ფულის გათეთრების საწინააღმდეგო პოლიტიკა: საფუძვლები

ნაწილი 7: ვირტუალური აქტივები

„ვირტუალური აქტივები“ განეკუთვნება აქტივების ახალ ფართო კლასს, რომელიც დაფუძნებულია განაწილებული რეესტრის (მონაცემთა ბაზის) ტექნოლოგიაზე (DLT). DLT ტექნოლოგია საერთო ქსელში მონაცემების სხვადასხვა ადგილას („დეცენტრალიზებულად“) შენახვის შესაძლებლობას იძლევა, რაც მონაწილეებს საშუალებას აძლევს, თვალი ადევნონ ვირტუალური აქტივების, როგორიცაა, მაგალითად ბიტკოინი, მფლობელობასა და გადაცემას. ვირტუალურ აქტივებს უნიკალური თავისებურებები, უპირატესობები და ნაკლოვანებები ახასიათებს ტრადიციულ აქტივებსა და გადახდებთან შედარებით. პროფესიონალი ბუღალტრები უნდა გაეცნონ იმ გზებსა და საშუალებებს, რომლის მეშვეობით ამ უნიკალური მახასიათებლების გამოყენება შეუძლიათ ფულის გამთეთრებლებსა და ტერორისტების დამფინანსებლებს ღირებული ნივთების/ქონების/აქტივების შესაძენად, გადასატანად და შესანახად ხშირად რეგულირებული (ლეგიტიმური) ფინანსური სისტემის ფარგლებს გარეთ და ფულადი სახსრების წარმოშობის წყაროს ან დანიშნულების შესანიღბად.

როგორ იყენებენ დამნაშავეები ბოროტად ვირტუალურ აქტივებს?

ფულის გათეთრების სქემაში ვირტუალური აქტივების ჩართვა შესაძლებელია ნებისმიერ ეტაპზე, მათ შორის:

- პრედიკატული დანაშაული: მაგალითად, ფულის მოზიდვა უკანონო საქმიანობის მეშვეობით, უკანონო საქონლის ან მომსახურების გაყიდვით ვირტუალურ აქტივებზე;
- განთავსება: უკანონოდ მოპოვებული ვირტუალური აქტივების გარდაქმნა ფიატურ ვალუტად (ფულად) ტრადიციული ფინანსური სისტემის ფარგლებში;
- დამალვა: როგორც წესი, კრიპტოვალუტებზე დაფუძნებულ ოპერაციებზე (ტრანზაქციებზე) შესაძლებელია თვალყურის დევნება ბლოკჩეინ ტექნოლოგიების მეშვეობით ჩატარებული ანალიზის მეშვეობით, თუმცა, შეიძლება არ არსებობდეს არანაირი კავშირი ტრანზაქციასა და რომელიმე კონკრეტულ პირს შორის, როდესაც ოპერაცია სრულდება რეგულირებული პერიმეტრის ფარგლებს გარეთ. გარდა ამისა, კრიპტოტრანზაქციებს შორის კავშირების გასაწყვეტად დამნაშავეებს შეუძლიათ ანონიმური მომსახურების გამოყენებაც, როგორიცაა „მიქშერების ან ტუმბლერების“ მომსახურება;
- დანაწევრება: ფიატური აქტივების ვირტუალურ აქტივებად გარდაქმნა, ვირტუალური აქტივების გაცვლა, სხვადასხვა სახის ვირტუალური აქტივის გადაცვლა და ვირტუალური აქტივების ფიატურ ვალუტად გარდაქმნა/გადაქცევა;
- ინტეგრაცია: „შავი“ ფიატური ფულის გათეთრების მსგავსად, ონლაინკომპანია, რომელიც კრიპტოვალუტით გადახდებს იღებს, შესაძლოა შექმნილი იყოს შემოსავლის ლეგიტიმაციისა და „შავი“ კრიპტოვალუტის გასათეთრებლად.

განმარტებები

ვირტუალური აქტივი (VA): ვირტუალური აქტივი არის ღირებულების ციფრული გამოსახულება, რომლის გადაცემა ან გადახდის განსახორციელებლად გამოყენება შესაძლებელია. იგი არ მოიცავს ციფრულ ფიატურ ვალუტას (ფულს).

კრიპტოვალუტა: კრიპტოგრაფიით დაცული დეცენტრალიზებული ვირტუალური აქტივი, რომლის გამოყენება შესაძლებელია გაცვლის, გადაცემის, შენახვის ან ელექტრონული ყიდვა-გაყიდვის საშუალებად. ათასობით კრიპტოვალუტიდან ყველაზე პოპულარულია ბიტკოინი და ეთერიუმი.

არაურთიერთშემცვლელი ტოკენი (NFT): სრულიად უნიკალური ვირტუალური აქტივი. მიუხედავად იმისა, რომ ბევრი ბიტკოინი არსებობს, თითოეული არაურთიერთშემცვლელი ტოკენის მხოლოდ ერთი ეგზემპლიარი არსებობს. ხშირად ეს არის ციფრული ხელოვნების ნაწარმოების კონკრეტული ნაწილი/ფრაგმენტი ან სხვა სახის ციფრული ან რეალური ქონება/საკუთრება.

ვირტუალური აქტივების მომსახურების პროვაიდერი (VASP): საწარმო, რომელიც უზრუნველყოფს რომელიმე ქვემოთ ჩამოთვლილ მომსახურებას:

- ვირტუალური აქტივებისა და ფიატური ვალუტის გადაცემა ან გაცვლა, ან სხვადასხვა სახის ვირტუალური აქტივის გადაცვლა.
- ვირტუალური აქტივების შენახვა/ადმინისტრირება;
- ვირტუალური აქტივების გამოშვებასთან დაკავშირებული ფინანსური მომსახურება.

ვირტუალური ვალუტის საფულე: ვირტუალური აქტივების ფლობის, შენახვისა და გადაცემის საშუალება.

მაგალითი

„გამომძალველი პროგრამით“ კიბერშეტევა კომპანია „კოლონიურ მილსადენზე“ (Colonial Pipeline)

ვირტუალური აქტივები სწრაფად გადაიქცა გამოსასყიდის გადახდის ყველაზე გავრცელებულ ფორმად „გამომძალველი პროგრამებით“ კიბერშეტევებისთვის, რასაც სულ უფრო ხშირად აწყდებიან პრაქტიკაში პროფესიონალი ბუღალტრები, კერძოდ, აუდიტორები და მათი დამკვეთები.

ამერიკის შეერთებულ შტატებში კომპანია Colonial Pipeline-ზე განხორციელებული კიბერშეტევა არის გამომძალველი პროგრამების შეტევის ერთ-ერთი თვალსაჩინო მაგალითი, რომელსაც კომპანიები რეგულარულად განიცდიან. 2021 წლის მაისში, კომპანია Colonial Pipeline-ზე განხორციელდა მასშტაბური კიბერშეტევა გამომძალველი პროგრამის მეშვეობით, რის შედეგადაც კომპანიის საქმიანობა ხუთი დღით გაჩერდა.

თავდამსხმელებმა გამოსასყიდის სახით მოითხოვეს 75 ბიტკოინი, 4.4 მლნ აშშ დოლარის ეკვივალენტი, რომელიც Colonial Pipeline-მა გადაიხადა. მართალია, სახელმწიფო ხელისუფლების ორგანოებმა შეძლეს გამოსასყიდი თანხის დიდი ნაწილის დაბრუნება, მაგრამ შემდგომი გამოკვლევიდან გამოჩნდა, რომ წინა წელს ამ თავდამსხმელებმა ბიტკოინების სახით მიიღეს 90 მლნ აშშ დოლარზე მეტი გამოსასყიდი თანხა 47 სხვადასხვა წყაროდან.

საბოლოოდ, აუცილებელი იქნება ზემოაღნიშნული უკანონო შემოსავლების ინტეგრირება ლეგიტიმურ ფინანსურ სისტემაში, რაც პოტენციურად პროფესიონალი ბუღალტრებისთვის ქმნის იმის შესაძლებლობას, რომ გამოავლინონ ასეთი დანაშაული და განაცხადონ ამის შესახებ. ამავდროულად, გამომძალველი პროგრამის მეშვეობით განხორციელებული კიბერშეტევები ხაზს უსვამს კიბერუსაფრთხოების ეფექტური კონტროლის მნიშვნელობას.

⚠ საფრთხის მაუწყებელი ძირითადი ნიშნები

გამოიყენება ფულის გათეთრებისათვის დამახასიათებელი საფრთხის მაუწყებელი „ტრადიციული“ ძირითადი ნიშნები. გარდა ამისა, არსებობს სხვა ნიშნებიც:

- დამკვეთის ქონების/სიმდიდრის წყაროს უდიდესი ნაწილი წარმოიქმნება ვირტუალურ აქტივებში განხორციელებული ინვესტიციებიდან, ყოველგვარი წერილობითი დოკუმენტაციის გარეშე;
- დამკვეთის ქონების წყაროს არაპროპორციულ ნაწილს წარმოადგენს ვირტუალური აქტივები, რომლებიც მიღებულია ვირტუალური აქტივების მომსახურების პროვაიდერებიდან, რომელთაც არ გააჩნიათ ფულის გათეთრების/ტერორიზმის დაფინანსების წინააღმდეგ ბრძოლის სფეროს კონტროლის მექანიზმები;
- დამკვეთი იყენებს ვირტუალური აქტივების ბირჟებს მაღალი რისკის მქონე იურისდიქციაში, სადაც არ არსებობს ფულის გათეთრების/ ტერორიზმის დაფინანსების წინააღმდეგ ბრძოლის სფეროს კონტროლი;
- დამკვეთი ხშირად იცვლის საიდენტიფიკაციო ინფორმაციას, მათ შორის ელფოსტისა და IP მისამართებს.

კრიპტოფულის გათეთრების ბოლოდროინდელ სქემებში გამოყენებული იყო შემდეგი:

- კრიპტოვალუტების არარეგულირებული ბირჟები (რომლებიც არ შეესაბამება ფულის გათეთრების წინააღმდეგ ბრძოლის/იცნობდე შენს კლიენტს პროცედურის მოთხოვნებს);
- აზარტული თამაშების და სათამაშო ვებგვერდები;
- „მიქშერების ან ტუმბლერების“ მომსახურება (მაგ., Anonymix);
- კრიპტოვალუტის ბანკომატები, რომლისთვისაც დამახასიათებელია რისკების სუსტი მართვა;
- წინასწარ გადახდილი კრიპტოვალუტის სადებეტო ბარათები.

მნიშვნელოვან ოპერაციებს, რომელშიც ზემოაღნიშნული პროდუქტები/მომსახურება გამოიყენება, ბუღალტრებმა კიდევ ერთხელ უნდა გადახედონ და დეტალურად გამოიკვლიონ.

ბოლოდროინდელი დამატებები FATF სტანდარტებში

ტერმინები „ვირტუალური აქტივი“ და „ვირტუალური აქტივების მომსახურების პროვაიდერი“ ახალი დამატებებია FATF სტანდარტის ტერმინების გლოსარში. ეს ტერმინები გლოსარს 2018 წელს დაემატა. ამავდროულად, ვირტუალური აქტივების მომსახურების პროვაიდერები შევიდნენ FATF-ის მარეგულირებელ ბაზაში. ფულის გათეთრებისა და ტერორიზმის დაფინანსების წინააღმდეგ ბრძოლის კონტექსტში, უფრო დეტალური ინფორმაციის მისაღებად ვირტუალური აქტივებისა და ვირტუალური აქტივების მომსახურების პროვაიდერების შესახებ იხილეთ FATF-ის „განახლებული სახელმძღვანელო რისკზე დაფუძნებული მიდგომის გამოყენების შესახებ ვირტუალური აქტივებისა და ვირტუალური აქტივების მომსახურების პროვაიდერების მიმართ“.

რა შემთხვევაში უნდა თქვათ უარი გარიგებაზე?

- მოთხოვნილი მომსახურება შეიძლება სპეციალიზებული ხასიათის იყოს, რომელიც სცილდება თქვენი კომპეტენციის ფარგლებს.
- არ არსებობს სავაჭრო ან საინვესტიციო საქმიანობის/ოპერაციების ჩანაწერები, სადაც დეტალურად არის აღწერილი ფულადი სახსრების წარმოშობის წყარო.
- თქვენ ეჭვი გაქვთ ვირტუალური აქტივის, მისი ემიტენტ(ებ)ისა და ბირჟ(ებ)ის რეპუტაციის შესახებ.
- არ არსებობს ემიტენტ(ებ)ისა და ბირჟ(ებ)ის მიერ დაწესებული კონტროლის მექანიზმები ფულის გათეთრების/ტერორიზმის დაფინანსების წინააღმდეგ ბრძოლის სფეროსთვის.
- ეჭვი გეპარებათ დამკვეთის მიერ მოწოდებული ინფორმაციის სისწორეში, ან სხვა ეჭვები გაქვთ თავად დამკვეთთან დაკავშირებით.

დამატებითი დახმარება

ფულის გათეთრების წინააღმდეგ ბრძოლასთან დაკავშირებული ზოგადი მითითებების გასაცნობად იხილეთ FATF-ის „სახელმძღვანელო მითითებები ბუღალტერიის პროფესიის რისკზე დაფუძნებული მიდგომის შესახებ“. ხოლო ადგილობრივი დეტალური ინფორმაციის მისაღებად, მათ შორის, შესაბამისი მარეგულირებელი მოთხოვნების შესახებ, დაუკავშირდით ბუღალტერთა პროფესიულ ორგანიზაციას, რომლის წევრიც ხართ.

ანგარიშის წარდგენა საეჭვო საქმიანობის შესახებ (SAR)

თუ ეჭვი გაგიჩნდებათ, რომ აქტივების გადაცემას შესაძლოა უკავშირდებოდეს დანაშაულებრივი აქტივობა ან უკანონო შემოსავლები, მაშინ შეგიძლიათ ფინანსური მონიტორინგის ადგილობრივ ორგანოს წარუდგინოთ ანგარიში საეჭვო საქმიანობის შესახებ. ზოგიერთ იურისდიქციაში ამგვარი ანგარიშის წარდგენა პროფესიონალი ბუღალტრის სამართლებრივი ვალდებულებაა.

IFAC International Federation of Accountants®
529 FifthAvenue, NewYork 10017
www.ifac.org | +1 (212) 286-9344 | @ifac | company/ifac

ICAEW
www.icaew.com
@icaew | company/icaew

Copyright © September 2020 bytheInternationalFederationofAccountants (IFAC) andthe INSTITUTE OF CHARTERED ACCOUTANTS IN ENGLAND AND WALES (ICAEW). Allrightsreserved. Usedwithpermissionof IFAC andICAEW.Contact permissions@ifac.org forpermissiontoreproduce, storeortransmit, ortomakeothersimilarusesofthisdocument.

ბუღალტერთა საერთაშორისო ფედერაციის (IFAC) თანხმობით მის მიერ ინგლისურ ენაზე გამოცემული დოკუმენტი „ფულის გათეთრების საწინააღმდეგო პოლიტიკა: საფუძვლები - ნაწილი 7: ვირტუალური აქტივები“ - ქართულ ენაზე ითარგმნა და გამოქვეყნდა საქართველოს პროფესიონალ ბუღალტერთა და აუდიტორთა ფედერაციის მიერ. IFAC-ის მიერ დამტკიცებულ ტექსტს წარმოადგენს მის მიერ გამოცემული ინგლისურენოვანი ვერსია. IFAC თავის თავზე არ იღებს პასუხისმგებლობას თარგმანის სისწორესა და სისრულეზე, არც მისგან გამომდინარე არანაირ ქმედებაზე.

„ფულის გათეთრების საწინააღმდეგო პოლიტიკა: საფუძვლები - ნაწილი 7: ვირტუალური აქტივები“ - ინგლისურენოვანი ვერსია © [2020], IFAC. ყველა უფლება დაცულია.

„ფულის გათეთრების საწინააღმდეგო პოლიტიკა: საფუძვლები - ნაწილი 7: ვირტუალური აქტივები“ - ქართულენოვანი ვერსია © [2022], IFAC. ყველა უფლება დაცულია.

სათაური ინგლისურ ენაზე: Anti-money laundering: The Basics – Installment 7: Virtual Assets.

წინამდებარე დოკუმენტის გავრცელების, შენახვისა და გადაცემის, ან ნებისმიერი სხვა სახით მისი გამოყენების თაობაზე დაუკავშირდით IFAC-ს: *Permissions@ifac.org*