tên người đó để chuyển và nhận tiền thay. Những người này trở thành những con la tiền (money mules), tức là cho phép người khác sử dụng tài khoản ngân hàng, thẻ điện tử, tài

khoản tiền điện tử hoặc số điện thoại của mình cho hoạt động tội phạm chuyển tiền và rửa tiền. Chúng sử dụng thủ đoạn này để chuyển tiền nhằm tránh sự theo dõi của các cơ quan thực thi pháp luật. Ngân hàng Nhà nước cần chỉ đạo các ngân hàng phải có trách nhiệm chủ động giám sát và ngăn chặn việc mở các tài khoản con la để ngăn ngừa tình trạng lừa đảo này. Bằng cách giám sát chặt chẽ cả giao dịch đến và đi cũng như phân tích hành vi tài khoản, các ngân hàng có thể phá vỡ chuỗi tài khoản con la và phát hiện các tài khoản con la liên quan đến danh tính tổng hợp hoặc bị đánh cắp và các trường hợp chiếm đoạt tài khoản. Tập trung vào tài khoản con la cũng có khả năng phá vỡ toàn bộ mạng lưới tội phạm và tạo ra tiến bộ trong việc ngăn chặn tội phạm lừa đảo tài chính rộng hơn.

Để hệ thống của ngân hàng phát hiện một cách hiệu quả lừa đảo chuyển tiền qua tài khoản, hệ thống cần trang bị công nghệ tiên tiến nhất, được hỗ trợ bởi trí tuệ nhân tạo và phát hiện theo thời gian thực, đặc biệt là trong bối cảnh thế giới ngày càng có nhiều giao dịch được hoàn thành chỉ trong vài giây. Các hệ thống dựa trên trí tuệ hành vi (Behavioral intelligence) có thể dựa trên việc phân tích một số tiền bất thường, thời gian giao dịch bất

thường, người nhận thanh toán từ nước ngoài, cuộc gọi diễn ra đồng thời với giao dịch và một số lượng lớn các điểm bất thường về sinh trắc học, giao dịch, thiết bị hoặc các điểm bất thường khác để cho thấy dấu hiệu hoạt động lừa đảo chuyển tiền. Những hệ thống như trên rất cần thiết không chỉ để giảm thiểu tổn thất mà còn là lợi thế cạnh tranh giúp nâng cao niềm tin và giữ chân khách hàng. Bằng cách ưu tiên phát hiện và ngăn chặn lừa đảo chuyển tiền, các tổ chức tài chính có thể biến thách thức của hoạt động lừa đảo thành cơ hội để tạo sự khác biệt và cải thiện dịch vụ khách hàng.

Chính phủ cần xem xét những thay đổi về luật pháp liên quan đến thủ tục mở tài khoản, cắt thanh toán ngay lập tức hoặc các phản ứng chính đáng tương tự khác nhằm giúp ngành Ngân hàng hành động chủ động hơn khi có nghi ngờ lừa đảo và ngăn chặn tội phạm này. Đồng thời, các cơ quan quản lý hệ thống thanh toán cần xem xét những đổi mới trong dài hạn để giúp khách hàng xác định rõ hơn người mà họ đang giao dịch. Điều này có thể bao gồm một hệ thống để xác minh chi tiết nhân thân người nhận tiền trước khi thực hiện chuyển khoản. Với những yêu cầu bổ sung nhiệm vụ giám sát lừa đảo mới như trên có thể khiến một số giao dịch gặp nhiều bất tiện hơn khi thực hiện, đặc biệt là các giao

dịch có giá trị lớn. Sự xung đột này là cần thiết để bảo vệ khách hàng khỏi các giao dịch lừa đảo.

Đề cao việc xử lý các vụ lừa đảo chuyển tiền như các tội phạm khác: Mức độ lo ngại và thiệt hại của người dân từ lừa đảo chuyển tiền qua tài khoản ngày càng tăng. Nhiều quốc gia đã bắt đầu tài trợ cho một đơn vị cảnh sát chuyên trách giải quyết các vụ gian lận và lừa đảo tài chính chẳng hạn như Singapore hay Nhật Bản.

Khi nhận được các đơn trình báo của nạn nhân về các tài khoản lừa đảo, các cơ quan điều tra cần phát thông báo và cho phép đóng tài khoản để tránh kẻ lừa đảo tiếp tục sử dụng những thủ đoạn tương tự. Cần nhìn nhận rằng, việc nạn nhân tự nguyện chuyển tiền qua tài khoản vì lý do tình cảm... không phải đang tham gia vào một giao dịch đồng thuận mà bị lừa gạt. Do đó, họ cần cơ quan thực thi pháp luật giúp đỡ. Tuy nhiên, nỗ lực truy tìm kẻ lừa đảo ở nước ngoài và thu hồi số tiền là hầu như rơi vào bế tắc, các cơ quan thực thi pháp luật phải được cung cấp những công cụ mạnh hơn, cần được chia sẻ thông tin dữ liệu để thực hiện chức năng tốt hơn.

Tất cả những biện pháp này đều đòi hỏi phải có sự thay đổi từ phía luật pháp. Không có giải pháp nhanh chóng hay chắc chắn nào, nhưng các cơ quan quản lý Nhà nước cần quyết tâm trấn áp tội phạm này trên mọi

mặt trận. Một trong những phát hiện đáng lo ngại nhất từ báo cáo của các quốc gia là tỷ lệ trình báo rất thấp các vụ lừa đảo cho thấy việc chưa tin tưởng vào chính quyền, các cơ quan thực thi pháp luật và sự không chắc chắn về nơi để trình báo các vụ lừa đảo. Điều này đã dẫn đến một khoảng trống đáng kể trong việc hỗ trợ các nạn nhân thu hồi số tiền bị tổn thất, cũng như cho thấy nhu cầu cấp thiết về cơ chế báo cáo rõ ràng hơn. Do đó, các cơ quan quản lý cần xây dựng các quy trình nhất quán để tiếp nhận thông báo của nạn nhân về lừa đảo chuyển tiền qua tài khoản. Cần đơn giản hóa các cách trình báo, cung cấp hệ thống hỗ trợ để tiếp cận cho nạn nhân để khuyến khích nhiều nạn nhân hơn tìm kiếm trợ giúp và báo cáo về các vụ lừa đảo.

KẾT LUẬN

Cuộc chiến chống lừa đảo chuyển tiền qua tài khoản phải tiếp tục và trách nhiệm không thể chỉ thuộc về cơ quan thực thi pháp luật. Sáng suốt và cảnh giác là chìa khoá cần thiết để bảo vệ bản thân và cộng đồng khỏi những kẻ lừa đảo chuyển tiền với những trò lừa đảo tinh vi hơn đang xuất hiện. Các cơ quan quản lý, các tổ chức có liên quan cần chủ động bảo vệ tài chính cho người dân thông qua dự đoán, giáo dục nhận thức, phát hiện và ngăn chặn các mối đe dọa từ lừa đảo chuyển tiền qua tài khoản ♦

TÀI LIỆU THAM KHẢO:

- *Annual Fraud Report, UK Finance, 2024.*
- *Annual fraud report, The definitive overview of payment industry fraud in 2022.*
- *Annual Scams and Cybercrime Brief 2023, Singapore Police Force.*
- *An Assessment of Scams in East Asia – in Australia, HongKong and Singapore, Financial Scams Report, 2024.*
- *National Anti-Scam Centre in action, Australia Government, 2023.*
- <https://www.threatmark.com/changing-landscape-fraud-liability/>
- <https://www.ncpc.org.sg/news-and-events/events/scaminar-2023/>
- <https://www.straitstimes.com/singapore/new-framework-holds-financial-institutions-telcos-accountable-to-scam-victims-kicks-in-on-dec-16>
- <https://treasury.gov.au/consultation/c2024-573813>
- <https://trustpair.com/blog/wire-transfer-fraud-prevention-best-practices-and-recovery/>
- <https://www.linkedin.com/pulse/protecting-against-escalating-financial-fraud-japan-comprehensive>
- <https://cashesentials.org/japan-why-the-police-want-to-restrict-the-use-of-bank-cards-for-the-over-65s/>
- <https://thesaigontimes.vn/wp-content/uploads/2024/01/State-of-Scam-Report-2023-Vietnam.pdf>
- <https://opengovasia.com/2024/06/04/thailand-strengthens-anti-fraud-measures/>
- <https://edition.cnn.com/2024/08/02/business/zelle-fraud-scam-payment/index.html>
- <https://www.statista.com/statistics/266362/phishing-attacks-country/>