الأصول الافتراضية

مؤشرات تنبيه (Red flags) في مجال غسل الأموال وتمويل الإرهاب

شهر سبتمبر ٢٠٢٠

يُعتبر فريق العمل المالي - فاتف - منظمة حكومية دولية مستقلة تعمل على تطوير وسنّ السياسات التي تحمي النظام المالي العالمي من عمليات غسل الأموال وتمويل الإرهاب والحد من تمويل أسلحة الدمار الشامل. وتُعرف توصيات فريق العمل المالي - فاتف - بأنها المعايير العالمية لمكافحة غسل الأموال ومكافحة تمويل الإرهاب.

وللمزيد من المعلومات بشأن فريق العمل المالي - فاتف - نأمل زيارة الموقع التالي: www.fatf-gafi.org

المحتويات

اختصار

مقدمة

المنهجية والمصادر المستخدمة في تحديد قائمة مؤشرات تنبيه

(Red flags)

نقاط مهمة لملاحظتها عند قراءة هذا التقرير

تنبيه (Red flags)

مؤشرات تنبيه (Red flags) فيما يتعلق بالتحويلات المالية

مؤشرات تنبيه (Red flags) فيما يتعلق بأساليب التحويل

مؤشرات تنبيه (Red flags) بشأن عدم الكشف عن الهوية

مؤشرات تنبيه (Red flags) فيما يتعلق بالمرسلين والمتلقين

مؤشرات تنبيه (Red flags) فيما يتعلق بمصدر الأموال أو

الثروة

مؤشرات تنبيه (Red flags) في إطار المخاطر الجغرافية

التوصيات

المراجع

قائمة المصطلحات المذكورة في التقرير

(AEC) : العملات المجهولة الهوية والمشفرة المعززة

(CDD): العناية الواجبة بالعملاء

(DNFBPs): المهن والأعمال غير المالية المحددة

(DNS) : المختصين بتسجيل أسماء المجال

(FATF): فريق العمل المالي

(FIs): المؤسسات المالية

(FIUs): وحدات التحريات المالية

(ICO): الطرح الأولي للعملة

(KYC): اعرف عميلك

(LEAs): سلطات إنفاذ القانون

(ML): غسل الأموال

(STRs): تقارير الحوالات المشبوهة

(TF): تمويل الإرهاب

(VA\ Vas) : الأصول الافتراضية

(VASPs): مزودي خدمات الأصول الافتراضية

مقدمة

١. الأصول الافتراضية والخدمات ذات العلاقة، لديها القدرة على تحفيز الابتكار المالي والفعالية، ولكن خصالتها المميزة تخلق فرصاً جديدة لغاسلي الأموال، وممولي الإرهاب، والمجرمين الآخرين، لغسل أموالهم أو تمويل أنشطتهم غير المشروعة. القدرة على التحويل خارج الحدود بشكل متكرر لا يسمح فقط للمجرمين بالحصول على الأموال ونقلها وتخزين الأصول رقمياً خارج إطار النظام المالي غالباً، بل يساعد أيضاً في إخفاء مصدر أو وجهة هذه الأموال وعليه فإنه من الصعب على الكيانات التعرف على الأنشطة المشبوهة في الوقت المناسب. وتضيف هذه العناصر عقبات جديدة أمام الكشف عن الأنشطة الإجرامية والتحقيق فيها من قبل السلطات الوطنية.

٢. في شهر أكتوبر ٢٠١٨، قام فريق العمل المالي - فاتف - بتحديث معاييرهِ وذلك لتوضيح تطبيق معايير فريق العمل المالي فيما يتعلق بالأصول الافتراضية ومزودي خدمات الأصول الافتراضية، وذلك لمساعدة السلطات القضائية في التخفيف من مخاطر غسل

الأموال وتمويل الإرهاب المرتبطة بالأصول الافتراضية ولحماية نزاهة النظام المالي العالمي. في شهر يونيو ٢٠١٩، تبنى فريق العمل المالي - فاتف - مذكرة تفسيرية بشأن التوصية (١٥) تتعلق بتطبيق متطلبات فريق العمل المالي حول أنشطة الأصول الافتراضية أو عملياتها ومزودي خدمة الأصول الافتراضية مع الأخذ بعين الاعتبار الإبلاغ عن الحوالات المالية المشبوهة.

٣. وقد أعد فريق العمل المالي - فاتف - تقريراً مختصراً بشأن مؤشرات تنبيه (Redflags) فيما يتعلق بأنشطة غسل الأموال وتمويل الإرهاب بما في ذلك الأصول الافتراضية لمساعدة الكيانات ومن ضمنها المؤسسات المالية، المهن والأعمال غير المالية المحددة، ومزودي خدمة الأصول الافتراضية. من جهة أخرى، فقد تم تصنيفها تحت إطار التعرف والإبلاغ عن أنشطة غسل الأموال وتمويل الإرهاب بما في ذلك الأصول الافتراضية. ويسهل التقرير على الكيانات المبلغة تطبيق النهج القائم على المخاطر حول متطلبات العناية الواجبة بالعملاء والتي تتطلب تحديد عملائهم والملاك المستفيدين وفهم طبيعة وهدف العلاقة العملية ومعرفة مصدر الأموال.

٤. إن الإدارات العملية بما في ذلك وحدات التحريات المالية، سلطات إنفاذ القانون، والمدعين العامين، قد

يجدون في هذا التقرير مرجعاً مفيداً لتحليل تقارير الحوالات المشبوهة أو تطوير الكشف، التحقيق ومصادرة الأصول الافتراضية التي يتم إساءة استخدامها.

٥. مالياً، فإن الجهات الرقابية/التنظيمية للمهن والأعمال غير المالية المحددة و مزودي خدمة الأصول الافتراضية قد يجدون هذه المؤشرات مفيدة عند إعداد تقارير الحوالات المشبوهة، ومراقبة امتثال الكيانات لضوابط أنشطة غسل الأموال ومكافحة تمويل الإرهاب. وحينما يملك الكيان المبلغ معلومات تشير لوجود مؤشر أو أكثر دون توضيح تجاري منطقي، ولكن يفشل في تقديم تقرير الحوالات المشبوهة.

**المنهجية والمصادر المستخدمة في تحديد قائمة تنبيه
(Redflags)**

٦. إن مؤشرات تنبيهه (Redflags) المذكورة في هذا التقرير مبنية على دراسة أكثر من مائة قضية تم المساهمة بها من قبل سلطات قضائية خلال الفترة من ٢٠١٧-٢٠٢٠، ويتضمن ذلك أيضاً مخرجات تقرير فريق العمل المالي السري بشأن التحقيق المالي والمتضمن الأصول الافتراضية (يونيو ٢٠١٩) وتقرير فريق العمل المالي عن العملات الافتراضية وتعريفاتها الرئيسية واحتمالية وجود مخاطر تتعلق بأنشطة غسل الأموال ومكافحة تمويل الإرهاب والذي تم نشره في شهر (يونيو ٢٠١٤). وكذلك سوء استخدام الأصول الافتراضية بشكل عام.

نقاط مهمة في استخدام الأصول الافتراضية بغرض غسل الأموال وتمويل الإرهاب

إن غالبية الجرائم المرتبطة بالأصول الافتراضية تركز على جرائم غسل الأموال، رغم أن المجرمين يستخدمون الأصول الافتراضية لتجنب العقوبات المالية وزيادة الأموال الداعمة للإرهاب.

إن أنواع الجرائم المشار إليها من السلطات المعنية تتضمن غسل الأموال، بيع المواد الخاضعة للرقابة وأهداف أخرى غير قانونية بما في ذلك الأسلحة،

الاحتتيال، التهرب الضريبي، جرائم الكمبيوتر (مثل على ذلك: الهجمات الالكترونية التي ينتج عنها سرقات)، استغلال الأطفال، تهريب البشر، التهرب من العقوبات وتمويل الإرهاب. إضافة إلى ذلك، المواد سواءً كانت يتم بيعها مباشرة من خلال الأصول الافتراضية أو استخدام العملات الافتراضية كما في غسل الأموال بتقنية الطبقات. كما أن ثاني تصنيف شائع في استخدامها يرتبط بالاحتتيال، النصب، البرمجيات الضارة (Ransomwarer) والابتزاز. حالياً، بدأت شبكات غسل الأموال المحترفة في استغلال الأصول الافتراضية كواحدة من الوسائل لتحويل وجمع أو إخفاء العوائد.

نقاط مهمة لملاحظتها عند قراءة هذا التقرير

7. هذه المؤشرات مرتبطة بطبيعة الأصول الافتراضية والأنشطة ذات العلاقة بها بشكل شامل. كما أن الأنشطة المشبوهة التي يدخل فيها استخدام الأصول الافتراضية لها سمات مشتركة مع أنشطة غسل الأموال وتمويل الإرهاب بما في ذلك استخدام عملات ورقية أو أي نوع آخر من الأصول. ولذلك توجب على الكيانات المبلغة الأخذ بعين الاعتبار المخاطر المطروحة من قبل عملائهم، منتجاتهم وعملياتهم

وكذلك مؤشرات المخاطر العادية. ويجب أن تؤخذ مؤشرات تنبيهه (Redflags) بعين الاعتبار في نفس الإطار.

٨. الفهم الحر للأعلام أدناه يمكن بلورتها عند تحليلها مع المعلومات الواردة من الوكالات العملية والتي يمكن بعد ذلك تطويرها والعمل عليها من خلال الشراكات الخاصة والعامة. إن عمليات التقييم الدورية تأخذ بعين الاعتبار المخاطر المستجدة وحالة السلطة، نوع العميل أو نوع الكيان نفسه. وجود مؤشر تنبيهه (Redflags) ليس محصوراً بالضرورة على أسس غسل الأموال وتمويل الإرهاب وإنما يؤدي لرقابة وتحقيق إضافيين بشكل غير محدود. على سبيل المثال: يمكن للعميل تقديم توضيحات لتبرير مؤشر تنبيهه (Redflags) سواءً كان التبرير تجاري أو اقتصادي وكذلك الغرض من التحويل.

٩. ويجب أن تعي السلطات المختصة، سواءً وحدات التحري المالية و المهن والأعمال غير المالية المحددة ومزودي خدمة الأصول الافتراضية، أنه عندما يتم تقييم أنشطة مشبوهة، فإن مؤشرات تنبيهه (Redflags) قد لا تكون واضحة إلا خلال مراجعات التحويل المحددة. إن ملاحظة مؤشر أو أكثر من مؤشرات العلم الأحمر مبني على خطوط الأعمال،

المنتجات، أو الخدمات التي يقدمها مزودي خدمة الأصول الافتراضية دون تحديد الهدف الاقتصادي أو الغرض التجاري. وقد يساعد ذلك أيضاً الكيانات المبلغة بأن تعرف بأن عملية غسل الأموال أو تمويل الإرهاب تحصل بالفعل، ولا يجب بأن تكون مؤشرات تنبيهه (Redflags) هي الوحيدة والمنفردة التي يجب تعبئتها في تقرير الاشتباه بالحوالات ويجب أن تأخذ الكيانات المبلغة تعبئة تقرير الاشتباه في بعين الاعتبار حال معرفتهم، اشتباههم أو عند وجود أساسات منطقية.

مؤشرات تنبيهه (Redflags)

١٠. إن الأقسام التالية تحتوي على مجموعة من مؤشرات تنبيهه (Redflags) للاشتباه بنشاطات الأصول الافتراضية أو محاولات محتملة لتجنب رقابة سلطات إنفاذ القانون، وكما يتضح في أكثر من مائة دراسة لقضايا مختلفة تم جمعها منذ عام ٢٠١٧ من خلال فريق العمل المالي- فاتف-، ومن خلال المراجعات والبحث عبر المصادر المفتوحة. وكما ذكر سابقاً، فإن وجود مؤشر واحد لا يعني بالضرورة وجود نشاط إجرامي وغالباً ظهور عدة مؤشرات في حوالة واحدة

دون وجود شرح منطقي حول العمل التجاري الداعي لهذا التحويل يعزز من الشكوك حول ما إذا كان هناك نشاط إجرامي محتمل. ويجب أن يشجع وجود المؤشرات عمليات الرقابة، التحقق، والابلاغ متى ما كان ذلك ضرورياً.

تنبيه (Redflags) ذات العلاقة بالحوالات

١١. بالرغم من أن الأصول الافتراضية لم تصبح مستخدمة في كافة أرجاء العالم من قبل العامة، فقد أدى استخدامها للقبض على عدد من المجرمين. بدأ استخدام الأصول الافتراضية بهدف غسل الأموال منذ عقد من الزمن ومن ثم أصبحت الأصول الافتراضية تستخدم بشكل مهول لنشاطات إجرامية كثيرة. إن المؤشرات الموضوعية تشرح كيف أن التنبيهات (Redflags) مرتبطة تقليدياً مع وسائل الدفع العادية التي تظل ذات صلة باكتشاف النشاط غير المشروع المحتمل المتعلق بالأصول الافتراضية.

حجم وتكرار الحوالات

• ترتيب الأصول الافتراضية (على سبيل المثال: التبادل أو التحويل) بكميات قليلة أو كميات تحت

الكميات التي يمكن الاحتفاظ بها في السجلات أو الإبلاغ عن الحدود القصوى، يشابه ترتيب الحوالات النقدية.

● إجراء حوالات متعددة وذات قيمة عالية:

- خلال مدة قصيرة ، مثل مدة أربعة وعشرين ساعة

- بأسلوب مفاجئ أو غير منتظم، بدون وجود حوالات إضافية مسجلة خلال فترة طويلة وهذه الطريقة شائعة في القضايا المتعلقة بالبرمجيات الضارة (Ransomware).

- إلى حساب جديد أو حساب كان سابقاً مجمد.

● تحويل أصول افتراضية بشكل مباشر لعدد من مزودي خدمة الأصول الافتراضية وخاصة الذين يعملون في دول أخرى.

- وليس هناك علاقة بمقر إقامة العميل أو نشاط عمله.

- عدم وجود أو ضعف تشريعات غسل الأموال ومكافحة الإرهاب.

● إيداع الأصول الافتراضية في أسلوب تبادل بشكل فوري

- سحب الأصول الافتراضية دون وجود أنشطة تبادل مع أصول افتراضية أخرى، وهي خطوة غير ضرورية ينتج عنها رسوم تحويل.
- تحويل الأصول الافتراضية لعدة أنواع من الأصول الافتراضية مما ينتج عنه رسوم تحويل إضافية ولكن دون توضيح سبب تجاري منطقي (على سبيل المثال: تنوع المحفظة).
- سحب الأصول الافتراضية من مزودي خدمة الأصول الافتراضية مباشرة لمحفظة خاصة، وهذه العملية تحول الصراف/ مزود خدمات الأصول الافتراضية إلى خالط غسل الأموال (Mixer).

- قبول الأموال المشتبه بها كونها ناتجة عن احتيال أو سرقة

- إيداع أموال من عناوين الأصول الافتراضية التي تم تحديدها بأنها تحتوي على أموال مسروقة، أو عناوين أصول افتراضية مرتبطة بحاملي أموال مسروقة.

دراسة حالة: ١ - عدة تحويلات مباشرة لأصول افتراضية إلى مزودي خدمة أصول افتراضية في دول أخرى.

قدم مزود خدمة أصول افتراضية محلي تقريراً عن الاشتباه بحوالة متبوعاً بشكوك تتعلق بشراء كمية كبيرة من الأصول الافتراضية من قبل عدد من الأشخاص وقاموا بتحويلها فوراً لمزود خدمة أصول افتراضية في دولة أخرى. وقد تبين بأن كافة الأفراد يتشاركون في عنوان الإقامة ذاته، وأن معظم الأصول الافتراضية قد تم الوصول إليها من خلال نفس عنوان مزود خدمة الانترنت مما يشير لاحتمالية استخدام الأموال من قبل غاسلي أموال محترفين لغسل العائدات غير المشروعة.

بالإضافة إلى ذلك، تمر الأموال النقدية بعدة مراحل قبل شراء الأصول الافتراضية من قبل الأشخاص الذين يقومون بتحويل مبالغ أصلها غير مشروع. ولإخفاء مصدر الأموال، تم إيداع المبالغ النقدية أولاً في حسابات مختلفة وفي مؤسسات مالية مختلفة داخل الدولة. وبعد ذلك تم تحويل تلك الأموال لحسابات مختلفة مملوكة لكيانات متواجدة بتلك الدولة. وتمت عمليات شراء على تلك الحسابات بمبالغ صغيرة. وبعد ذلك، تم تحويل الأموال لمجموعة أخرى من الحسابات قبل الوصول لحسابات أشخاص لهم علاقة بمزودي خدمة الأصول الافتراضية. وقد تم شراء أصول افتراضية فوراً وتحويلها لمزود خدمة أصول افتراضية خارجي. وقد تورط

أكثر من ١٥٠ شخصاً في هذه القضية وهم مسؤولين عن تحويل مبلغ وقدره (108,352,900) دولار أمريكي أو ١١,٩٦٠ بعملة بتكوين لعدة حسابات عملة افتراضية مملوكة لشركتين مزودة لخدمة الأصول الافتراضية خارج البلاد.

المصدر: جنوب أفريقيا

دراسة حالة ٢: تحويل عدة أصول افتراضية لمزود خدمة أصول افتراضية خارجي.

مؤسسة تبادل أصول افتراضية أبلغت عن ما يقارب ٤٠٠ مليون وون كوري جنوبي أي ما يعادل ١,١٠٧,٣٠١ دولار قد تم سرقتها من ضحايا "التصيد الإلكتروني" وقد تم تحويلها إلى أصول افتراضية بالتدرج. وسبب الإبلاغ، هو تعدد التحويلات عالية القيمة لمزود خدمة أصول افتراضية خارجي ولمحافظة واحدة. تم تحويل الأموال المسروقة بشكل نقدي أولاً إلى ثلاثة أنواع من الأصول الافتراضية وبعدها تم إيداعها لمحافظة الأصول الافتراضية الموجودة لدى مزود أصول افتراضية محلي. ومن ثم قام المشتبه به بالتغطية على تلك المبالغ من خلال ٥٥ عملية تحويل عبر ٤٨ حساب منفصل

في مختلف مؤسسات تزويد الخدمة المحلية، ومنها إلى
محافظ أصول افتراضية بالخارج.

المصدر: كوريا الجنوبية.

مؤشرات تنبيه (Redflags) المرتبطة بأساليب التحويل

١٢. بما يشابه الجزئية السابقة، فإن التنبيهات
(Redflags) أدناه تشرح كيف يمكن التعرف على سوء
استخدام الأصول الافتراضية لأغراض غسل الأموال
وتمويل الإرهاب من خلال أساليب تحويل غير
معتادة، وغير شائعة.

تحويلات العملاء الجدد

- إيداع مبلغ كبير عند فتح محفظة جديدة لدى
مزودي خدمة الأصول الافتراضية بينما المبلغ
المودع لا يتوافق مع ملف العميل.
- إيداع مبلغ كبير عند فتح محفظة جديدة لدى
مزودي خدمة الأصول الافتراضية وإيداع المبلغ
كاملاً في أول يوم، ويبدأ العميل بالتجارة بكافة
المبلغ أو كمية كبيرة من المبلغ بنفس اليوم أو
اليوم الذي بعده، وقيام العميل بسحب كافة
المبلغ في اليوم الذي يليه. وبما أن أغلب

الأصول الافتراضية لها حدود نقل محددة للإيداعات، وفي حين أن غسل الأموال يتطلب مبالغ كبيرة أيضاً يمكن أن يكون من خلال تداول خارج البورصة.

- ويهدف العميل الحديث بالمتاجرة بكافة مبلغ الأصول الافتراضية أو سحب الأصول الافتراضية ومحاولة إخراج كافة الرصيد من المنصة.

دراسة حالة ٣: الإيداع الأساسي لا يتوافق مع ملف العميل.

إن تقديم مؤشرات الاشتباه أدناه يدفع المؤسسات المالية (البنوك) لتقديم تقرير اشتباه في حوالة مالية للسلطات، مما يؤدي لتحقيق بشأن غسل أموال:

- التحويلات لا تتناسب مع ملف صاحب الحساب في اليومين الأولى بعد إنشاء الحساب لشخص شاب، وتلقى الحساب إيداعات ذات طبيعة تجارية من عدة أشخاص مختلفين وبمبالغ كبيرة.

- أنماط التحويل - تم تحويل الأموال المودعة فوراً لحسابات متعددة خاصة بمزودي خدمة الأصول الافتراضية (في يوم واحد) لشراء أصول افتراضية (بيتكوين).

- ملف العميل - أحد الجهات الطالبة كان معروفاً لدى البنك كمطلوب في قضية احتيال. وقام البنك أيضاً بالإبلاغ عن عناوين تزويد خدمة الانترنت للسلطات.

وفقاً للتحقيقات، اتضح بأن صاحب الحساب الشخصي. قد تم استدراجه من قبل مجرمين على منصات التواصل الاجتماعي للمساعدة في تلقي ما يدعى بأنها مدفوعات لبضائع تم بيعها عبر الانترنت. من ناحية أخرى، يبدو أن هذه الأموال قد أودعت من قبل شركات كانت أيضاً ضحية ولم تكن مدفوعات بضائع. وقد تم تحويل المبالغ المودعة فوراً من الحساب الشخصي. من خلال عمليات بيع مقسمة لحساب آخر تملكه شركة أسهم في التشيك، ومن ثم استبدالها بعملة بتكوين موجودة لدى عدد من مزودي خدمة الأصول الافتراضية ومن ثم تم سحبها من الحساب. بالإضافة إلى تعبئة تقرير الاشتباه بحوالة مالية، أوقف البنك أيضاً الحوالات المشبوهة مما جعل مصادرة الأموال المسروقة ممكناً.

لقد لاحظ مزودي خدمة الأصول الافتراضية عدم انتظام في الأموال المتلقاه وأبلغوا عن معلومات مفيدة ساعدت كثيراً في التحقيقات. واحتوت المعلومات على: الظروف المحيطة حيث تم شراء الأصول الافتراضية، مستندات تعريف الحوالة للشراء واسم المشتري الشرعي مما سمح للسلطات طلب معلومات إضافية من البنوك (مثل: كشف حساب بنكي).
المصدر: جمهورية التشيك

الحوالات الخاصة بكافة المستخدمين

- الحوالات التي يكون بها أصول افتراضية متنوعة أو حسابات مختلفة دون وجود سبب تجاري منطقي.
- الحوالات المتكررة في نفس الفترة من الزمن (مثال: يوم، أسبوع، شهر.. إلخ) لنفس حساب الأصول الافتراضية :
. من خلال أكثر من شخص .
. بنفس عنوان مزود خدمة الانترنت من قبل شخص أو عدة أشخاص وبمبالغ كبيرة
- الحوالات القادمة من محافظ مالية غير مترابطة بمبالغ مالية صغيرة ومترابطة (تراكم

الأموال) مع وجود تحويلات بعد ذلك لمحافظ
أخرى أو استبدال كامل إلى العملة النقدية.
- إن تبديل العملة من نقدية إلى أصول افتراضية
يؤدي لخسارة محتملة (مثل: عندما يتم مقارنة
القيمة مع معايير الصناعة وخاصةً عندما تكون
الحوالات بدون تبرير تجاري منطقي).
- تحويل مبالغ كبيرة من العملات الورقية إلى
أصول افتراضية أو نوع واحد من الأصول
الافتراضية إلى أنواع أخرى منها.

دراسة حالة ٤: الحوالات التي تتم في وقت متكرر.

قامت مؤسسة مالية محلية بتعبئة تقرير اشتباه بحوالة مالية
بشأن مدفوعات غير مرخصة بين سمسار حسابات أصول
افتراضية وشخص أجنبي. وأبلغت الشركة الأمنية عن تلك
الأنشطة بعدما جرى تحديد المبالغ التي ستحول وإجمالي
تلك المبالغ أربعة مليون وثمانمائة ألف دولار أمريكي
بتحويلين منفصلين بينها ست دقائق من نفس اليوم) وتعبئة
نموذج للسمسار لفتح حساب متاجرة في يوم العمل التالي.
ولم تكن المحفظة مستضافة في جزر كايمان. وقاد تقرير
الاشتباه بالحوالة المالية لتبادل معلومات ناجحة مع وحدات

تحريات مالية أجنبية وتم إعادة معظم المبالغ للضحية مما سمح أيضاً للسلطة القضائية في تلك الدولة بتجميد حساب المشتبه به قبل إتمام الجريمة.
المصدر: جزر كايمان.

مؤشرات تنبيه (Redflags) فيما يتعلق بعدم الكشف عن الهوية

١٣. تحدد هذه المؤشرات خصائص أساسية وذات قيمة ترتبط بالتقنية الأساسية للأصول الافتراضية. إن تنوع السمات التقنية أدناه تضيف عدم الكشف عن الهوية وتضيف عقبات للتعرف على النشاطات الإجرامية من قبل سلطات إنفاذ القانون مما يجعل الأصول الافتراضية مغرية للمجرمين الذين يودون إخفاء أموالهم. بالإضافة، إلى أن مجرد ظهور هذه السمات في نشاط ما لا يعني مباشرة وجود حوالات غير مشروعة. على سبيل المثال: استخدام قرص صلب أو محفظة ورقية قد يكون مقبولاً كطريقة لحفظ الأصول الالكترونية ضد السرقة. مرةً أخرى، إن ظهور هذه المؤشرات يجب أخذه بعين الاعتبار في إطار

أشمل ومع عناصر أخرى تتعلق بالعميل وعلاقته أو التوضيح التجاري المنطقي.

- الحوالات من قبل العميل التي تحتوي على أكثر من نوع من الأصول الالكترونية بالرغم من الرسوم الإضافية للتحويل وخاصةً تلك التي لديها مستوى أعلى من عدم الكشف عن الهوية مثل العملات المجهولة الهوية والمشفرة المعززة أو العملات الخاصة.

- تحريك الأصول الافتراضية في نطاقات عامة وشفافة مثل بيتكوين للتمركز والعمل على تحويل العملة والمتاجرة بها مباشرةً في العملات المجهولة الهوية والمشفرة المعززة أو العملات الخاصة.

- العملاء الذين يديرون خدمات تزويد العملة الافتراضية دون ترخيص بمواقع شيء مقابل شيء (P2P). وبالأخص عندما يكون هناك مخاوف بأن من يديرون تلك المواقع يملكون كميات كبيرة من الأصول الافتراضية نيابةً عن عملائهم ويستبدل رسوم أعلى لعميله من خدمات التحويل التي تعرض من قبل مواقع تبادل أخرى.

- نشاط حوالات أكثر من المعتاد من حيث (الحجم والمستوى) من الأصول الافتراضية وصرها في مواقع التبادل المرتبطة بالمحافظ دون وجود توضيح تجاري منطقي.
- يتم تحويل الأصول الرقمية من/إلى المحافظ التي تظهر أنماط سابقة من النشاطات التي ترتبط باستخدامات مزودي خدمة الأصول الرقمية والتي تعمل على خدمات الخلط أو التعويم أو منصة P2P.
- وتستفيد الحوالات من خدمات الخلط والتعويم مما يشير إلى نية إخفاء تدفق الأموال الغير مشروعة بين عناوين المحافظ المعروفة ومواقع الانترنت الخفي التجارية.
- يتم إيداع الأموال أو سحبها من عناوين الأصول الافتراضية أو محافظ ذات روابط كشف مباشر أو غير مباشر لمصادر معروفة ومشتبه بها بما في ذلك مواقع الانترنت المظلم التجارية، خدمات الخلط والتعويم، مواقع المقامرة المشكوك بها، الأنشطة الغير قانونية (البرمجيات الخبيثة) و سرقة التقارير.

- استخدام قرص صلب أو محافظ ورقية غير مستضافة لنقل الأصول الافتراضية عبر الحدود.

- المستخدمين الذين يدخلون منصات مزودي خدمات الأصول الالكترونية الذين يسجلون اسم مجال الانترنت من خلال البروكسي. أو من خلال استخدام أسماء مسجلي المجال مما يوضح أسماء مالكي المجال.

- إن المستخدمين الذين يدخلون منصات مزودي خدمة الأصول الافتراضية يستخدمون عناوين تزويد خدمة انترنت مرتبطة بالانترنت المظلم أو برامج أخرى والتي تسمح بالتواصل دون الكشف عن الهوية بما في ذلك رسائل البريد الالكتروني المشفرة. إن الحوالات بين الشركاء من خلال اتصالات مشفرة ومتعددة يعني وجود (نماذج، محادثات، تطبيقات، ألعاب الكترونية) بديلة عن مزودي خدمة الأصول الافتراضية.

- إدارة عدة محافظ أصول افتراضية غير متصلة ببعضها البعض من قبل مزود خدمة انترنت واحد أو عنوان ماك (Mac address)، والتي يرتبط بها استخدام محافظ مسجلة بأسماء

أشخاص آخرين لإخفاء علاقتهم ببعضهم البعض.

- استخدام الأصول الافتراضية التي يكون تصميمها غير موثق بشكل كافي أو مرتبطة باحتيال محتمل أو أي أدوات أخرى توضح وجود مخططات احتيالية (مثل مخطط بونزي).

- تلقي أموال من / إرسال أموال إلى مزودي خدمة الأصول الافتراضية المطلعين على العناية الواجبة بالعملاء أو اعرف عميلك هي بشكل واضح ضعيفة أو غير موجودة.

- استخدام صرافات الأصول الافتراضية/ محلات صغيرة.

- بالرغم من الرسوم العالية على التحويلات وخاصة التي تستخدم غالباً من قبل أشخاص مغرر بهم أو ضحايا احتيال.

- في المناطق عالية الخطورة التي تظهر بها الأنشطة الاجرامية.

- الاستخدام الوحيد للصرافات الآلية/ أكشاك غير كافي للكشف عن تنبيهه (Redflags)، ولكن قد تكون كافية في الدول التي تعتبر عالية المخاطر أو تم استخدامها في تحويل مبالغ

مالية بسيطة بشكل متكرر (أو أي عوامل أخرى إضافية).

دراسة حالة ٥: استخدام عناوين تزويد خدمة انترنت مرتبطة بمواقع التجارة بالانترنت المظلم – ألفا باي (Alpha Bay) .

ألفا باي ، هو أكبر سوق إجرامي تم اكتشافه في الانترنت المظلم عام ٢٠١٧ ، من قبل السلطات حيث كان يستخدم من قبل مئات الآلاف من المتعاملين لبيع وشراء مخدرات غير مشروعة، ومستندات مزورة ومسروقة والدخول على الأجهزة، والبضائع المزيفة، وبرامج الكمبيوتر الخبيثة وأدوات التهكير والمواد الكيميائية السامة. وكان الموقع يعمل كخدمة مخفية على شبكة TOR لإخفاء مواقع السيرفرات وهويات الذين يديرون الموقع والمشرفين والمستخدمين. كما أن البائعين عبر موقع ألفا باي، يستخدمون عدة أنواع من الأصول الافتراضية ولديهم ما يقارب من مائتي ألف مستخدم وما يقارب أربعون ألف بائع، ومائتين وخمسين ألف من القوائم وقد سهلوا خلال الفترة ما بين ٢٠١٥ – ٢٠١٧ تداول بليون دولار أمريكي من الأصول الافتراضية.

في يوليو ٢٠١٧ ، قامت الحكومة الأمريكية بالتعاون مع أطراف خارجية بإيقاف السيرفرات المستضيفة لموقع ألفا

باي التجاري، وقبضت على المشرفين وأصدرت أمراً في شرق كاليفورنيا بمصادرة الأصول الحقيقية والافتراضية من الموقع التجاري، وقد حصل الفيدراليون على المذكرات بعد تعقب أصول تحويلات افتراضية بدأت من ألفا باي لحسابات أصول افتراضية أخرى وتعرفوا على الحسابات البنكية وأصول أخرى يديرها أعضاء إدارة موقع ألفا باي المصدر: الولايات المتحدة الأمريكية

دراسة حالة ٦: استخدام الخالطات والمعومات - الحلزونية (Mixing and tumbling- Helix)

إن الانترنت المظلم يعتمد على مزودي خدمة الأصول الافتراضية، وتضيف الحلزونية خدمات الخلط والاسقاط التي تساعد العملاء على إخفاء مصدر أو مالكي الأصول الافتراضية لمدة تزيد عن ثلاث سنوات. وقد ساعدت الحلزونية بشكل غير قانوني على إخفاء أكثر من ٣٥٠,٠٠٠ بتكوين والتي كانت تقدر قيمتها وقتها بمبلغ ثلاثمائة مليون دولار أمريكي. وقد أعلن مشغل هذه الخدمة بالتحديد على أن الخدمة تساعد في إخفاء الحوالات عبر الانترنت المظلم عن السلطات المختصة. في فبراير ٢٠٢٠، تم توجيه تهم بما فيها

التأمر لغسل الأموال ولقيامه بنشاط تحويل أموال غير مرخص بحق شخص يدير الحلزونية.

وكانت الحلزونية تتشارك مع ألفا باي لحين مصادرة ألفا باي من قبل سلطات إنفاذ القانون في عام ٢٠١٧.

المصدر: الولايات المتحدة الأمريكية

دراسة حالة ٧: استخدام المحفظة اللامركزية

توضح القضية كيف أن المجرمين يستخدمون المحفظة اللامركزية لإخفاء مصدر الأموال غير القانونية والتي ترد عبر المخدرات وأنشطة التهريب . وفي هذا الاطار، المجرمين المنخرطين في بيع المخدرات بكميات كبيرة عبر الانترنت لا يقبلون فقط المبالغ النقدية ولكن يمكن الدفع أيضاً بالاصول الالكترونية بتكوين، إكس كودز، إكسمو، شيكات (Bitcoin- Ex-codes, EXMO-cheques)

ويتم تحويل الأموال المتلقاة نقداً إلى أصول افتراضية من خلال حسابات مجهولة على منصة تجارة السلسلة الالكترونية . بعض الأموال بصيغة الأصول الافتراضية وبعد ذلك يتم تحويلها مرة أخرى إلى نقد من خلال استبدالها، قبل أن يتم تحويلها مرة أخرى للمجرمين من خلال الأصول

الافتراضية، حيث تم نقلها أولاً لمحافظ بتكوين غير مركزية مملوكة لمجرمين آخرين قبل أن يتم نقلها مرة أخرى لمحافظ بتكوين أخرى بتبادلات متعددة مما يزيد من صعوبة من تعقب ومتابعة الأموال. بشكل مماثل، تم تحويل الأموال المغسولة (أصول افتراضية) إلى نقد مرة أخرى قبل أن يتم إيداعها في حسابات بنكية. وقد أدين المجرم وحكم عليه بالسجن لمدة سبع سنوات وغرامة مالية.

المصدر: روسيا الاتحادية.

مؤشرات تنبيهه (Redflags) فيما يتعلق بالمرسل والمستقبل

١٤. مجموعة من المؤشرات ذات العلاقة بالمحفظه و السلوك الغير معتاد من قبل المرسل أو المستقبل للحوالات غير المشروعة.

المخالفات التي تم رصدها عند فتح حساب

- إنشاء حسابات منفصلة تحت أسماء متعددة لتجنب الضوابط الخاصة بالتجارة أو حدود السحب المعتمدة من قبل مزودي خدمة الأصول الافتراضية.

- التحويلات الصادرة من عناوين تزويد خدمة انترنت غير موثوقة، أو عناوين تزويد خدمات انترنت في دول خاضعة للعقوبات، أو عناوين تزويد خدمة سبق التأشير عليها كمشتبه بها.
- محاولة فتح عدة حسابات لدى نفس مزود خدمة العملات الافتراضية من قبل نفس عنوان مزود خدمة الانترنت.
- بشأن التجار/ والمستخدمين المتواطئين، تكون سجلات مجالهم في دول أخرى غير دولهم الأساسية أو في دولة ذات تسجيل ضعيف للمجال.

المخالفات التي تم رصدها خلال عملية العناية الواجبة بالعملاء

- معلومات ناقصة أو غير مكتملة بشأن اعرف عميلك أو رفض العميل تقديم مستندات اعرف عميلك أو طلبات بخصوص مصدر الأموال
- عدم معرفة المرسل/ المستقبل لكافة التفاصيل أو تزويد المختصين بمعلومات غير دقيقة

بشأن الحوالة، مصدر الأموال، أو التعاون مع الأطراف الأخرى.

- تقديم العميل لمستندات مزورة أو إعداد صور مستندات تعريف كجزء من عملية الاعداد.

دراسة حالة ٨: رفض العميل للإدلاء بمعلومات عن مصدر الأموال

قامت المؤسسة المالية (البنك) بتعبئة تقرير الاشتباه في حوالة بخصوص حساب شركة محلية تحصل على الأموال من خلال بيع الكوبونات التي يمكن استخدامها مع المنتجات (البلاستيك الحيوي في هذه القضية). وقد تم إيداع الأموال من قبل الأشخاص الطبيعيين والقانونيين وبعض تلك الأموال أصلاً أصول افتراضية. وخلاف المتطلبات الإضافية للبنك، ممثلي صاحب الحساب لم يقوموا بتزويد البنك بأي معلومات عن مصدر تلك الأموال. وقد أشار تحقيق السلطات المختصة إلى أن الأموال تم إرسالها من قبل شركة ترتبط بأشخاص على علاقة وثيقة بالجريمة المنظمة كما أن الأموال تم الحصول عليها كانت من مشاريع احتيال.

المصدر: إيطاليا.

الملف

- يقدم العميل تعريفاً أو توثيقاً للحساب (مثال: عناوين تزويد الخدمة الغير مطابقة للمواصفات ، ملفات تعريف الارتباط) والتي يتم مشاركتها من قبل حساب آخر).
- التناقضات التي تطرأ بين عناوين تزويد الخدمة المرتبطة بملفات العملاء و عناوين تزويد خدمة الانترنت من مكان إجراء التحويلات.
- عنوان العميل الخاص بالأصول الافتراضية يظهر بشكل عام مرتبطاً بالنشاطات الغير قانونية.
- العميل المعروف من خلال المعلومات العامة المتوفرة لدى سلطات إنفاذ القانون نظراً لارتباطاته الاجرامية السابقة.

دراسة حالة ٩: ملف عميل لا يتطابق مع التجارة عالية القيمة في الأصول الافتراضية

قام المسؤول عن التبادل (مزود خدمة الأصول الافتراضية) والمؤسسة المالية) بتعبئة تقرير الاشتباه بحوالة مالية تتعلق بتجارة أصول افتراضية عالية القيمة والتي بدأت عندما تم فتح الحساب لدى المسؤول عن التبادل. كان لدى صاحب الحساب أصول افتراضية متعددة ويقوم بالشراء والبيع وبلغت التحويلات ١٨٠ ألف يورو والذي لا يتوافق مع ملف العميل (بما في ذلك الراتب والمنصب الوظيفي). وأظهرت التحقيقات بأن الأصول الافتراضية كانت تستخدم للتالي:

- التجارة عبر الانترنت المظلم
- المراهنة
- تحويلات عبر مزودي خدمة أصول افتراضية لا تخضع لتدابير مكافحة غسل الأموال وتمويل الإرهاب أو التي تورطت في تحقيقات غسل أموال سابقة بتحويل ملايين الدولارات
- عمليات على منصات تقدم خدمات تحويل العمل الافتراضية بخدمة (P2P).
- الخلط ، حيث استخدم صاحب الحساب أيضاً مختلف الوسائل (مثال: تحويل الأموال، البنوك الالكترونية، البطاقات مسبقة الدفع) لنقل مبالغ كبيرة خارج حسابه في نفس الوقت.

إن الأموال التي تلقاها صاحب الحساب يبدو أنها تأتي من شبكة من الأشخاص الذين اشتروا الأصول الافتراضية (بيتكوين) نقداً وتم تحديد أماكنهم في مختلف الدول في آسيا وأوروبا بما فيها إيطاليا عبر تحويل الأموال أو نظام البنك. حيث تلقى أيضاً أموال عبر بطاقات مسبقة الدفع من مواطنين يسكنون في إيطاليا وفي الخارج. هذه الأموال تم استخدامها في الحوالات الخارجية والقمار وتم سحبها عبر صرافات بنكية في إيطاليا.

المصدر: إيطاليا.

ملف وسيط نقل أموال غير مشروعة أو ضحية احتيال

- لا يبدو المرسل على معرفة بتقنية الأصول الافتراضية أو حلول المحفظة الالكترونية. هؤلاء الأشخاص يمكن أن يكونوا وسطاء لنقل الأموال غير المشروعة المتحصلة من غاسلي أموال محترفين أو يصبح ضحية الاحتيال وسيط لنقل الأموال غير المشروعة الذين يتم خداعهم لتحويل الأموال غير المشروعة دون معرفة أصلها.

- عندما يكون العميل أكبر من المعدل العمري لمستخدمي المنصة ويعمل على فتح حساب

ويرتبط بحوالات ضخمة ، مما يشير إلى أنه ضحية لمشروع ابتزاز مالي أكبر أو وسيط لنقل الأموال غير المشروعة.

- العميل عندما يكون سريع التأثر وضعيف الشخصية ويتم استخدامه غالباً من قبل تجار المخدرات لمساعدتهم في عملهم.

- العميل الذي يشتري كميات كبيرة من الأصول الافتراضية ليست متوافقة مع ثروته المتاحة أو ملف سجله المالي مما يشير لوجود غسل أموال، أو أنه وسيط لنقل الأموال غير المشروعة أو ضحية احتيال.

دراسة حالة ١٠: ضحية احتيال أصبح وسيط لنقل الأموال غير المشروعة.

في هذه القضية ضحايا استثمار، حيث تواصل أجنب مع متقاعدين كبيرين السن من خلال الاتصالات المباشرة، البريد الإلكتروني أو من خلال وسائل التواصل الاجتماعي وقدموا لهم فرص استثمارية في (بيتكوين) أو أي أصل مالي آخر ووعدهم بجني فوائد كبيرة نظراً لزيادة شعبية الأصول الافتراضية وأسعارها. الاستثمار الأساسي بمبلغ بسيط (في حالات كثيرة أقل من ٢٥٠ يورو) تم تحويلها من قبل

حسابات الضحايا أو عبر البطاقة الائتمانية أو خدمات دفع أخرى وانتهى بها المطاف في يد المجرمين. بدلاً من ذلك، تم توجيه الضحايا لتبديل العملة الورقية لبيتكوين باستخدام صرافات الأصول الافتراضية وتحويلها لعنوان محدد من قبل المجرمين.

ولم يكن لدى الضحايا أي خبرات في التقنية ولم يفهموا بشكل عام تقنية الأصول الافتراضية أو ما يستثمرون فيه. حيث طلب المجرمون أيضاً من الضحايا تثبيت تطبيق للتحكم بسطح المكتب عن بعد بحسابات محددة ليساعدوهم في تحويل المبالغ بشكل صحيح. مما اخترق حسابات الضحايا وأصبح بإمكان المجرمين التحويل دون علم الضحية بذلك مما يؤدي لعدم ملاحظة التحويل إلا عندما مشاهدة نقص الأموال من الحساب. في بعض القضايا، زور المجرمون مقالات تشير إلى أن مشاهير أو رجال أعمال أثرياء يروجون للأصول الافتراضية والاستثمار بها مما يعطي الضحايا شعوراً بالثقة والقناعة للاستثمار.

سلوكيات أخرى غير معتادة

- عندما يقوم العميل بتغيير بياناته التعريفية بما في ذلك البريد الإلكتروني وعنوان الإقامة، وعناوين تزويد خدمة الانترنت أو المعلومات

المالية والتي ربما بأن الحساب قد تم الاستيلاء عليه من قبل شخص آخر.

- عندما يحاول العميل الدخول لمنصة أو أكثر من منصات مزودي خدمة الأصول الرقمية من عناوين تزويد خدمة انترنت مختلفة طوال اليوم بشكل متكرر.

مؤشرات تنبيه (Redflags) وفقاً لمصدر الأموال أو الثراء

١٥. كما وضحت القضايا التي شاركتها الدول، فإن سوء استعمال الأصول الافتراضية غالباً يتعلق بأنشطة إجرامية، مثل تهريب المخدرات والمؤثرات العقلية، الاحتيال، السرقة والابتزاز (بما في ذلك الجرائم الالكترونية). تجردون أدناه التنبيهات (Redflags) الشائعة والمرتبطة بمصدر الأموال أو الثراء التي ترتبط بأنشطة إجرامية:

- عناوين حوالات الأصول الافتراضية أو بطاقات البنك المتصلة باحتيال معروف، ابتزاز أو برنامج خبيث، العناوين الخاضعة للعقوبة، مواقع التجارة بالانترنت المظلم أو أي مواقع أخرى غير قانونية.

- الحوالات الأصول الافتراضية التي تتحصل من المراهنة عبر الانترنت.
- استخدام بطاقة ائتمانية واحدة أو عدة بطاقات وربطها بمحفظة الاصول الافتراضية لسحب مبالغ كبيرة نقداً أو أموال لشراء الأصول الافتراضية سبق وأن تم إيداعها في البطاقة الائتمانية.
- الايداع في حساب أو عنوان الاصول الافتراضية بمبلغ أعلى من المعتاد بدون وجود مصدر لتلك الأموال ومتبوعاً بتحويل تلك الأموال لعملة نقدية مما يشير لسرقة أموال.
- غياب الشفافية أو أن المعلومات غير كافية عن مصدر ومالكي الأموال، مثل تلك المتعلقة باستخدام شركات وهمية أو تلك الأموال المودعة في أول طرح للعملة حيث تكون البيانات الشخصية للمستثمرين غير متوفرة أو الحوالات الواردة من أنظمة الدفع عبر الانترنت من خلال بطاقات ائتمانية أو بطاقات مسبقة الدفع متبوعاً بسحب المبلغ.
- أموال العميل التي يكون مصدرها طرف ثالث لخدمات التجارة أو إدارة المحافظ.

- أن يكون حجم مصدر ثروة العميل مستمداً من استثمارات في الأصول الالكترونية أو الطرح الأولي للعملة أو الاحتيايل... الخ.
- عندما يكون مصدر ثراء العميل من الأصول الافتراضية أو مزودي خدمة الأصول الافتراضية الذين لا يخضعون لمراقبة أنشطة غسل الأموال ومكافحة تمويل الارهاب.

دراسة حالة ١١ : استخدام الشركات الوهمية (Deep Dot Web)

الولايات المتحدة الأمريكية، مايو ٢٠١٩، صادرت سلطات إنفاذ القانون موقع (Deep Dot Web) بناءً على أمر من المحكمة. وقد تم اتهام الملاك والمسؤولين عن الموقع بالتآمر على غسل الأموال بملايين الدولارات حيث تلقوا عمولات لتمكين الأفراد من دخول المواقع التجارية بالانترنت المظلم من خلال مواقعهم. حيث أنهم يتلقون تلك العمولات ومن خلال روابط الاحالة والتي تمثل عمولة شراء بضائع غير مشروعة مثل الفنتنايل والهروين من قبل أفراد أيضاً أحيلوا للانترنت المظلم عبر نفس الموقع.

وكانت هذه العمولات على شكل أصول افتراضية وتم تحويلها لمحفظة بيتكوين الخاصة بالموقع. ولإخفاء مصدر تلك الأموال الغير مشروعة والتي تقدر قيمتها بأكثر من ١٥ مليون دولار أمريكي، قام الملاك والمشغلين بتحويل مدفوعات العمولات الغير مشروعة من المحفظة إلى محافظ بيتكوين أخرى ولحسابات تستخدم الشركات الوهمية للحصول على عمولاتهم ولتنفيذ نشاطات أخرى تتعلق بالموقع. وخلال خمس سنوات، تلقى الموقع ما يقارب ٨١٥٥ بتكوين على شكل عمولات من قبل مواقع التجارة بالانترنت المظلم وهو ما يساوي تقريباً ثمانية ملايين دولار أمريكي وتم العمل على تحويلها بشكل منتظم وبمبالغ محدودة. وقد تم تحويل عملات البيتكوين للمحفظة الخاصة بالموقع والتي يتحكم بها الجناة في أكثر من أربعين ألف تحويل وقد كانت تسحب بشكل متواصل لجهات متعددة وبلغت عدد الحوالات أكثر من ٢٧٠٠. وتقدر المبالغ المسحوبة من المحفظة ما يقارب خمسة عشر مليون دولار أمريكي.

المصدر: الولايات المتحدة

دراسة حالة ١٢: استخدام دور صرافة متعددة للعملة الافتراضية، وثائق هوية مزورة للعناية الواجبة بالعملاء و البطاقات مسبقة الدفع.

أدار المتهمون في هذه القضية عملية غسل أموال ترتبط
بمجرمين عبر الانترنت قاموا بتهكير تبادل أصول افتراضية
وسرقوا مبلغ يقدر بمائتين وخمسين مليون دولار منها. وتمكن
اثنين من المتهمين من غسل واحد وتسعين مليون دولار
أمريكي ومن ثم تسعة ملايين ونصف من المسروقات
الالكترونية.

وقد تم تتبع الأصول الافتراضية من خلال مئات التحويلات
وتبادل أصول افتراضية متعددة الأشكال. وقد استخدم
غاسلي تلك الأموال صورة طبيب و زوروا مستندات هويته في
بعض الحالات لخداع إجراءات اعرف عميلك. وتم تحويل
خمسة وثلاثين مليون دولار أمريكي لحسابات أجنبية وتم
استخدامها لشراء بطاقات مسبقة الدفع والتي ربما استبدلت
أيضاً بأصول افتراضية. وعمل المتهمون من خلال حسابات
مستقلة ومتراصة وقدموا خدمات حوالات عملات افتراضية
مثل تحويل عملات افتراضية إلى عملات ورقية لأشخاص
مقابل رسوم. كما تورط المتهمون في أعمال تجارية بالولايات
المتحدة.

المصدر: الولايات المتحدة

مؤشرات تنبيه (Redflags) المرتبطة بالمخاطر الجغرافية

١٦. توضح هذه المؤشرات كيف يكون لدى المجرمين الأولوية عند نقل أموالهم على عدة مستويات في دول تخضع لمعايير فريق العمل المالي -فاتف- في ما يتعلق بالأصول الافتراضية ومزودي خدمة الأصول الافتراضية. وبناءً على القضايا التي وردت من الدول، استغل المجرمون ثغرات أنظمة مكافحة تمويل الإرهاب وغسل الأموال المطبقة على الأصول الافتراضية لنقل أموالهم لدول لا تخضع لأنظمة مكافحة تمويل الإرهاب وأنشطة غسل الأموال. وقد لا يكون لدى الدولة أنظمة تتعلق بذلك ولا تقرير إبلاغ عن الاشتباه بحوالة لتغطية ما يتعلق بالأصول الافتراضية، أو لا يملكون أنظمة صارمة مقارنة لمعايير فريق العمل المالي -فاتف-. وحيث أن هذا التقرير لا يعمل على تحديد الدول "عالية المخاطر"، ولكن يجب على الكيانات المبلغة أن تأخذ بالحسبان المؤشرات التالية عندما يتعلق الأمر بالمخاطر الجغرافية. وهذه المخاطر مرتبطة مع مصدر، ووجهة وبلد التحويل. وكذلك على صلة بمخاطر منشئ-الحوالة والمستفيد من الأموال والذي ربما يكون

مرتبطاً بدولة عالية المخاطر. بالإضافة، إلى أنها ربما تكون مطبقة على العملاء من المواطنين والمقيمين أو مكان العمل.

- أموال الزبائن محولة من، أو مرسلة إلى، تبديل عملة في غير الدولة التي يوجد بها العميل أو مكان الاستبدال.

- فائدة العميل من استبدال الأصول الافتراضية في دولة ذات مخاطر عالية أو ليس لديها تنظيمات كافية تتعلق بأنشطة غسل الأموال ومكافحة تمويل الارهاب للأصول الافتراضية بما في ذلك إجراءات غير كافية بشأن اعرف عميلك والعناية الواجبة بالعملاء.

- عندما يرسل العميل أموال إلى مزودي خدمة الأصول الافتراضية التي ليس لديها تنظيمات خاصة بالأصول الافتراضية أو رقابة مطبقة بشأن غسل الأموال وتمويل الارهاب.

- عندما يقوم العميل بإنشاء مكاتب أو نقلها لدول ليس لديها قوانين تحكم الأصول الافتراضية أو إنشاء مكتب في دولة حيث لا يوجد عمل تجاري واضح.

دراسة حالة ١٣: تاجر بتكوين يملك عمل تجاري لنقل الأموال بدون الحصول على رخصة (عبر الحدود).

في أبريل ٢٠١٩، تلقى العميل حكماً بالسجن لمدة عامين لتشغيله نشاط نقل أموال بدون رخصة بعد بيع عملات بتكوين بآلاف الدولارات لأكثر من ١٠٠٠ عميل في الولايات المتحدة الأمريكية.

وأعلن عن خدمات عبر مواقع الأصول الافتراضية لدى المستخدمين، وواجه عدداً من المستخدمين شخصياً لقبوله المبالغ النقدية وتبديلها بعملات رقمية. ودفع له زبائن آخرين على الصعيد الوطني عبر الصرافات أو خدمات تحويل الأموال. وتلقى خمسة بالمائة كعمولة سائدة عند تنفيذ خدماته. وقد حصل في البداية على البتكوين عبر تبادلات في الولايات المتحدة، وعندما جذب الانتباه، أقفل حسابه. ومن ثم قام بالتغيير إلى تبادل عبر آسيا. وباستخدام ذلك التبادل، اشترى المتهم ٣.٢٩ مليون دولار أمريكي من البتكوين عن طريق مئات الحوالات المنفصلة ما بين مارس ٢٠١٥ و أبريل ٢٠١٧. كما اعترف المتهم بأنه قد بدل مبالغه النقدية التي يحتفظ بها في دول أجنبية للعملة الأمريكية وقد هرب خلال الفترة من نهاية ٢٠١٦ إلى بداية ٢٠١٨ مبلغ مليون دولار

للولايات المتحدة في مبالغ بسيطة جداً تقدر بعشرة آلاف دولار.

المصدر: الولايات المتحدة الأمريكية.

**نقل مزودي خدمات العملات الافتراضية أعمالهم إلى دول
ليس بها قوانين قوية تتعلق بأنشطة غسل الأموال
ومكافحة تمويل الإرهاب.**

قبل تنفيذ سياسة منع مزودي خدمة الأصول الافتراضية في دولة ما في آسيا في عام ٢٠١٧، بدأ مزودي تلك الخدمة بالانتقال من هذه الدولة إلى دولة أخرى في نفس المنطقة. في عام ٢٠١٨ قامت الدولة الثانية بالبداية بأنظمة ضد تمويل الارهاب وأنشطة غسل الأموال، وأعلن مزود خدمة الأصول الافتراضية بأنه سينتقل لبلد آخر ويقع في أوروبا (والتي لا تملك نظام قوي يتعلق بتمويل الارهاب وأنشطة غسل الأموال). في نوفمبر ٢٠١٨ قامت الدولة بتقديم أنظمة محددة بخصوص ذلك وفي عام ٢٠٢٠ جرى منع مزودي خدمة الأصول الافتراضية من العمل. وحسب التقارير الحالية لعام ٢٠٢٠ فقد انتقل مزودي تلك الخدمة إلى أفريقيا.

التوصيات

١٧. هذا التقرير تم إعداده بمشاركة أعضاء فريق العمل المالي- فاتف - في العالم ويهدف لتقديم أدوات عملية للقطاعات الحكومية والخاصة في التعرف والتحقق وكذلك إيقاف المجرمين في غسل الأموال وتمويل الارهاب ذات العلاقة بالأصول الافتراضية.

١٨. إن المؤشرات المذكورة في هذا التقرير محددة وأساسية وكذلك لا يمكن أن تنطبق في كافة الاوضاع حيث أن المؤشرات هي عنصر واحد من عدة عناصر تساهم في تقديم نظرة شاملة لاحتمالية وجود مخاطر غسل أموال أو تمويل إرهاب ومن المهم أن لا يؤخذ المؤشر بمعزل عن بقية المؤشرات ويجب الأخذ بها مع ما يتوفر من معلومات لدى السلطات المختصة.

١٩. مقارنة مبنية على المخاطر تم اعتماده في حديث ثنائي بين القطاع الخاص والقطاع الحكومي قد يحسن بلا شك من فاعلية التقارير. ولذلك نشجع السلطات المختصة لمشاركة هذا التقرير مع الكيانات المبلغة وأن تقوم بعقد ورش عمل لرفع الوعي وفهم ما احتواه هذا التقرير.

٢٠. بينما تتطور المؤشرات بشكل دائم ومستمر، هناك ممارسات إيجابية أخرى يمكن الاستفادة منها من

خلال الحصول على المعلومات من السلطات المحلية والمصادر المفتوحة. وقد تزود السلطات المختصة القطاع الخاص بالمؤشرات والمعلومات ذات العلاقة بالدولة. على سبيل المثال، استخدام المعلومات في هذا التقرير لإعداد تحذيراتهم للسلطات المبلغة. من ناحية أخرى، لا يجب أن يستخدم هذا التقرير كأداة للتحقق وقياس الامتثال أو قائمة تحقق عندما يتم مراقبة القطاع الخاص كما أن ليس كافة المؤشرات يمكن أن تنطبق على كافة البلدان أو المؤسسات.