ФАТФ-ын тайлан

Виртуал хөрөнгийн

Мөнгө угаах, терроризмыг санхүүжүүлэхтэй холбоотой байж болох **шинж тэмдгүүд**

2020 оны 9-р сар

Санхүүгийн арга хэмжээ авах байгууллага (ФАТФ) нь олон улсын санхүүгийн системийг мөнгө угаах, терроризмыг санхүүжүүлэх болон үй олноор хөнөөх зэвсэг дэлгэрүүлэхийг санхүүжүүлэхээс хамгаалах, урьдчилан сэргийлэх бодлого боловсруулах болон түгээн дэмжих үүрэг бүхий засгийн газар хоорондын бие даасан байгууллага юм. ФАТФ-ын Зөвлөмжийг олон улсын мөнгө угаах болон терроризмыг санхүүжүүлэхтэй тэмцэх стандарт гэж хүлээн зөвшөөрдөг.

ФАТФ-тай холбоотой нэмэлт мэдээллийг доорх цахим хуудаснаас авна уу.
www.fatf-gafi.org

Энэ баримт бичиг, ашигласан газрын зураг нь аливаа нутаг дэвсгэр, хот болон бүс нутгийн статус, тусгаар тогтнол, олон улсын хил хязгаарыг хөндөх зорилго агуулаагүй болно.

Орчуулгыг: Санхүүгийн мэдээллийн алба. 2022.01.31

ФАТФ (2020), Виртуал хөрөнгийн - Мөнгө угаах, терроризмыг санхүүжүүлэхтэй холбоотой байж болох шинж тэмдгүүд, ФАТФ, Парис, Франц Улс
www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html

© 2020 FATF/OECD. Зохиогчийн эрх хуулиар хамгаалагдсан.

Урьдчилсан бичгээр зөвшөөрөл аваагүй тохиолдолд хэвлэх, хуулбарлах болон орчуулахыг хориглоно. Нийтээр нь болон хэсэгчилэн хэвлэхтэй холбоотой зөвшөөрлийн хүсэлтийг ФАТФ-ын Нарийн бичгийн даргын газарт хүлээн авна: 2 рью Андре Паскал 75775 Парис хот Цедекс 16, Франц Улс (Факс: +33 1 44 30 61 37, э-мэйл: contact@fatf-gafi.org)

Зургийг: ©Gettyimages

Агуулга

Товчилсон үгсийн жагсаалт

ВХ	Виртуал хөрөнгө
ВХҮҮ	Виртуал хөрөнгийн үйлчилгээ үзүүлэгч
ЗТ	Зөвлөмжийн тайлбар
МУТС	Мөнгө угаах, терроризмыг санхүүжүүлэх
МҮЭ	Мэдээлэх үүрэгтэй этгээд
СБ	Санхүүгийн байгууллага
СББМҮҮ	Санхүүгийн бус бизнес, мэргэжлийн үйлчилгээ үзүүлэгч
СГТ	Сэжигтэй гүйлгээний тайлан
СМА	Санхүүгийн мэдээллийн алба
ТС	Терроризмыг санхүүжүүлэх
ХСБ	Хууль сахиулах байгууллага
ХТМ	Харилцагчийг таньж мэдэх
ФАТФ	Санхүүгийн арга хэмжээ авах байгууллага

©FATF/OECD 2020

Танилцуулга

1. Виртуал хөрөнгө (ВХ) болон холбогдох үйлчилгээнүүд нь санхүүгийн инноваци, бүтээмжийг нэмэгдүүлэхийн хажуугаар тэдгээрийн өвөрмөц онцлог нь мөнгө угаах, терроризмыг санхүүжүүлэх болон бусад суурь гэмт хэрэг үйлдэж буй этгээдэд гэмт хэргийн замаар олсон хөрөнгө, орлогоо хувиргах болон хууль бус үйл ажиллагаагаа санхүүжүүлэх шинэ боломжийг олгож байна. Хил дамнасан гүйлгээг хурдан хийх нь гэмт хэрэгтнүүдэд хөрөнгө, мөнгийг зохицуулалттай санхүүгийн системээс гадуур, дижитал хэлбэрээр авах, шилжүүлэх болон хадгалах боломжийг олгодог төдийгүй хөрөнгийн гарал үүсэл, хүлээн авагчийг бүдгэрүүлж, мэдээлэх үүрэгтэй этгээдэд сэжигтэй үйл ажиллагааг цаг тухайд нь таньж илрүүлэхэд хүндрэл учруулдаг. Эдгээр хүчин зүйлүүд нь дотоодын эрх бүхий байгууллагуудад гэмт хэргийн шинжтэй үйлдлийг илрүүлэх, мөрдөн шалгахад мөн бэрхшээл учруулж байна.

2. Санхүүгийн арга хэмжээ авах байгууллага (ФАТФ) нь 2018 оны 10 дугаар сард улс орнуудад ВХ-ийн үйл ажиллагаатай холбоотой үүсэх мөнгө угаах, терроризмыг санхүүжүүлэх (МУТС) эрсдэлийг бууруулахад дэмжлэг үзүүлэх, дэлхийн санхүүгийн системийн найдвартай байдлыг хамгаалах зорилгоор ВХ болон Виртуал хөрөнгийн үйлчилгээ үзүүлэгч (ВХҮҮ)-ийн үйл ажиллагаанд ФАТФ-ын стандартыг хэрхэн ашиглахыг тодорхой болгох үүднээс Стандартуудаа шинэчилсэн. Улмаар 2019 оны 6 дугаар сард Зөвлөмж 15-ын тайлбар (ЗТ.15)-ыг баталсан бөгөөд ВХ болон ВХҮҮ-ийн үйл ажиллагаанд, тэр дундаа сэжигтэй гүйлгээг илрүүлж мэдээлэхэд ФАТФ-ын стандарт, шаардлагуудыг хэрхэн ойлгож ашиглах талаар илүү тодорхой тайлбарласан болно.

3. ФАТФ нь ВХ-тэй холбоотой МУТС шинж тэмдгүүдийн талаарх энэхүү товч тайланг аливаа мэдээлэх үүрэгтэй этгээд (МҮЭ), санхүүгийн байгууллага (СБ), санхүүгийн бус бизнес, мэргэжлийн үйлчилгээ үзүүлэгчид (СББМҮҮ) болон ВХҮҮ-дэд ВХ-тэй холбоотой мөнгө угаах, терроризмыг санхүүжүүлэх сэжигтэй үйл ажиллагааг таньж илрүүлэх, мэдээлэхэд туслалцаа, дэмжлэг үзүүлэх зорилгоор бэлтгэн гаргаж байна. Мөн энэхүү тайлан нь МҮЭ-дэд харилцагчийг таньж мэдэх (ХТМ) үйл ажиллагааг хэрэгжүүлэхдээ эрсдэлд суурилсан аргачлалыг ашиглан харилцагч болон эцсийн өмчлөгчийг хэн болохыг мэдэх, түүний бизнесийн харилцааны мөн чанар, зорилго, хөрөнгийн эх үүсвэрийг тодорхойлоход дэмжлэг үзүүлэх зорилготой юм.

4. Санхүүгийн мэдээллийн алба (СМА), хууль сахиулах байгууллага (ХСБ) болон прокурорын байгууллага нь СГТ-д дүн шинжилгээ хийх болон хууль бусаар ашиглагдаж буй ВХ-ийг илрүүлэх, мөрдөн шалгах, хөрөнгө хураах ажиллагааг сайжруулахад энэхүү тайланг ашиглах боломжтой.

5. Нөгөө талаас санхүүгийн байгууллага, СББМҮҮ болон ВХҮҮ-ийг зохицуулагч байгууллагууд нь МҮЭ-ийн МУТСТ, урьдчилан сэргийлэх үйл ажиллагааг хэрхэн хэрэгжүүлж байгаад хяналт тавихад ч энэ тайлан дахь мэдээллийг ашиглаж болно. Хэрэв МҮЭ нь бизнесийн логик тайлбаргүй нэг буюу хэд хэдэн шинж тэмдэг илэрсэн, харилцагчийн зөрүүтэй тайлбарыг харгалзалгүй СГТ мэдүүлээгүй, гүйлгээний талаар

©FATF/OECD 2020

нэмэлт тодруулга аваагүй тохиолдолд эрх бүхий байгууллагууд нь МҮЭ-дийн бизнесийг харгалзан илүү дэлгэрэнгүй нягтлан үзэж болно.

Шинж тэмдгүүдийг боловсруулахад ашигласан аргачлал, эх сурвалж

6. Энэхүү тайланд тусгагдсан сэжигтэй шинж тэмдгүүд нь улс, орнуудын 2017-2020 оны хооронд ирүүлсэн зуу гаруй кейс судалгаа, “ВХ-тэй холбоотой санхүүгийн мөрдөн шалгах ажиллагааны талаарх ФАТФ-ын тайлан”-ийн үр дүн (2019 оны 6-р сар) болон ФАТФ-аас гаргасан “Виртуал валюттай холбоотой үндсэн тодорхойлолтууд болон МУТС эрсдэлүүд” (2014 оны 6-р сар) зэрэг тайлангууд болон ВХ-ийг зүй бусаар ашигласан олон нийтэд нээлттэй мэдээлэлд үндэслэсэн боловсруулсан болно.

ВХ-ийг МУТС-д ашиглах хандлага

ВХ-тэй холбоотой гэмт хэргийн дийлэнх нь суурь болон мөнгө угаах гэмт хэргүүдтэй холбоотой байгаа хэдий ч гэмт хэрэгтнүүд санхүүгийн зорилтот хориг арга хэмжээнээс зайлсхийх, терроризмыг дэмжих хөрөнгө босгохын тулд ВХ-ийг ашигласан байна.

Улс орнуудад бүртгэгдсэн ВХ-тэй холбоотой гэмт хэргийн төрөлд МУ, хориотой бодис болон бусад хориотой бараа (галт зэвсэг гэх мэт) худалдах, залилан мэхлэх, татвараас зайлсхийх, компьютерийн гэмт хэрэг (жишээ нь, кибер халдлага үйлдэн хулгайлах), хүүхдийн мөлжлөг, хүний наймаа, хориг арга хэмжээнээс зайлсхийх, ТС зэрэг багтсан байна. Эдгээрийн дотроос хамгийн түгээмэл гарсан нь хориотой бодисын хууль бус наймаа бөгөөд борлуулалтыг нь ВХ-өөр хийх болон МУ-ын үйл ажиллагааны нуун далдах үе шатанд ВХ-ийг ашиглах явдал юм. Дараагийн түгээмэл үйлдэгдсэн гэмт хэрэг нь залилан, луйвар, рэнсомвэйр (ransomware) болон дээрмийн гэмт хэргүүд байсан байна. Сүүлийн үед мэргэжлийн МУ сүлжээнүүд нь ВХ-ийг орлого шилжүүлэх, цуглуулах, нуун далдлах нэг хэрэгсэл болгон ашиглаж эхэлсэн байна.

Эх сурвалж: 2017-2020 онуудад улс орнуудаас ирүүлсэн кэйс судалгаа

Тайлантай танилцахад анхаарах зүйлс

7. Эдгээр шинж тэмдгүүд нь ВХ-ийн шинж чанар болон тэдгээртэй холбоотой санхүүгийн үйл ажиллагааны онцлогт илүү тулгуурласан бөгөөд бүх үзүүлэлтийг хамраагүйг анхаарна уу. ВХ ашиглахтай холбоотой сэжигтэй үйл ажиллагаа нь албан ёсны мөнгөн тэмдэгт (fiat money) болон бусад хөрөнгийг ашиглаж үйлдэх МУТС үйл ажиллагаатай ижил шинж чанартай байж болно. Иймд МҮЭ нь харилцагч, бүтээгдэхүүн, үйл ажиллагаанаас учирч болох эрсдэл болон уламжлалт эрсдэлийн шинж тэмдгүүд байгаа эсэхийг анхаарах хэрэгтэй. Мөн сэжигтэй гүйлгээний шинж тэмдгүүдийг үргэлж тухайн тохиолдлын нөхцөл байдалтай уялдуулан авч үзэх хэрэгтэй.

©FATF/OECD 2020

8. Эдгээр шинж тэмдгүүдийг улс орнууд цаашид хөгжүүлэн дэлгэрүүлж эрх бүхий байгууллагуудын мэдээлэлтэй нэгтгэн боловсруулж төр, хувийн хэвшлийн хамтын ажиллагааны хүрээнд харилцагчийн төрөл төдийгүй өөрсдийн эрсдэлийн нөхцөл байдал, харилцагчийн төрөл, МҮЭ-ийн онцлог байдлыг харгалзан тогтмол шинэчлэх нь нээлттэй. Шинж тэмдэг илэрсэн гэдэг нь МУ эсвэл ТС байж болзошгүй гэж үзэх сэжиглэх үндэслэл болохгүй хэдий ч цаашид нягтлах, дэлгэрүүлж шалгах шаардлагатайг илэрхийлж байгаа юм. Гол нь харилцагч өөрөө тухайн гүйлгээний зорилго, сэжигтэй шинж тэмдэг зэргийг зөвтгөх тайлбар гаргах боломжтой гэдгийг санах хэрэгтэй.

9. Эрх бүхий байгууллага, СБ, СББМҮҮ болон ВХҮҮ-дэд зарим шинж тэмдгүүд гүйлгээний ерөнхий хяналтыг хийх үед илүү хялбар ажиглагдах боломжтой байхад зарим шинж тэмдгүүд гүйлгээний тусгайлсан хяналтыг хийхэд илүү ажиглагдаж болохыг анхаарах хэрэгтэй. Нэг буюу хэд хэдэн шинж тэмдгүүд илрэх нь тухайн байгууллага болон ВХҮҮ-ийн санал болгож буй бизнесийн чиглэл, бүтээгдэхүүн, үйлчилгээ болон харилцагчидтай хэрхэн харьцаж байгаагаас мөн хамаарч болдог. Нэг буюу хэд хэдэн шинж тэмдэг илэрсэн төдийгүй хууль ёсны эдийн засаг, бизнесийн тодорхой зорилгогүй байх тохиолдолд МҮЭ-дэд МУ эсвэл ТС-тэй холбоотой гэсэн сэжиг төрөх магадлал өндөр байх болно[1]. Эдгээр шинж тэмдгүүд нь СГТ мэдээлэх эсэхийг тодорхойлох цорын ганц хүчин зүйл байж болохгүй. МҮЭ нь МУТС гэмт хэрэг үйлдсэн гэдгийг мэдсэн, сэжиглэсэн эсвэл болзошгүй гэж үзэх хангалттай үндэслэлтэй бол СГТ мэдээлдэг байх хэрэгтэй.

Шинж тэмдгүүд

10. Дараах хэсгүүдэд ФАТФ-ын глобал сүлжээгээр 2017 оноос хойш цуглуулсан зуу гаруй тохиолдлын судалгаа, ном зохиолын тойм, нээлттэй эх сурвалжийн судалгаагаар тогтоогдсон сэжигтэй ВХ-ийн үйл ажиллагаа эсвэл ХСБ-ын шалгалтаас зайлсхийх оролдлогын талаарх сэжигтэй гүйлгээний шинж тэмдгүүдийг тусгалаа. Өмнө дурдсанчлан, нэг шинж тэмдэг байгаа нь заавал гэмт хэргийн шинжтэй үйлдлийг илэрхийлэх албагүй. Ихэнхдээ гүйлгээнд бизнесийн логик тайлбаргүй олон шинж тэмдгүүд илрэх нь гэмт хэргийн шинжтэй үйл ажиллагааны сэжиглэлийг төрүүлдэг. Шинж тэмдэг илэрч байгаа нь цаашид нягтлах, дэлгэрүүлж шалгах шаардлагатай бол гүйлгээг мэдээлэхийг дэмжиж байгаа гэсэн үг юм.

Гүйлгээтэй холбоотой шинж тэмдгүүд

11. Олон нийт ВХ-ийг төдийлөн өргөн ашиглаагүй хэвээр байгаа ч гэмт хэрэгтнүүд хэрэглэх нь улам нэмэгдэж байна. Анх 10 гаруй жилийн өмнө ВХ-ийг МУ зорилгоор ашиглах үйлдэл гарсан бөгөөд ВХ-ийг гэмт хэрэгт ашиглах нь улам бүр түгээмэл болж байна. Мөн

[1] Хэд хэдэн шинж тэмдгүүд нь МУ болон ТС тохиолдлуудын аль алинд нь хамаарч болно, жишээлбэл: хөрөнгө босгох үйл ажиллагаа, гадаадын террорист этгээдүүдийг санхүүжүүлэх, ВХ ашиглан зэвсэг худалдан авах гэх мэт. Үүнтэй холбоотойгоор ФАТФ-аас гаргасан Терроризмыг санхүүжүүлэх үйл ажиллагааг илрүүлэх: Холбогдох эрсдэлийн үзүүлэлтүүд (2016 оны 6-р сар) хаалттай тайлантай танилцана уу.

©FATF/OECD 2020

төлбөр тооцооны уламжлалт арга хэрэгсэлийн гүйлгээнийй сэжигтэй шинж тэмдгүүд нь ВХ-ийн хууль бус үйл үйл ажиллагааг илрүүлэхэд хамааралтай болохыг харуулж байна.

Гүйлгээний давтамж болон хэмжээтэй холбоотой шинж тэмдгүүд

- ВХ-ийн гүйлгээг (жишээ нь арилжаа болон шилжүүлэг) бэлэн мөнгөтэй ижил баримт материал хадгалах болон мэдээлэх босго дүнгээс доогуур, жижиг дүнгээр хуваан хийх;
- Өндөр дүнтэй олон гүйлгээ хийх
    - Ойрхон давтамжтай, тухайлбал 24 цагийн дотор;
    - Огцом өөрчлөгдсөний дараа хэвийн гүйлгээ хийгдэх, түүний дараа урт хугацаанд ямар нэг гүйлгээ хийгдэхгүй байх ялангуяа рэнсомвэйртэй (ransomware) холбоотой кейсийн үед их тохиолддог;
    - Шинээр нээсэн болон өмнө нь идэвхгүй байсан данс ашиглах.

- ВХ-ийг богино хугацаанд хэд хэдэн ВХҮҮ нарт шилжүүлэх, ялангуяа гадаад улсад бүртгэлтэй ВХҮҮ болон үйл ажиллагаа нь гадаадад явагддаг бол -
    - Харилцагчийн оршин суугаа газар болон бизнесийн үйл ажиллагаатай ямар нэгэн холбоогүй улс орон руу шилжүүлэх;
    - МУТСТ тогтолцоогүй болон сул тогтолцоотой улс орон руу шилжүүлэх.

- ВХ-ийг биржид хадгалж байснаа гэнэт –
    - Өөр ВХ-өөр солих ажиллагаа хийхгүйгээр ВХ-ийг шаардлагагүй гүйлгээний шимтгэл төлж эргүүлэн татах;
    - Ямар нэгэн бизнесийн үндэслэл тайлбаргүйгээр (портфолио үүсгэх г.м.), нэмэлт гүйлгээний төлбөр төлж ВХ-ийг олон төрлийн ВХ-д хувиргах;
    - ВХҮҮ-ээс ВХ-ийг эргүүлэн татаж хувийн хэтэвчиндээ шууд авах. Энэ нь бирж болон ВХҮҮ-ийг мөнгө угаахад ашиглаж буй хэлбэр юм.

- Хулгайлагдсан болон луйвардсан гэж сэжиглэж буй хөрөнгө хүлээн авах –
    - Хулгайн хөрөнгийг өөртөө байршуулж байсан эсвэл хулгайн хөрөнгийг эзэмшигчтэй холбоотой ВХ-ийн хаягаас хөрөнгө шилжүүлэх.

Кейс 1. Гадаадын ВХҮҮ руу олон удаагийн хийсэн өндөр дүнтэй ВХ-ийн шилжүүлэг

Дотоодын ВХҮҮ нь хэсэг хүмүүс өндөр дүнтэй ВХ худалдан авч, гадаадын улсад байрлах ВХҮҮ рүү шилжүүлж байгаатай холбоотой СГТ мэдээлсэн байна. Зарим хүмүүс нь ижил оршин суух хаягтай байсан бөгөөд ихэнх ВХ-ийн хаягууд руу ижил IP хаягаас хандсан нь мэргэжлийн мөнгө угаагчид хууль бус орлогоо угаахын тулд хөлсөлсөн байж болзошгүйг харуулж байв.

Эдгээр хүмүүс нь ВХ худалдаж авахаас өмнө албан ёсны мөнгөн тэмдэгтийг олон шат дамжлагаар нуун далдлах ажлыг зохион байгуулсан бөгөөд хөрөнгийн гарал үүслийг нуун дарагдуулахын тулд эхлээд бэлэн мөнгийг төрөл бүрийн СБ-ийн олон дансанд

©FATF/OECD 2020

байршуулжээ. Дараа нь эдгээр хөрөнгийг тухайн улсад бүртгэлтэй хуулийн этгээдийн эзэмшдэг дансууд руу шилжүүлсэн бөгөөд тухайн дансууд руу цахим хэлбэрээр бага дүнтэй шилжүүлгүүд хийсэн байв. Үүний дараа дотоодын BXYY-ийн данс руу орохоос өмнө өөр бас хэсэг бүлэг данс руу мөнгө шилжүүлсэн ба BX-ийг худалдан авмагцаа гадаадын BXYY-д шилжүүлжээ. Энэ хэрэгт 150 гаруй хүн холбогдсон бөгөөд нийт 108,352,900.00 ам.доллар (эсвэл 11,960 биткойн)-ыг бусад улсын хоёр BXYY-ийн олон тооны BX-ийн данс руу шилжүүлсэн байв.

Эх сурвалж: Өмнөд Африк

Кейс 2. Гадаадын BXYY рүү олон удаагийн шилжүүлгээр олон тооны BX-ийг шилжүүлсэн

Дотоодын BX-ийн биржийн мэдээлснээр фишинг (нэг хэлбэрийн залилан)-ийн хохирогчдоос ойролцоогоор 400,000,000.00 вон (301,170.00 евро)-ыг хулгайлсан бөгөөд тус хөрөнгийн гарал үүслийг нь нуун далдлах зорилгоор BX-өөр сольсон байна. Энэ талаар мэдээлэхэд нөлөөлсөн хүчин зүйл нь гадаадын нэг BXYY-ийн хэтэвч рүү шилжүүлсэн өндөр дүнтэй олон гүйлгээ юм. Албан ёсны мөнгөн тэмдэгтээр байсан хөрөнгийг хулгайлж гурван өөр төрлийн BX-өөр сольж, дараа нь сэжигтний дотоодын BXYY-д эзэмшдэг BX-ийн хэтэвчинд хийсэн байна. Дараа нь сэжигтэн дотоодын өөр өөр BXYY-д эзэмшиж буй 48 дансаар дамжуулан 55 удаагийн шилжүүлэг хийж, гадаадын улсад байрладаг өөр BX-ийн хэтэвч рүү шилжүүлэх замаар хөрөнгийн эх үүсвэрийг төөрөгдүүлэхийг оролджээ.

Эх сурвалж: БНСУ

Гүйлгээ хийж буй хэлбэртэй холбоотой шинж тэмдгүүд

12. Доор дурдсан гүйлгээний шинж тэмдгүүд нь МУТС зорилгоор BX-ийг зүй бусаар ашиглах үйлдлийг гүйлгээний тогтмол бус, хэвийн бус болон нийтлэг бус хэв маягаас хэрхэн тодорхойлох боломжтойг харуулсан.

Шинэ хэрэглэгчтэй холбоотой гүйлгээ

- BXYY-тэй шинээр харилцаа үүсгэхдээ өндөр дүнтэй хөрөнгийг байршуулах бөгөөд хөрөнгийн дүн нь харицлагчийн мэдээлэлтэй уялдахгүй байх
- BXYY-тэй шинээр харилцаа үүсгэхдээ өндөр дүнтэй хөрөнгийг байршуулж, эхний өдрөө хуримтлалаа тэр чигт нь ашиглах, харилцагч нь нийт дүнгээр юм уу өндөр дүнгээр арилжаа хийж эхлэх болон харилцагч дараа өдөр нь бүх мөнгөө эргүүлэн татах гэх мэт. Ихэнх BX нь орлогын гүйлгээний хязгаартай байдаг тул биржийн бус арилжаагаар[2] дамжуулан өндөр дүнгээр хөрөнгө угааж болдог

[2] Биржийн бус арилжаа гэдэг нь албан ёсны биржид бүртгэлгүй компаниуд болон брокер, дилерээр арилжаалагддаг үнэт цаасыг хэлнэ.

©FATF/OECD 2020

- Шинэ хэрэглэгч ВХ-ийн нийт дүнгээр арилжаа хийхийг оролдох болон ВХ-ийг эргүүлэн татаж, бүх хөрөнгийг тухайн талбараас гаргахаар шилжүүлэхийг оролдох.

Кейс 3. Харилцагчийн мэдээлэлтэй нийцэхгүй орлого

Дараах сэжигтэй шинж тэмдгүүдэд үндэслэн СБ (банк) нь СГТ мэдүүлсэн бөгөөд үүний дараа мөнгө угаахыг мөрдөн шалгах ажиллагааг эхлүүлсэн байна. Үүнд:

- данс эзэмшигчийн хувийн мэдээлэлтэй нийцэхгүй гүйлгээ – нэг залуугийн нээсэн хувийн дансанд, данс нээснээс хойш эхний хоёр хоногт олон хуулийн этгээдээс их хэмжээний арилжааны шинж чанартай орлого орж ирсэн;
- гүйлгээний хэлбэр - байршуулсан хөрөнгийг ВХ худалдан авах (биткойн) худалдан авах зорилгоор хэд хэдэн ВХҮҮ-ийн данс руу тэр даруй (нэг өдрийн дотор) шилжүүлэг хийсэн;
- харилцагчийн профайл - захиалга өгсөн талуудын нэг нь залилангийн хэргийн субьект гэдгээр банканд танигдсан этгээд байсан бөгөөд тус банкнаас интернет банкны үйлчилгээнд ашигладаг IP хаягийн мэдээллийг эрх бүхий байгууллагад гаргаж өгсөн байна.

Мөрдөн шалгах ажиллагааны үр дүнд онлайнаар зарагдсан барааны төлбөрийг хүлээн авахад туслуулах нэрийн дор гэмт хэрэгтнүүд данс эзэмшигчийг мөнгө угаагчаар ашиглаж байсныг тогтоожээ. Шилжүүлсэн хөрөнгө нь барааны төлбөр биш байсан бөгөөд өөр хохирогч аж ахуйн нэгжүүдийнх байжээ. Байршуулсан хөрөнгийг нэн даруй банкны данснаас хэд хэд хувааж Чех улсын хувьцаат компанийн эзэмшдэг өөр данс руу шилжүүлж, дотоодын хэд хэдэн ВХҮҮ-д эзэмшдэг ВХ (Биткойн)-өөр сольсон. Дараа нь эдгээр ВХҮҮ-дийг данснуудыг нэн даруй хассан байна. Банк СГТ мэдүүлэхээс гадна сэжигтэй шилжүүлгийг түр зогсоосноор хөрөнгө хураах боломжтой болсон.

Дотоодын ВХҮҮ нь мөн хүлээн авсан хөрөнгийг асуудалтай болохыг анзаарч, мөрдөн шалгах ажиллагаанд туслах дараах мэдээллийг өгсөн байна. ВХ-ийг худалдаж авсан нөхцөл байдал; гүйлгээ болон бусад ХТМ мэдээлэл, тухайлбал хэтэвчний хаяг, худалдан авалтад хууль бусаар ашигласан баримт бичгийн хуулбар, худалдан авагчийн нэр зэрэг хэрэгтэй мэдээллүүдийг өгсөн. Эдгээр мэдээлэлд үндэслэн эрх бүхий байгууллагууд банкнаас нэмэлт мэдээлэл (жишээ нь, банкны хуулга) авах боломжтой болсон байна.

Эх сурвалж: Чех Улс

Нийт хэрэглэгчдэд хамааралтай гүйлгээ

- Тодорхой бизнесийн болон логик үндэслэлгүй олон ВХ, олон данс ашиглан хийсэн гүйлгээнүүд.
- ВХ-ийн нэг данс руу олон удаа (тухайлбал өдөр бүр, долоо хоног бүр, сар бүр гэх мэт) шилжүүлэг хийх –
    - Шилжүүлгийг нэгээс олон хүмүүс хийх;
    - Шилжүүлгийг нэг болон түүнээс дээш тооны хүмүүс ижил IP хаягаас хийх;
    - Шилжүүлгийг өндөр дүнгээр хийх.

©FATF/OECD 2020

- Ямар нэгэн хоорондоо холбоогүй, олон төрлийн өөр хэтэвчнээс харьцангуй бага дүнгээр (хөрөнгийн хуримтлал) орлогын гүйлгээ хийж, түүний дараа өөр хэтэвч рүү шилжүүлэг хийх эсвэл бүхэлд нь албан ёсны мөнгөн тэмдэгт болгон солих. Ийм хэд хэдэн хуримлуулах гүйлгээг холбогдох хуримтлалын дансанд хийхдээ албан ёсны мөнгөн тэмдэгт бус ВХ-ийг ашиглан хийх магадлалтай.
- Алдагдалтай байсан ч хамаагүй ВХ-ийг албан ёсны мөнгөн тэмдэгтээр солиулах (тухайлбал, ВХ-ийн үнэ нь хэлбэлзэж байгаа, эсвэл дунджаас хавь илүү өндөр шимтгэл төлөх зэргээс үл шалтгаалан солих, ялангуяа гүйлгээнд ямар нэгэн үндэслэл бүхий тайлбар өгч чадахгүй байх)
- Тодорхой үндэслэлгүйгээр өндөр дүнтэй албан ёсны мөнгөн тэмдэгтийг ВХ-д хувиргах, эсвэл нэг төрлийн их хэмжээний ВХ-ийг өөр ВХ-өөр солих.

Кейс 4. Давтан хийсэн шилжүүлэг

Дотоодын СБ (үнэт цаасны компани) нь брокер болон гадаадын иргэний ВХ-ийн дансаас зөвшөөрөлгүй төлбөр хийгдсэн талаар СГТ мэдээлсэн. Гадаадын иргэн нийт 4,800,000.00 ам.долларын шилжүүлэг хийгдсэн болохыг (нэг өдөр 6 минутын зайтай хоёр тусдаа гүйлгээ хийсэн) дараагийн ажлын өдөр нь арилжааны данстай холбоотой гомдлоо брокерт өгч үнэт цаасны компани энэ үйлдлийг мэдээлсэн. Хэтэвч Кайманы арлуудад бүртгэлгүй байсан хэдий ч СГТ-гийн мэдээллийг гадаадын СМА-тай амжилттай мэдээлэл солилцож, гадаад улсад байрлах онлайн платформ дээр сэжигтний дансыг царцаах боломжтой байсан тул хөрөнгийн ихэнхийг хохирогчид амжилттай буцааж өгсөн байна.

Эх сурвалж: Кайманы арал

Нэрний нууцлалтай холбоотой шинж тэмдгүүд

13. Энэхүү багц шинж тэмдгүүд ВХ-ийн үндсэн технологитой холбоотой өвөрмөц шинж чанар, түүний сул талтай холбоотой. Дараах төрөл бүрийн технологийн онцлогууд нь нэрээ нууцлах боломжийг нэмэгдүүлж, ХСБ-ын гэмт хэргийг илрүүлэхэд саад тотгор учруулдаг байна. Эдгээр хүчин зүйлс нь хөрөнгөө нуун далдлах болон хадгалахыг зорьж байгаа гэмт хэрэгтнүүдэд ВХ-ийг ашиглах таатай нөхцөлийг бий болгодог хэдий ч эдгээр шинж тэмдгүүд байна гэдэг нь хууль бус гүйлгээ болохыг шууд харуулахгүй. Жишээлбэл, төхөөрөмж болон цаасан (paper) хэтэвч ашиглах нь ВХ-ийг хулгайд алдахаас хамгаалах хууль ёсны арга байж болно. Дахин хэлэхэд эдгээр шинж тэмдгүүд байгаа эсэхийг харилцагч, харилцааны бусад хүчин зүйлс болон бизнесийн үндэслэл бүхий тайлбарын хамт авч үзэх хэрэгтэй. Үүнд:
    - Нэмэлт гүйлгээний шимтгэлийг үл харгалзан харилцагч нь нэгээс олон төрлийн ВХ-ийг хамруулсан гүйлгээ хийх, тэр дундаа өндөр түвшинд нэрээ нууцлах боломжтой “нэрээ нууцалсан криптовалют (ННК, anonymity-enhanced cryptocurrency) эсвэл хувийн койн (Privacy coin)” зэрэг ВХ-ийг ашиглах.
    - Биткойн шиг олон нийтэд ил тод, блокчэйн талбарт арилжаалдаг ВХ-ийг төвлөрсөн биржид арилжиж, тэр даруй ННК болон хувийн койноор арилжих.

©FATF/OECD 2020

- Харилцагч нь P2P (хэрэглэгч хоорондын дундын зуучлалгүй харилцаа – peer to peer) биржийн цахим хуудаст бүртгэлгүй/тусгай зөвшөөрөлгүй ВХҮҮ хэлбэрээр үйл ажиллагаа эрхлэх, ялангуяа харилцагчийн нэрийн өмнөөс их хэмжээний ВХ-ийг арилждаг бөгөөд бусад биржтэй харьцуулахад өндөр дүнтэй шимтгэл авдаг байх. Эдгээр P2P гүйлгээг хөнгөвчлөх зорилгоор банкны данс ашиглах.
- Тодорхой үндэслэл бүхий тайлбаргүйгээр P2P платформтой холбоотой хэтэвчнээс ВХ-ийн хэвийн бус (хэмжээ болон тооны хувьд) гүйлгээг хийж, биржээс бэлэн мөнгө гаргах.
- Урьд өмнө нь P2P платформ ашиглаж байсан, эсвэл “холих”, эсвэл “хөрвөх” үйлчилгээг үзүүлдэг ВХҮҮ-тэй холбоотой үйл ажиллагаа эрхэлж байсан хэтэвчнээс ВХ шилжүүлэх эсвэл ВХ-ийг уг хэтэвчинд хүлээн авах.
- Ил болсон хэтэвчний хаяг болон “darknet” зах зээлийн хооронд хууль бус хөрөнгийн урсгалыг далдлах боломжийг олгох зорилготой “холих” эсвэл “хөрвөх” үйлчилгээг ашиглан гүйлгээ хийх.
- ВХ-ийн хаяг болон хэтэвчинд сэжигтэй эх сурвалж, холбоосоос шууд болон шууд бусаар хөрөнгө хүлээн авах болон шилжүүлэх. Сэжигтэй эх сурвалжид “darknet” зах, холих/хөрвөх үйлчилгээ, эргэлзээтэй цахим мөрийтэй тоглоомын сайтууд, хууль бус үйл ажиллагаа (жишээ нь рэнсомвэйр), хулгай зэрэг багтана.
- Төвлөрсөн бус/unhosted төхөөрөмж болон цаасан (paper) хэтэвч ашиглан ВХ-ийг хилээр нэвтрүүлэх.
- ВХҮҮ-ийн талбарт нэвтрэн орж буй хэрэглэгчид нь домайн нэрээ бүртгүүлэхдээ proxy ашиглах болон домайн нэр эзэмшигчийг далдлах, өөрчлөх боломжтой домайн нэр бүртгэгч (DNS) ашиглах.
- ВХҮҮ-ийн талбарт хэрэглэгчид нь “darknet”-д холбогдсон IP хаяг ашиглан болон бусад ижил төрлийн нууцлалтай холбоо, шифрлэсэн и-мэйл, VPN зэрэг төрлийн програм ашиглан нэвтрэх. ВХҮҮ-ийн оронд, янз бүрийн нэрээ нууцалсан шифрлэсэн харилцаа холбоо (жишээ нь, форум, чат, утасны аппликэйшн, онлайн тоглоом гэх мэт) ашиглан талуудын хооронд хийгдэх гүйлгээ.
- Олон тооны хоорондоо харилцаа хамааралгүй ВХ-ийн хэтэвчүүдийг нэг IP хаягаас (эсвэл медиа хандалтыг хянах хаягаас – MAC address) удирдах ба энэ нь ондоо хэрэглэгчдийн халхавч хэтэвчийг ашиглан хоорондын хамаарлыг нуун далдалж байж болзошгүй.
- ВХ-ийн хэлбэр нь зохих ёсоор баталгаажаагүй, залилан болон бусад хуурамч схемийг хэрэгжүүлэхэд чиглэсэн хэрэгслүүдтэй холбоотой байж болзошгүй (Понзи схем зэрэг).
- ХТМ үйл ажиллагаа сул болон ийм тогтолцоо байдаггүй ВХҮҮ-ээс хөрөнгө хүлээн авах, шилжүүлэх.
- ВХ-ийн АТМ/Киоск машин ашиглах –
    - Гүйлгээний өндөр шимтгэлтэй ч төлбөр авч мөнгө угаагч этгээдүүд болон луйврын хохирогчид түгээмэл ашиглагддаг
    - Гэмт хэрэг их гардаг өндөр эрсдэлтэй байршилд байгаа АТМ/Киоск ашиглах

©FATF/OECD 2020

Нэг удаагийн АТМ/Киоск машин ашиглах нь дангаараа шинж тэмдэг болж чадахгүй бөгөөд эрсдэлтэй бүсэд байх, бага хэмжээний олон гүйлгээнд ашиглагдах зэрэг бусад хүчин зүйлс нэмэгдвэл шинж тэмдэг болно.

Кейс 5. Даркнет зах Alpha Bay-тэй холбоотой IP хаяг ашигласан

Эрх баригчид 2017 онд хамгийн том Даркнет зах болох AlphaBay-ийг татан буулгасан. Уг захыг олон зуун мянган хүмүүс хоёр жилийн хугацаанд хууль бус эм, хулгайлсан, залилангийн баримт бичиг, нэвтрэх төхөөрөмж, хуурамч бараа, хортой програм, хакерын хэрэгсэл, галт зэвсэг болон химийн хорт бодис арилжаалах зорилгоор ашиглаж байжээ.

Энэ сайт нь үндсэн серверүүдийнхээ байршил, администраторууд, зохицуулагчид, хэрэглэгчдийн хувийн мэдээллийг нуух зорилгоор TOR сүлжээнд далд үйлчилгээ хэлбэрээр ажилладаг байв. AlphaBay борлуулагчид хэд хэдэн төрлийн ВХ ашигладаг байсан бөгөөд 2015 оноос 2017 оны хооронд ойролцоогоор 200,000 хэрэглэгч, 40,000 борлуулагч, 250,000 зүйлсийн 1 тэрбум гаруй ам.долларын ВХ-ийн гүйлгээ хийсэн байна.

2017 оны 7 дугаар сард АНУ-ын засгийн газар, гадаад улсын туслалцаатайгаар AlphaBay захын серверийг битүүмжилж, администраторыг нь баривчилж, Калифорнийн зүүн дүүрэгт битүүмжлэх тогтоолын дагуу тус захын бодит мөнгө болон ВХ-ийг хураан авчээ. Холбооны мөрдөх товчооноос AlphaBay-ээс бусад ВХ-ийн данс руу хийсэн ВХ-ийн гүйлгээг судалж, банкны дансууд болон администраторын хяналтанд байдаг бусад бодит мөнгөн хөрөнгийг тодорхойлсны дараа битүүмжлэх шийдвэрүүд гаргуулсан байна.

Эх сурвалж: Америкийн Нэгдсэн Улс

Кейс 6. Хэликс – BXYY-ийн холих болон хөрвүүлэх үйлчилгээ

Даркнет захын Хеликс BXYY нь гурван жилийн хугацаанд харилцагчиддаа ВХ-ийн эх үүсвэр болон эзэмшигчийг нуух зорилготой холих болон хөрвүүлэх үйлчилгээг үзүүлжээ. Хеликс нь 350,000 гаруй биткойныг шилжүүлсэн гэж таамаглаж байгаа бөгөөд дамжуулах үеийн үнэлгээ 300 сая ам.доллараас давсан байна. Оператор энэ үйлчилгээг даркнет дээрх гүйлгээг хууль сахиулах байгууллагаас нуун дарагдуулах боломжтой арга гэж тусгайлан сурталчилж байсан байна. 2020 оны 2 дугаар сард Хеликсийг ажиллуулж байсан этгээдэд МУ гэмт хэрэг, зөвшөөрөлгүй мөнгөн шилжүүлгийн үйлчилгээ үзүүлсэн зэргээр эрүүгийн хэрэг үүсгэсэн.

Хеликс нь 2017 онд хууль сахиулах байгууллагуудын татан буулгасан AlphaBay даркнет захтай хамтран ажиллаж байжээ.

Эх сурвалж: Америкийн Нэгдсэн Улс

©FATF/OECD 2020

Кейс 7. Төвлөрсөн бус хэтэвч ашиглах

Энэ хэрэг нь гэмт хэрэгтнүүд хар тамхины хууль бус наймаанаас олсон хууль бус хөрөнгийн эх үүсвэрийг нуухын тулд төвлөрсөн бус хэтэвчийг хэрхэн ашиглаж байгааг харуулна. Энэ хэргийн хувьд гэмт хэрэгтнүүд интернетээр их хэмжээний хар тамхины худалдаа хийж, төлбөрийг зөвхөн фиат валютаар (албан ёсны валют) бус ВХ (биткойн, EX-codes, EXMO-чек) хэлбэрээр авахыг зорьсон байна. Фиат валютаар хүлээн авсан хууль бус хөрөнгийг онлайн блокчейн худалдааны платформ дээр нэрээ нууцалсан дансны тусламжтайгаар ВХ болгон хөрвүүлсэн. ВХ хэлбэрээр ийм хөрөнгийг гэмт хэрэгтнүүдийн хувийн банкны картын данс руу шилжүүлэхээс өмнө арилжаагаар дамжуулан буцаан фиат валют болгон хөрвүүлсэн. ВХ хэлбэрээр хүлээн авсан хууль бус хөрөнгийн хувьд гэмт хэрэгтнүүдийн эзэмшиж байсан төвлөрсөн бус биткойны түрийвч рүү шилжүүлж, дараа нь өөр биржүүд дээр олон биткойн түрийвч рүү шилжүүлсэн. Энэ нь хөрөнгийг мөрдөх, хянахад хүндрэл учруулдаг. Үүнтэй адил угаасан мөнгийг (ВХ-өөрх) гэмт хэрэгтний банкны картын дансанд оруулахаас өмнө буцаан фиат валют болгон хөрвүүлсэн. Гэмт хэрэгтнийг буруутган шүүхннс 7 жилийн хорих ял оноож, торгууль ногдуулсан.

Эх сурвалж: Оросын Холбооны Улс

Шилжүүлэгч, хүлээн авагчтай холбоотой шинж тэмдгүүд

14. Доорх шинж тэмдгүүд нь хууль бус гүйлгээний шилжүүлэгч, хүлээн авагчийн ердийн бус шинж чанар, зан үйлтэй холбоотой. Үүнд:

Данс нээхэд ажиглагдсан хэвийн бус зүйлс

- ВХҮҮ-ийн арилжааны хазгаар болон татах боломжтой дүнгийн хязгаарлалтаас зайлсхийх зорилгоор өөр нэрээр тусдаа данс үүсгэх.
- Сэжигтэй гэж өмнө нь илэрсэн, хориг арга хэмжээнд орсон бүс нутгийн болон итгэж болохгүй IP хаягаас шилжүүлсэн гүйлгээ байх.
- Нэг IP хаягаас ВХҮҮ-д данс нээхээр байнга оролдох.
- Борлуулагч болон корпорацийн хэрэглэгчдийн хувьд тэдний интернет домайны бүртгэл нь үүсгэн байгуулагдсан газраас ондоо улс оронд бүртгэгдсэн байх, домайн бүртгэлийн сул тогтолцоотой улс оронд бүртгэлтэй байх.

Харилцагчийн таньж мэдэх явцын хэвийн бус зүйлс

- Бүрэн бус ХТМ мэдээлэл өгөх, харилцагч нь ХТМ баримт бичиг болон хөрөнгийн эх үүсвэрийн талаарх мэдээлэл гаргаж өгөхөөс татгалзах.
- Шилжүүлэгч/хүлээн авагчийн талаарх мэдээлэлгүй байх, гүйлгээ, хөрөнгийн эх үүсвэр нөгөө талын харилцааны талаар буруу мэдээлэл өгөх.
- Харилцагч данс нээхдээ хуурамч болон зассан, янзалсан баримт бичиг, зураг илгээх.

©FATF/OECD 2020

Кейс 8. Харилцагч өөрийн хөрөнгийн эх үүсвэрийн талаар мэдээлэл өгөхөөс татгалзав

Санхүүгийн байгууллагаас нэг компанитай холбоотой СГТ-нг ирүүлсэн ба тус компани нь бүтээгдэхүүн (биопластик)-аар солих боломжтой купоны борлуулалтын орлого ордог данстай байв. Дансанд хувь хүмүүс болон хуулийн этгээдээс орлого ордог бөгөөд зарим нь ВХ-өөр байв. Банкнаас данс эзэмшигчид хөрөнгийн эх үүсвэрийн талаар мэдээлэл өгөхийг хүссэн ч мэдээлэл ирүүлээгүй байна. Эрх бүхий байгууллагуудын шалгалтаар тус компанийн хүлээн авсан мөнгө нь зохион байгуулалттай гэмт хэрэгтэй холбоотой субьект болон төслөөс залилсан хөрөнгөтэй холбоотой болохыг илрүүлжээ.

Эх сурвалж: Итали

Харилцагчийн профайл

- Харилцагч нь өөр данс нээхэд ашигласан баримт бичиг болон дансны мэдээллийг ашиглах (жишээ нь стандарт бус IP хаяг).
- Харилцагчийн хувийн мэдээллээр өгсөн IP хаяг болон гүйлгээ анхлан хийгдсэн IP хаяг хоорондоо зөрөх.
- Харилцагчийн ВХ-ийн хаяг нь олон нийтийн хууль бус форумтай холбогдсон байх.
- Харилцагч нь эрүүгийн гэмт хэрэгтэй холбоотойгоор олон нийтэд танигдсан байх.

Кейс 9. Харилцагчийн профайл нь тогтмол өндөр дүнтэй хийдэг ВХ-ийн арилжаатай нийцээгүй

СМА-нд ВХҮҮ, санхүүгийн байгууллага хоёр ВХ-ийн арилжаанд оролцохоор данс нээлгэсэн этгээдийн өндөр дүнтэй гүйлгээтэй холбоотой СГТ-нг мэдээлсэн. Тодруулбал, данс эзэмшигч нь 180,000 еврогоос дээш үнийн дүнтэй ВХ худалдан авах, худалдах янз бүрийн гүйлгээг хийж байсан нь данс эзэмшигчийн хувийн мэдээлэлтэй (мэргэжил, цалингийн хэмжээ) таарахгүй байв.

Дүн шинжилгээгээр ВХ-ийг дараах үйл ажиллагаанд ашигласан болохыг тогтоосон. Үүнд: (i) даркнет зах зээл дээрх гүйлгээнд ашигласан; (ii) цахим бооцоо тавьсан; (iii) МУТС зохих хяналтгүй болон өмнө нь олон сая долларын гэмт хэрэгт шалгагдаж байсан ВХҮҮ-тэй гүйлгээ хийсэн; (iv) ВХ-ийн P2P гүйлгээг санал болгосон платформ дээрх үйл ажиллагаа; ба (v) "холих буюу mixing". Данс эзэмшигч данснаасаа тогтмол хэмжээний мөнгийг шилжүүлэхийн тулд янз бүрийн арга хэрэгслийг (мөнгөн шилжүүлэг, цахим банк, урьдчилсан төлбөрт карт) ашигласан байна. Дансны эзэмшигчийн хүлээн авсан хөрөнгө нь цахим шилжүүлэг болон банкны шилжүүлгээр ирсэн бөгөөд ВХ (Биткойн)-ийг бэлнээр худалдаж авсан Ази, Европын (Итали зэрэг) өөр өөр улсуудаас ирсэн байв. Тэрээр мөн Африк, Ойрхи Дорнодын этгээдүүдээс урьдчилсан төлбөрт картандаа мөнгө хүлээн авсан бөгөөд тэд Итали болон гадаадад оршин суудаг иргэдээс мөнгө цуглуулсан байжээ. Дараа нь эдгээр мөнгийг хил дамнасан мөнгөн шилжүүлэг, цахим мөрийтэй тоглоом тоглоход зарцуулж мөн Итали дахь АТМ-аас бэлнээр авчээ.

Эх сурвалж: Итали

©FATF/OECD 2020

Төлбөр авч мөнгө угаагч этгээд эсвэл луйврын хохирогчийн профайл

- Шилжүүлэгч нь ВХ-ийн технологи болон онлайн кастодиан хэтэвчний шийдлийн талаар мэдлэггүй байх. Эдрээр хүмүүс нь мэргэжлийн мөнгө угаагч нарт хөлслөгдсөн тодорхой төлбөр авч байгаа этгээд эсвэл хууль бус хөрөнгийн эх үүсвэр гэдгийг мэдэлгүйгээр хууртагдсан луйврын хохирогч байж болно.
- Харилцагчийн нас нь виртуал хөрөнгийн талбарыг ашиглан данс нээж, их хэмжээний гүйлгээ хийдэг хүмүүсийн дундаж наснаас илт настай байх нь ВХ-ийн хууль бус ажиллагаа эрхлэн тодорхой төлбөр авч байгаа этгээд эсвэл ахмад настан санхүүгийн мөлжлөгийн хохирогч болсон байх боломжтой.
- Харилцагч нь ихэвчлэн хар тамхи тээвэрлэх бизнест ороцолдож, хар тамхины наймаачдад ашиглагддаг санхүүгийн бололцоогүй хүн байх.
- Харилцагчийн ВХ-ийн их хэмжээний худалдан авалт нь өмнөх санхүүгийн түүх болон бусад хөрөнгийн хэмжээ зэрэг мэдээлэлтэй уялдахгүй байх. Энэ нь мөнгө угаах үйл ажиллагаа, тодорхой төлбөр авч байгаа этгээд эсвэл хууль бус хөрөнгийн эх үүсвэр гэдгийг мэдэлгүйгээр хууртагдсан луйврын хохирогч байж болно.

Кейс 10. Луйврын хохирогчид гэмт хэрэгт оролцогч болжээ

Энэхүү хөрөнгө оруулалтын луйвраар гадаад улсын иргэд тэтгэврийн өндөр настай хүмүүстэй утсаар ярьж, цахим шуудангаар болон олон нийтийн мэдээллийн хэрэгслээр (сошлмедиа) холбогдож, үнэ нэмэгдэж байгаатай холбоотойгоор биткойн болон бусад ВХ-нд хөрөнгө оруулахыг санал болгожээ. Анхны хөрөнгө оруулалтыг бага хэмжээгээр (ихэнх тохиолдолд 250 еврогоос ихгүй) хийлгүүлж хохирогчдын банкны данс, кредит карт эсвэл бусад төлбөрийн хэрэгслээр гүйлгээ хийлгүүлж мөнгө нь гэмт хэрэгтнүүдийн гарт очжээ. Гэмт хэрэгтнүүд хохирогчдод ВХ-ийг АТМ ашиглан фиат валютыг биткойноор сольж, гэмт хэрэгтнүүдийн заасан хаягт илгээхийг зааварчилжээ.

Хохирогчид технологийн мэдлэг хомс байсан тул ВХ-ийн технологи болон юунд хөрөнгө оруулалт хийж байгаагаа ерөнхийд нь ойлгоогүй байна. Мөн гэмт хэрэгтнүүд хохирогчдыг төхөөрөмж дээрээ зайнаас хандах програм суулгахыг хүссэн бөгөөд ингэснээр гэмт хэрэгтнүүд зөв данс руу мөнгө шилжүүлэхэд тусалж байгаа гэдэгт итгэсэн байна. Энэ нь гэмт этгээдүүд хохирогчдын төхөөрөмжид нэвтэрч, данснаас нь хохирогчдод мэдэгдэхгүйгээр, зөвшөөрөлгүй мөнгө шилжүүлэх боломж олгосон байв. Зарим тохиолдолд гэмт хэрэгтнүүд алдартай одууд эсвэл томоохон бизнесменүүд болон мэдээний хөтлөгчид ВХ-ийн хөрөнгө оруулалтыг сурталчилж байна гэсэн нийтлэл зохиож, улмаар хохирогчдод хөрөнгө оруулалтад итгэх итгэл, хууль ёсны хөрөнгө оруулалтын мэдрэмжийг төрүүлж чаджээ.

Эх сурвалж: Финланд

Бусад ердийн бус зан төлөвтэй холбоотой шинж тэмдгүүд

• Харилцагч нь имэйл хаяг, IP хаяг, санхүүгийн мэдээлэл зэрэг мэдээллээ байнга өөрчилдөг энэ нь мөн харилцагчийн дансыг өөр хүмүүс ашиглаж байгааг харуулдаг.

©FATF/OECD 2020

• Харилцагч өдрийн турш өөр өөр IP хаягаас нэг буюу хэд хэдэн ВХҮҮ руу байнга нэвтрэхийг оролдох.

• ВХ мессежийн талбарт ашиглаж байгаа яриа, хэл нь хууль бус үйл ажиллагааг дэмжих болон хар тамхи, хулгайлагдсан зээлийн картын мэдээлэл гэх мэт хууль бус бараа худалдан авах гүйлгээг илтгэж харуулж болно.

• Харилцагч их хэмжээний ашиг эсвэл алдагдалтай гүйлгээг тодорхой хүмүүстэй дахин дахин хийдэг. Энэ нь дансыг өөр хүмүүс булаан авсан, арилжааны замаар хохирогчийн хөрөнгийг шилжүүлж авах оролдлого болон ВХҮҮ-ийн дэд бүтцээр хөрөнгийн урсгалыг бүдгэрүүлэх МУ схемийг илэрхийлж болно.

Хөрөнгийн эх үүсвэртэй холбоотой шинж тэмдгүүд

15. Улс орнуудаас ирүүлсэн хэргүүдээс харахад ВХ-ийг буруугаар ашиглах нь ихэвчлэн хар тамхи, сэтгэцэд нөлөөт бодисын хууль бус эргэлт, залилан мэхлэх, хулгайлах, дээрэмдэх зэрэг гэмт хэргийн шинжтэй үйлдлүүдтэй холбоотой байдаг (кибер гэмт хэрэг ч багтана). Ийм гэмт хэргийн үйл ажиллагаатай холбоотой хөрөнгө, хөрөнгийн эх үүсвэртэй холбоотой шинж тэмдүүдийг дор дурдлаа. Үүнд:

- Залилан, сүрдүүлгээр мөнгө авах, эсвэл “ransomware” схем, хориг арга хэмжээнд багтсан хаяг, “darknet” зах зээл болон бусад хууль бус цахим хуудастай холбогдсон ВХ-ийн данс, банкны карт ашиглан гүйлгээ хийх.

- ВХ-ийн гүйлгээний эх үүсвэр эсвэл хүлээн авагч нь цахим мөрийтэй тоглоомын үйлчилгээ байх.

- ВХ-ийн хэтэвчнээс их хэмжээний фиат валют татах зорилгоор нэг эсвэл олон тооны дебит, кредит картыг холбох болон ВХ-ийг худалдан авсан хөрөнгийн эх үүсвэр нь кредит картад хийсэн бэлэн мөнгө байх.

- Хэвийн хэмжээнээс их тодорхойгүй хөрөнгө ВХ хаяг болон дансанд хийгээд ВХ-ийг фиат валютад хөрвүүлэх нь хөрөнгийн хулгайн гэмт хэргийн шинжийг агуулж болно.

- Хөрөнгийн эх үүсвэр, эзэмшигчийн талаарх мэдээлэл хангалтгүй, ил тод байдал дутагддаг халхавч компани ашигласан, анхдагч зоосны санал (Initial Coin Offering (ICO))-д хөрөнгөө оруулсан болон кредит/урьдчилсан төлбөрт картад онлайн төлбөрийн орлогын гүйлгээ хийж тэр даруй түүнийг татах нь.

- Харилцагчийн хөрөнгийн эх үүсвэр нь гуравдагч “холих” үйлчилгээ үзүүлэгч эсвэл хэтэвчийг “хөрвүүлэх” үйлчилгээнээс шууд орж ирсэн байх.

- Харилцагчийн хөрөнгийн ихэнх хэсэг нь ВХ-ийн хөрөнгө оруулалт, ICO эсвэл хуурамч ICO зэргээс олсон орлогоос бүрдсэн байх.

©FATF/OECD 2020

- Харилцагчийн хөрөнгийн ихэнх хэсэг нь МУТСТ хяналтын дутагдалтай бусад ВХҮҮ-ийн ВХ-өөс гаралтай байх.

Кейс 11. Халхавч компани ашиглах- Deep Dot Web (DDW)

АНУ-ын хууль сахиулах байгууллагууд шүүхийн шийдвэрийн дагуу 2019 оны 5 дугаар сард DeepDotWeb (DDW) вэбсайтыг зогсоосон. DDW-ийн эзэмшигчид болон операторуудыг DDW вэбсайтаар хувь хүмүүсийг даркнет захад оруулж олон сая долларын орлоготой холбоотой МУ гэмт хэрэгт буруутгагдсан. Линк, холбоосоор дамжуулан DDW-ийн эзэмшигч болон операторууд DDW сайтаас даркнет захад холбогдсон хүмүүст фентанил, героин зэрэг хууль бус бараа бүтээгдэхүүн худалдааны орлогоос шимтгэл гэж орлого хүлээн авсан.

Эдгээр шимтгэлийн орлогыг ВХ-өөр хүлээн авсан тухайлбал, DDW-ийн хяналттай биткойн түрийвч рүү төлдөг байсан байна. Нийт 15 сая гаруй ам.доллартай тэнцэх хууль бус орлогын эх үүсвэрийг хүлээн авсан бөгөөд нуун дарагдуулах зорилгоор эзэмшигчид болон операторууд өөрсдийн DDW биткойн түрийвчнээсээ орлогоо бусад биткойн түрийвч, мөн өөрсдийн хяналтын халхавч компаний банкны данс руу шилжүүлсэн байна. Гэмт хэрэгтнүүд нь эдгээр компанийг хууль бусаар олсон орлогоо шилжүүлэх, DDW-тэй холбоотой бусад үйл ажиллагааг явуулах зорилгоор ашиглажээ. Таван жилийн хугацаанд тус вэбсайт нь тухайн үеийн биткойны ханшаар ойролцоогоор 8 сая ам.долларын үнэ бүхий 8155 биткойныг төлбөрт хүлээн авсан байна. Биткойныг гэмт хэрэгтнүүдийн хяналтад байдаг DDW-ийн биткойн түрийвч 40000 гаруй удаагийн шилжүүлэг хүлээн авч, 2700 гаруй гүйлгээгээр шилжүүлсэн байна. DDW биткойн түрийвчнээс биткойныг шилжүүлэх үед биткойны үнэлгээ ойролцоогоор 15 сая доллартай тэнцэж байв.

Эх сурвалж: Америкийн Нэгдсэн Улс

Кейс 12. Олон тооны ВХ-ийн арилжаа болон ХТМ үйл ажиллагаанд хуурамч баримт бичиг болон урьдчилсан төлбөрт карт ашиглах

Энэ хэргийн холбогдогчдыг ВХ-ийн биржийг хакердаж, 250 сая долларын ВХ хулгайлсан кибер гэмт хэрэгтнүүдтэй холбоотой МУ схем ашигласан гэж үзэж байна. Хоёр холбогдогч ВХ- 91 сая орчим ам.долларын хулгайлагдсан ВХ, мөн өөр цахим хулгайн гэмт хэргийн 9.5 сая ам.доллар угаасан байж болзошгүй.

Хулгайлагдсан ВХ-үүдийг олон зуун автоматжуулсан ВХ-ийн гүйлгээ болон олон ВХ-ийн арилжаагаар дамжуулсан. Мөнгө угаагч нар ВХ-ийн бирж дээрх ХТМ үйл ажиллагаанд зарим тохиолдолд хуурмч зураг, хуурамч баримт бичиг ашигласан. Хууль бус хөрөнгийн 35 сая ам.доллар нь гадаадын банкны данс руу шилжсэн бөгөөд ВХ-өөр сольж болох урьдчилсан төлбөрт карт худалдан авахад зарцуулагдсан. Холбогдогч нар бие даасан болон холбоотой дансаар дамжуулан үйл ажиллагаа явуулж, ВХ-ийг фиат валют болгон хөрвүүлэх зэрэг ВХ-ийн шилжүүлэх үйлчилгээ төлбөртэй үзүүлжээ. Түүнчлэн холбогдогч нар нь АНУ-д бизнес эрхэлдэг байсан ч Санхүүгийн гэмт хэрэгтэй тэмцэх сүлжээнд (FinCEN) бүртгүүлээгүй байсан байна.

Эх сурвалж: Америкийн Нэгдсэн Улс

©FATF/OECD 2020

Газар зүйн байршилтай холбоотой шинж тэмдгүүд

16. Энэхүү багц шалгуур үзүүлэлтүүд нь гэмт хэрэгтнүүд хууль бус хөрөнгөө шилжүүлэхдээ ФАТФ-ын ВХҮҮ-ийн олон улсын стандартыг[3] хэрэгжүүлсэн байдал улс орнуудад харилцан адилгүй байгаа сул талыг ашигласан болохыг онцлов. Улс орнуудын тайлагнасан кейсүүдэд гэмт хэрэгтнүүд ВХ, ВХҮҮ-ийн МУТСТ дэглэмийн цоорхойг ашиглан хууль бус хөрөнгөө ВХ, ВХҮҮ-ийн МУТСТ эрх зүйн зохицуулалт сул байгаа улс орнуудад бүртгэлтэй болон тухайн улсуудад үйл ажиллагаа явуулж буй ВХҮҮ-д шилжүүлсэн байв. Эдгээр улс орнууд ВХ, ВХҮҮ-ийн бүртгэл/тусгай зөвшөөрлийн зохицуулалт байхгүй, ВХ, ВХҮҮ-тэй холбоотой СГТ мэдээлэх шаардлагад хамрагддаггүй болон ФАТФ-ын стандартад заасан урьдчилан сэргийлэх арга хэмжээг бүрэн нэвтрүүлээгүй байдаг. Энэ гарын авлага нь “өндөр эрсдэлтэй” улс орнуудын жагсаалтыг тодорхойлохгүй боловч мэдээлэх үүрэгтэй этгээдүүд газар зүйн эрсдэлийг тооцоход харгалзан үзэх үзүүлэлтүүдийг танилцуулж байна. Эдгээр эрсдэлүүд нь гүйлгээний шилжүүлэгч, хүлээн авагч, дамжин өнгөрөх улс оронтой холбоотой. Эдгээр эрсдэл нь гүйлгээг шилжүүлэгч тал болон хүлээн авагч хүний өндөр эрсдэлтэй улс оронтой холбоотой байж болох эрсдэлд мөн хамааралтай. Түүнчлэн эдгээр нь харилцагчийн харьяалал, оршин суугаа газар болон бизнесийн үйл ажиллагаа явуулдаг газарт хамаарах боломжтой.

- Харилцагч хөрөнгийг шилжүүлсэн/хүлээн авсан бирж нь тухайн харилцагчийн болон биржийн бүртгэлтэй улс орон биш байх.

- Харилцагч нь зохих ХТМ арга хэмжаа авдаггүй, ВХҮҮ-дэд МУТСТ хангалтгүй хяналттай нь тогтоогдсон өндөр эрсдэлтэй улс оронд байршсан ВХ-ийн бирж болон гадаад улсын мөнгө, үнэ бүхий зүйл шилжүүлэх үйлчилгээ ашиглах.

- Харилцагч нь хөрөнгийг ВХ-ийн тодорхой зохицуулалтгүй болон МУТСТ хяналтгүй улсад үйл ажиллагаа эрхлэгч ВХҮҮ-д шилжүүлэх.

- Харилцагч нь ВХ-ийн зохицуулалтгүй улсад оффисоо байршуулах, шилжих болон ямар нэгэн тодорхой бизнесийн зорилгогүйгээр өөр улсад шинэ оффис байгуулах.

Кейс 13. Биткойны дилер зөвшөөрөлгүй мөнгөн гуйвуулгын үйлчилгээ үзүүлэв (хил дамнасан)

АНУ-д 2019 оны 4 дүгээр сард яллагдагч хэдэн зуун мянган долларын ВХ (биткойн) худалдсан, 1000 гаруй үйлчлүүлэгчдэд зөвшөөрөлгүй мөнгөн гуйвуулгын үйлчилгээ үзүүлсэн гэж хоёр жилийн хорих ял авав. Түүнчлэн яллагдагчаас 823,357 ам.долларыг хураан авах шийдвэр гаргажээ.

Яллагдагч нь ВХ хэрэглэгчдэд зориулсан вэбсайтууд дээр үйлчилгээгээ сурталчилж, зарим харилцагчидтай биечлэн уулзаж, ВХ-ийг бэлэн мөнгөөр солидог байв. Харилцагчид нь АТМ

[3] 2018 оны 7-р сард ФАТФ 12-Month Review of The Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers тайлан хэвлэсэн. Энэ тайлангийн 2-р хэсэгт 2018 оноос хойш улс орнууд олон улсын стандартыг хэрэгжүүлсэн байдал орсон.

©FATF/OECD 2020

болон мөнгө гуйвуулгын үйлчилгээгээр дамжуулан төлбөрөө төлдөг байсан байна. Яллагдагч нь үзүүлсэн үйлчилгээнийхээ төлөө 5%-ийн шимтгэл авдаг байв. Тэрээр анх биткойныг АНУ-ын биржээр дамжуулан авсан боловч түүний үйл ажиллагаа сэжиг төрүүлж, данс нь хаагдсаны дараагаар яллагдагч нь Азид байрлах бирж ашиглаж эхэлсэн байна. Энэ биржийг ашиглан 2015 оны 3 дугаар сараас 2017 оны 4 дүгээр сарын хооронд олон зуун гүйлгээгээр 3,29 сая ам.долларыг биткойноор худалдаж авсан. Түүнчлэн тэрээр АНУ-тай хиллэдэг өөр улсад хадгалагдаж байсан ам.долларaа үнэт металлын дилертэй солилцож, 2016 оны сүүлээс 2018 оны хүртэл бусад хүмүүсийн хамт нийт нэг сая гаруй ам.долларыг АНУ-д импортолсон гэдгээ хүлээн зөвшөөрсөн. Ингэхдээ тайлагнах доод хэмжээ буюу 10,000 ам.долларaас бага хэмжээгээр оруулж ирж байсан байна.

Эх сурвалж: Америкийн Нэгдсэн Улс

BXYY МУТСТ зохицуулалт багатай улс орон руу шилжиж байна.

Ази тивийн А улсад 2017 онд BXYY үзүүлэхийг хориглосон бодлогыг хэрэгжүүлэхийн өмнө тус улсад байгуулагдсан BXYY (бирж) нь үйл ажиллагаагаа тухайн бүс нутгийн Б улс руу шилжүүлсэн. 2018 онд Б улс нь зарим томоохон BXYY-ийг хакердсаны дараа BX-ийн МУТСТ эрх зүйн зохицуулалтаа чангатгажээ. 2018 оны 3 дугаар сард BXYY нь төв оффисоо Европ тив дэх С улс руу нүүлгэх хүсэлтэй байгаагаа зарлав. С улс нь тухайн үед BXYY-ийн хууль, эрх зүйн зохицуулалт нэвтрүүлээгүй байсан. 2018 оны 11 дүгээр сард С улсад BXYY-ийн талаар тодорхой зохицуулалтуудыг нэвтрүүлсэн бөгөөд 2020 оны 2 дугаар сард тухайн BXYY-д үйл ажиллагаа явуулах зөвшөөрөл өгөөгүй байна. Харин тус BXYY нь 2020 оны байдлаар Африк тивийн D улс руу шилжсэн байжээ.

Эх сурвалж: Нээлттэй эх сурвалж

©FATF/OECD 2020

Дүгнэлт

17. Энэхүү тайлан нь ФАТФ-ын гишүүн орнуудад хүргүүлсэн санал асуулгын дүнг нэгтгэсэн бөгөөд төр болон хувийн хэвшлийнхэнд зориулж ВХ-тэй холбоотой гэмт хэрэг, МУ/ТС үйл ажиллагааг илрүүлэх, таних болон урьдчилан сэргийлэх чиглэлийн практик туршлагад үндэслэн гаргав.

18. Энэхүү гарын авлагад тусгасан шинж тэмдгүүд нь ВХ-ийн үүсмэл шинж чанар, сул талтай уялдсан бөгөөд эдгээр нь бүх нөхцөл байдалд, бүрэн гүйцэд гэж үзэх боломжгүй. Шинж тэмдгүүд нь ихэвчлэн МУ/ТС болзошгүй эрсдэлийн ерөнхий дүр зургийг гаргахад хувь нэмэр оруулах нэг л хэсэг гэж үзэх учиртай. Түүнчлэн олон хүчин зүйлийн зөвхөн нэг нь байдаг бөгөөд шинж тэмдгүүдийг (эсвэл аль нэг үзүүлэлтийг) тусад нь авч үзэхгүй байх нь чухал. Эдгээр шинж тэмдгийг холбогдох байгууллагаас авсан мэдээлэл, нөхцөл байдалтай уялдуулах шаардлагатай.

19. Эрсдэлд суурилсан аргачлалыг төр болон хувийн хэвшлийн хоорондын тогтмол бөгөөд идэвхитэй хоёр талт хэлэлцүүлгийн хамт нэвтрүүлснээр энэ тайлангийн үр нөлөөг нэмэгдүүлнэ. Тиймээс эрх бүхий байгууллагууд энэ гарын авлагыг мэдээлэх үүрэгтэй этгээдэд түгээж, энэ талаарх ойлголтыг сайжруулахын тулд тэдэнтэй хамтран ажиллах, таниулах сургалт явуулахыг зөвлөж байна.

20. Тодорхойлсон шинж тэмдгүүд нь байнга хувьсан өөрчлөгдөж байдаг бөгөөд дотоодын хууль сахиулах байгууллага болон олон нийтийн эх сурвалжаас авсан бусад мэдээллийг нөхцөл байдалд уялдуулан ашиглахад илүү тохиромжтой. Эрх бүхий байгууллагууд хувийн хэвшлийг тухайн улс дахь хамгийн өндөр тохиолдох шинж тэмдгийн мэдээллээр хангаж болно. Тухайлбал, энэ гарын авлагын мэдээллийг ашиглан мэдээлэх үүрэгтэй этгээдүүдэд зориулан зөвлөгөө, мэдээллийг гаргаж болно. Гэхдээ тайлангийн шинж тэмдгүүд улс бүр, бүх байгууллагыг хамааралгүй учраас энэхүү тайланг хувийн хэвшлийн байгууллагуудад хяналт тавихад ашиглах хэрэгсэл, хянан шалгах жагсаалт болгон ашиглах зорилгогүй болно

©FATF/OECD 2020

Ашигласан материал

FATF (June 2014), FATF Report Virtual Currencies Key Definitions and Potential AML/CFT Risks

FATF (June 2019), FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers

FATF (June 2020), 12-month Review of Revised FATF Standards – Virtual Assets and VASPs

ФАТФ-ын гишүүдэд зориулсан тайлангууд

FATF (June 2016), Confidential FATF Report on Detecting Terrorist Financing: Relevant Risk Indicators

FATF (June 2019), Confidential FATF Report on Financial Investigations Involving Virtual Assets

www.fatf-gafi.org

2020.09-р сар

Виртуал хөрөнгийн - Мөнгө угаах, терроризмыг санхүүжүүлэхтэй холбоотой байж болох шинж тэмдгүүд

Виртуал хөрөнгө болон холбогдох үйлчилгээнүүд нь санхүүгийн инноваци, бүтээмжийг нэмэгдүүлэхийн хажуугаар тэдгээрийн өвөрмөц онцлог нь мөнгө угаах, терроризмыг санхүүжүүлэх болон бусад суурь гэмт хэрэг үйлдэж буй этгээдэд гэмт хэргийн замаар олсон хөрөнгө, орлогоо хувиргах эсвэл хууль бус үйл ажиллагаагаа санхүүжүүлэх шинэ боломжийг олгож байна.

ФАТФ нь виртуал хөрөнгөтэй холбоотой МУТС шинж тэмдгүүдийн талаарх энэхүү товч тайланг аливаа мэдээлэх үүрэгтэй этгээд, санхүүгийн байгууллага, санхүүгийн бус бизнес, мэргэжлийн үйлчилгээ үзүүлэгчид болон виртуал хөрөнгийн үйлчилгээ үзүүлэгч нарт виртуал хөрөнгөтэй холбоотой мөнгө угаах, терроризмыг санхүүжүүлэх сэжигтэй үйл ажиллагааг таньж илрүүлэх, мэдээлэхэд туслалцаа, дэмжлэг үзүүлэх зорилгоор бэлтгэн гаргасан болно.