

CHỐNG RỬA TIỀN: CÁC VẤN ĐỀ CƠ BẢN

Phần 7: Tài sản ảo



“Tài sản ảo” đề cập đến một loại tài sản mới được cung cấp bởi Công nghệ sổ tổng hợp phân phối (Distributed Ledger Technology - DLT). DLT cho phép dữ liệu được lưu trữ tại nhiều địa điểm (“phi tập trung”) trên một mạng lưới chia sẻ cho phép người tham gia theo dõi quyền sở hữu và chuyển nhượng tài sản ảo, như Bitcoin. Tài sản ảo thể hiện các tính năng độc đáo, ưu điểm và nhược điểm so với tài sản và thanh toán truyền thống. Kế toán viên chuyên nghiệp phải tự làm quen với các cách mà những kẻ rửa tiền và tài trợ khủng bố có thể sử dụng để thu được, di chuyển và lưu trữ giá trị, thường nằm ngoài hệ thống tài chính được quy định và che giấu nguồn gốc hoặc điểm đến của các khoản tiền.

Tội phạm có thể lạm dụng tài sản ảo như thế nào?

Tài sản ảo có thể liên quan đến bất kỳ giai đoạn nào của rửa tiền bao gồm:

- Dự đoán tội phạm: ví dụ, gây quỹ thông qua hoạt động bất hợp pháp bằng cách bán hàng hóa hoặc dịch vụ bất hợp pháp để đổi lấy tài sản ảo.
- Vị trí: chuyển đổi các tài sản ảo không hợp lệ thành tiền tệ pháp định trong hệ thống tài chính truyền thống.
- Che dấu: Các giao dịch dựa trên tiền điện tử thường có thể được theo dõi bằng phân tích công nghệ chuỗi, khối (blockchain), tuy nhiên, có thể không có bất kỳ liên kết nào giữa giao dịch và bất kỳ cá nhân cụ thể nào khi được thực hiện bên ngoài phạm vi quy định. Tội phạm cũng có thể sử dụng các dịch vụ ẩn danh như máy trộn (mixers) và làm lộn xộn (tumblers) để phá vỡ liên kết giữa các giao dịch tiền điện tử.
- Phân lớp: Chuyển đổi tài sản thực thành tài sản ảo, trao đổi tài sản ảo, chuyển đổi giữa các tài sản ảo và chuyển đổi tài sản ảo thành tiền tệ pháp định.
- Tích hợp: tương tự như rửa tiền bản, một công ty trực tuyến chấp nhận thanh toán bằng tiền điện tử có thể được thành lập để hợp pháp hóa thu nhập và làm sạch tiền điện tử bản.

Giải thích thuật ngữ

Tài sản ảo (VA): Tài sản ảo là một đại diện kỹ thuật số về giá trị có thể được chuyển nhượng hoặc sử dụng để thanh toán. Nó không bao gồm tiền tệ pháp định kỹ thuật số.

Tiền điện tử: Một tài sản ảo phi tập trung được bảo vệ bằng mật mã có thể được sử dụng làm phương tiện trao đổi, chuyển nhượng, lưu trữ và giao dịch điện tử. Phổ biến nhất trong số hàng nghìn loại tiền điện tử là Bitcoin và Ether.

NFT (Non-Fungible Token – Mã thông báo không thể thay thế): Một tài sản ảo hoàn toàn duy nhất. Mặc dù có nhiều Bitcoin, nhưng chỉ có một NFT. Chúng thường đại diện cho một phần cụ thể của tác phẩm nghệ thuật kỹ thuật số hoặc một số tài sản kỹ thuật số hoặc tài sản thực khác.

Nhà cung cấp dịch vụ tài sản ảo (Virtual Asset Service Provider - VASP): Doanh nghiệp cung cấp bất kỳ dịch vụ nào sau đây:

- Chuyển đổi hoặc trao đổi giữa tài sản ảo và tiền tệ pháp định hoặc giữa các tài sản ảo khác nhau;
- Giữ an toàn / quản lý tài sản ảo;
- Cung cấp các dịch vụ tài chính liên quan đến phát hành tài sản ảo.

Ví tiền ảo: Một phương tiện để nắm giữ, lưu trữ và chuyển các tài sản ảo.

NGHIÊN CỨU TÌNH HUỐNG

Cuộc tấn công bằng mã độc Pipeline Ransomware

Tài sản ảo đã nhanh chóng trở thành một hình thức thanh toán tiền chuộc yêu thích cho các cuộc tấn công bằng mã độc “ransomware” trên không gian mạng, hình thức này ngày càng được các kế toán viên chuyên nghiệp, đặc biệt là kiểm toán viên và khách hàng của họ quan tâm.

Cuộc tấn công bằng mã độc Pipeline Ransomware ở Hoa Kỳ là một ví dụ điển hình về các cuộc tấn công bằng mã độc mà các công ty phải chịu một cách thường xuyên. Vào tháng 5 năm 2021, Colonial Pipeline Company đã phải chịu một cuộc tấn công mạng bằng mã độc lớn dẫn đến việc ngừng hoạt động trong 5 ngày. Những kẻ tấn công yêu cầu 75 Bitcoin tiền chuộc, tương đương 4,4 triệu USD mà Colonial Pipeline đã trả. Trong khi các nhà chức trách có thể thu hồi phần lớn số tiền chuộc, nghiên cứu sâu hơn cho thấy những kẻ tấn công đã nhận được hơn 90 triệu USD Bitcoin từ 47 nguồn khác nhau trong năm trước.

Cuối cùng, những khoản tiền thu được bất hợp pháp đó sẽ cần được tích hợp vào hệ thống tài chính hợp pháp, có khả năng tạo cơ hội cho các kế toán viên chuyên nghiệp xác định và báo cáo. Đồng thời, các cuộc tấn công bằng mã độc làm nổi bật tầm quan trọng của các biện pháp kiểm soát an ninh mạng hiệu quả.

Bổ sung gần đây cho các tiêu chuẩn FATF

Các thuật ngữ “Tài sản ảo” và “Nhà cung cấp dịch vụ tài sản ảo” là những bổ sung mới trong Bảng thuật ngữ của FATF vào năm 2018. Đồng thời, VASP đã được đưa vào khuôn khổ quy định của FATF. Để có cái nhìn sâu hơn về VAs và VASPs từ góc độ chống rửa tiền và chống tài trợ khủng bố (AML / CFT), vui lòng xem [Hướng dẫn cập nhật của FATF về Phương pháp dựa trên rủi ro đối với tài sản ảo và nhà cung cấp dịch vụ tài sản ảo](#).

HỖ TRỢ BỔ SUNG



Để nắm được hướng dẫn chung về chống rửa tiền, vui lòng xem [Hướng dẫn về phương pháp dựa trên rủi ro cho nghề kế toán](#) của FATF. Để có thêm thông tin địa phương chi tiết, bao gồm các yêu cầu của pháp luật được áp dụng, vui lòng liên hệ với tổ chức kế toán chuyên nghiệp của bạn.



529 Fifth Avenue, New York 10017
www.ifac.org | +1 (212) 286-9344 | [@ifac](#) | [in](#) company/ifac

⚠️ Các báo động đỏ chính yếu

Các báo động đỏ cho rửa tiền “truyền thống” được áp dụng. Ngoài ra:

- Phần lớn nguồn tài sản của khách hàng có được từ các khoản đầu tư vào VA mà không có bất kỳ dấu vết nào trên giấy tờ.
- Nguồn của cải của khách hàng được lấy một cách không cân xứng từ các VA có nguồn gốc từ các nhà cung cấp dịch vụ tài sản ảo (VASPs) thiếu kiểm soát AML/CFT.
- Khách hàng sử dụng sản phẩm giao dịch VA trong khu vực pháp lý rủi ro cao mà thiếu các biện pháp kiểm soát AML /CFT.
- Khách hàng thường xuyên thay đổi thông tin nhận dạng của họ, bao gồm địa chỉ thư điện tử (email), địa chỉ IP.

Các kế hoạch rửa tiền mã hóa gần đây đã tận dụng những điều sau:

- Trao đổi tiền điện tử không được kiểm soát (không tuân thủ AML/ định danh khách hàng (Know Your Customer - KYC)).
- Các trang điện tử chơi cờ bạc và trò chơi.
- Sử dụng dịch vụ trộn (mixing services) hoặc công cụ trộn (Tumblers) (ví dụ: Anonymix/Trộn ẩn danh).
- Máy ATM tiền điện tử có khả năng quản lý rủi ro yếu.
- Thẻ ghi nợ tiền điện tử trả trước.

Hoạt động quan trọng tận dụng các sản phẩm / dịch vụ này cần được kế toán viên xem xét lần thứ hai và kiểm tra thêm.

Khi nào rút khỏi dịch vụ

- Các dịch vụ được yêu cầu có thể có tính chất chuyên môn nằm ngoài phạm vi năng lực của bạn.
- Không có hồ sơ giao dịch hoặc đầu tư chi tiết nguồn gốc của các khoản tiền.
- Bạn có lo ngại về danh tiếng của tài sản ảo, (các) nhà phát hành và (các) sản phẩm giao dịch.
- Thiếu các biện pháp kiểm soát AML/CFT hiệu quả do (các) tổ chức phát hành và (các) sản phẩm giao dịch đưa ra.
- Bạn có lo ngại về tính xác thực của thông tin được cung cấp bởi, hoặc có mối quan tâm về, khách hàng

Nộp báo cáo các hành động đáng ngờ (“SAR”)

Nếu bạn nghi ngờ rằng có thể có hoạt động tội phạm hoặc tiền phạm tội liên quan trong việc chuyên giao tài sản, khi đó bạn có thể báo cáo những nghi ngờ của mình cho đơn vị tình báo tài chính địa phương. Ở một số khu vực pháp lý, đây là nghĩa vụ pháp lý đối với các kế toán viên chuyên nghiệp.



www.icaew.com
[@icaew](#) | [in](#) company/icaew

Ấn phẩm “Chống rửa tiền, các vấn đề cơ bản: Phần 7 - Tài sản ảo” do Liên đoàn Kế toán quốc tế xuất bản tháng 02/2022 bằng tiếng Anh, được Hội Kiểm toán viên hành nghề Việt Nam dịch sang tiếng Việt vào tháng 06/2022, và được IFAC cho phép sử dụng. Các nội dung được phê duyệt của tất cả các ấn phẩm của IFAC do IFAC phát hành là bằng ngôn ngữ tiếng Anh. IFAC không chịu trách nhiệm về tính chính xác và hoàn chỉnh của bản dịch hoặc về các hành động có thể xảy ra sau đó do kết quả của bản dịch.

Bản quyền năm 2022 nội dung tiếng Anh của ấn phẩm “Chống rửa tiền, các vấn đề cơ bản: Phần 7 - Tài sản ảo” thuộc về IFAC. Tất cả bản quyền được đăng ký.

Bản quyền năm 2022 nội dung tiếng Việt của ấn phẩm “Chống rửa tiền, các vấn đề cơ bản: Phần 7 - Tài sản ảo” thuộc về IFAC. Tất cả bản quyền được đăng ký.

Tiêu đề gốc: “Anti-Money Laundering, The Basics Installment 7 - Virtual Assets”

Vui lòng liên hệ Permissions@ifac.org để được sao chép, lưu trữ hoặc truyền tải hoặc các hình thức sử dụng tương tự khác của tài liệu này.