Изворни научни рад 343.359:[336.71:004

Др Татјана Лукић, доцент
Правног факултета у Новом Саду

ПРИПЕЈД КАРТИЦЕ – НОВИ ИНСТРУМЕНТ ЗА ПРАЊЕ НОВЦА

Сажетак: *Прање новца је „срце“ скоро свих криминалних активности. То је процес којим се приход стечен криминалним активностима „пере“ и на тај начин се сакрива право порекло тог прихода, а на тај начин се прикрива и сама криминална активност. Иако је ову активност немогуће мерити као закониту економску активност, сматра се да је ова активност попримила изузетно велике сразмере. Међународни монетарни фонд (ММФ) је проценио да количина „опраног“ новца у свакој земљи износи између 2–5% бруто националног дохотка.*

Повећана интеграција међународних финансијских система, заједно са слободним кретањем капитала преко ослобађања од баријера је у многоме олакшала прање новца преносом истог из једне јурисдикције у другу онемогућавајући или знатно отежавајући улажење надлежних органа у трагу путевима прања новца. У овом раду аутор је посебну пажњу посветио припеј картицама као новом инструменту за прање новца, предностима и недостацима електронског банкарства, као и законским и привредним мерама које су усмерене у правцу превенције прања новца припеј картицама.

Кључне речи*: прање новца, припеј картице, платни систем, електронско банкарство*

Уводна разматрања

Прање новца је кривично дело које чине све организоване криминалне групе како би озакониле нелегално стечена средства и глобално, представља све већи изазов, посебно у погледу финансирања тероризма. У

европским земљама све више истрага организованог криминалитета везано је за дроге, па се и највећи број кривичних дела прања новца управо открива и доказује у вези са илегалном трговином наркотика. Међутим, подаци о прању новца стеченог другим врстама криминалитета, као што су трговина људима и кријумчарење лица (криминалитет комплементаран прању новца) говоре о све већем значају прања новца. Осим тога, с обзиром на значај привредног криминалитета у Југоисточној Европи, прање новца повезано са наведеним главним подручјима (организованог) привредног криминалитета могло би бити од истог значаја.

У Србији, што се тиче прања новца, већина „опраних" средстава потиче од утаје пореза, затим трговине дрогом и трговине људима и деликата насиља – отмице и изнуде. Сматра се да су обично извршиоци кривичних дела прања новца, без обзира на предикатна кривична дела, припадници организованих криминалних група са пословним искуством, као и искуством из економије. Зарада се углавном инвестира у приватизацију, некретнине и покретну имовину у разним државама, или се пребацује на банковне рачуне у земљи и иностранству. Велики трансфери новца се обављају преко Кипра, Аустрије и Мађарске, као и „off-shore " рачуна.[1]

Организоване криминалне групе се све више ослањају на комерцијалне структуре и, будући да границе између легалних и илегалних структура постају све мање јасне, прање новца константно изазива забринутост због уласка у легалну економију путем добити остварене криминалитетом и начинима плаћања.

Борба против прања новца је једно од најефикаснијих средстава за супротстављање организованом криминалу. Солидност, интегритет и стабилност кредитних и финансијских институција и поверење у финансијки систем у целини могу се озбиљно угрозити напорима криминалаца и њихових сарадника било прикривањем порекла добити стечене криминалном делатношћу, било усмеравањем законито стеченог новца у сврху терористичких активности. Незаконито стечена корист може се поново инвестирати у криминално пословање или легално предузетништво, може се потрошити или сакрити. Да би се спречило да буду одузета, средства стечена криминалитетом се претварају у легална, тако да се не могу разликовати

[1] CARPO регионални пројекат – Развој поузданих активности и функционалних система полицијског деловања, јачање борбе против главних криминалних активности и јачање полицијске сарадње – је пројекат тахничке сарадње који заједнички финансирају Савет Европе и ЕУ – Извештај о стању организованог и привредног криминалитета на подручју Југоисточне Европе, Стразбур, март 2006. (за реализацију пројекта задужен је Савет Европе у партнерству са Белгијом, Мађарском, Финском, Италијом, Словенијом, Шпанијом, Шведском и Међународном организацијом за миграције (IOM). www.coe.int/economiccrime

од легитимно зарађеног новца. Прање новца се одвија на много начина, а у најновије време све се више користе, односно злоупотребљавају електронско банкарство и електронски начин плаћања.

Електронско банкарство[2]

Електронско банкарство подразумева коришћење банкарских услуга електронским путем. То је систем који омогућава креирање и слање налога за плаћање и трансфер новца потписаних електронским потписом. Постоје две врсте електронског банкарства: *Интернет решење* и *софтверска инсталација код комитента*.

Систем електронског *On-Line* банкарства омогућава сталне информације о рачунима (промет, стања и изводе по свим рачунима, обавештење о приливу и преглед свих *loro* дознака, преглед свих плаћања и *SWIFT* порука, евиденције о обрачунатој провизији и курсне листе), плаћање (у земљи и иностранству) и пословање из било ког дела света. Плаћање рачуна преко Интернета електронским новцем или тзв. паметним картицама (Smart Cards) је активност коју банке такође омогућавају својим клијентима.

Предности Интернет банкарства у односу на класично банкарство огледају се пре свега у врменској и просторној неограничености, брзини обављања трансакција и нижој цени банкарских услуга.

Недостаци Интернет банкарства највише су изражени у одсуству сигурности при обављању послова, непостојању законске регулативе и опасности од злоупотребе Интернет банкарства у криминалне сврхе. Банке које користе електронску размену података у затвореним мрежама (*intranet*), осигуравају се утврђивањем идентитета и ауторизацијом људи који приступају мрежи. У отвореним мрежама, постојећи механизми техничке и правне заштите нису довољни да спрече неауторизован приступ и хакерске упаде. Одређеним криптографским технологијама (укључујући и дигитални потпис) дефинише се нова инфраструктура чија је основна предност виши ниво интегритета поруке и верификације приступа. Шифрирањем поруке обезбеђује се да је порука учесника у трансакцији осигурана и да је друга страна ауторизована за приступ.

Глобални систем комуницирања, какав је Интернет, захтева ажурне и адекватне правне регулативе које треба да дефинишу законске могућности пословања корисника услуга. Законска регулатива у вези Интернета и пословања на њему, разликује се од једне до друге државе. Два најразвијенија дела света, САД и ЕУ, имају различите ставове по питању законске регулативе о Интернету. Постоје два начина за решење овог пи-

[2] Више видети: http://pueblo.gsa.gov-FCIC ; http://www.ifg-inc.com ; http://www.charity-commission.gov.uk

тања. ***Први***, за који се залаже ЕУ, либералног је типа и заснива се на потпуној анонимности и приватности пословања. Овај систем је могућ захваљујући систему енкрипције података, уз помоћ које је загарантована анонимност у слању свих порука на Интернету. На овај начин, систем штити приватност правног и физичког лица у пословању, што је и основно правило банкарског пословања и предност овог система. Мане овог система изражене су у избегавању плаћања пореских и царинских обавеза, олакшаном „прању“ новца и пребацивању капитала из једне у другу државу без знања надлежних државних органа. Овакав систем без адекватне и ажурне законске регулативе могао би да уздрма и нанесе велику штету не само појединим земљама, већ и читавом банкарском систему. Банкарски системи САД и ЕУ били би угрожени због одлива велике количине капитала у тзв. *Off-Shore* банкарске центре. Ово је довело до тога да Интернет банке са подручја САД-а могу пословати само са резидентима САД-а, унутар банкарског система САД и искључиво у америчким доларима. ***Други***, за који се залаже САД, заснован је на комплетној контроли и евиденцији пословања, трансакција и података од стране државних органа. Овај систем би омогућавао државним органима комплетан увид у све банковне рачуне, у све Интернет трансакције и e-mail кореспонденцију. Слобода и приватност појединца као и основна правила пословног и банкарског понашања овим системом би била значајно ограничена.

Оба наведена решења имају своје добре и лоше стране. Нажалост, није могуће њихово просто комбиновање, већ је потребно пронаћи оптималну законску регулативу за пословање на Интернету. До тада, недостатак законске регулативе са једне стране онемогућава одређене сегменте пословања, док са друге омогућава примену широког спектра незаконитих активности у пословању правних и физичких лица, нарочито у свери „прања новца.“

Електронски и жичани трансфери:

Електронски или жичани трансфери подразумевају било коју трансакцију која се изврши у име физичког или правног лица преко финансијске институције на електронски начин уз могућност да се део новца омогући бенефиционој особи у другој финансијској институцији. Прво лице (физичко или правнмо) је власник рачуна, или када нема рачун – лице које поставља налог са финансијском институцијом ради завршетка електронског или жичаног трансфера. Бенефиционе финансијске институције морају имати процедуре идентификовања и испитивања жичаних трансфера који нису у потпуности комплетирани са информацијама о „полазнику“. Процедура адресирања таквих случајева подразумева да банка прво треба

да затражи информације о полазнику које недостају од финансијске институције која је послала жичани трансфер. Уколико информација која недостаје не долази, захтевајућа финансијска институција треба да размотри да ли у свим случајевима недостатак комплетне информације креира или иде у прилог сумњивости трансфера. Уколко се трансфер сматра сумњивим мора се пријавити надлежним органима, а уз то банка или финансијска институција могу да не прихвате трансфер.

Припејд вредносне картице

Припејд вредносне картице (MasterCard, Visa, AmericanExpres) – производ који је доживео експлозивни раст – представља идеалан инструмент за прање новца, без икакве бојазни од документовања, идентификације, сумње надлежних органа или одузимања ових средстава плаћања. У многим државама постоје прописи којима се забрањује одузимање ових картица. Због свега наведеног, криминалци веома радо користе ове картице за прање новца који потиче од најразличитијих криминалних активности. Ове картице функционишу као и редовна новчана средства јер уствари, представљају њихову замену. Редовно се обезбеђује анонимност држаоца картице када он улаже средства на рачун или подиже средства са рачуна картицом. Припејд картице су у много чему супериорне у успостављању метода за прање новца, а нарочито за преношење новца, односно кријумчарење великих свота новца. Криминалци највише воле да користе управо ове припејд картице уместо електронског трансфера новца јер, иако су ове операције сличне, коришћење припејд картице пружа додатне погодности. Ове картице су идеална замена за кријумчарење великих свота новца које се транспортују пошиљкама преко разних сервиса (нпр. поштом и сл.) код којих постоји велика вероватноћа да ће такве пошиљке бити откривене од стране надлежних власти.[3]

Припејд картице омогућују трговцима дрогом јединствен и веома једноставан метод прања новца којим се омогућава кријумчарење профита из једне у другу земљу, као и тзв. „инстант“ слање прекограничних пошиљки.

У многим земљама постоји неколико ***система вредносних картица*** као што су: **отворен систем**, **полу-отворен**, **затворен** и **полу-затворен систем**.

Отворен систем вредносних картица функционише као мрежа кредитних картица и може се користити било где где је ова мрежа прихваћена, најчешће укључујући широм света распрострањену ATM (automated

[3] Национална служба за борбу против дроге САД-а је проценила да се коришћењем припејд картица „опере“ између 13,6 – 47,7 билиона долара годишње. Више видети: U.S. Department of Justice / Ntional Drug Intelligence Center.

teller machine) – шалтерски аутомат – електромеханички уређај који омогућава овлашћеним корисницима који употребљавају пластичне картице да подигну готовину са својих рачуна и/или да користе и друге услуге као што је провера стања, трансфер средстава или прихватање депозита. Аутомати могу радити ***on-line*** са приступом дозвољеним подацима у реалном времену или ***off-line***.

Припејд картице су веома сличне некадашњим ***дебит*** картицама (тзв. дуговним картицама) којима се омогућава да се куповина њеног власника директно наплати са његовог рачуна у установи где је уложен новац, а некада може да се комбинује са неком другом функцијом као што је нпр. функција готовинске или чековне картице. Ове картице су сличне дебитним картицама и по томе што имају рељефни потпис власника картице.

Полу-отворен систем картица је веома сличан отвореном систему и његовим функцијама, али разлика је у томе да овим картицама не може подићи кеш новац са аутомата.

Затворен систем картица (тзв. gift cards) омогућава само тачно одређене новчане трансакције у једној затвореној мрежи.

Полу-затворен систем картица функционише преко мреже главних кредитних картица. Затворен и полузатворен систем картица су анонимни. Све припејд картице вуку вредност из средстава који је одредио програм менаџер.

У односу на наведене системе картица, прање новца највише има успеха у отвореном систему картица. Овај отворен систем картица функционише као заштићен, компактан и незамењив точак за физички транспорт новчаних средстава. Ове картице се такође могу користити за електронски пренос новчаних средстава на тај начин што се на једном месту уложе новчана средства на картицу, а на сасвим другој локацији се са картице повуку новчана средства са аутомата. Ове картице се могу и продати на једном од све већег броја места на Интернету, укључујући ту и веб-сајтове намењене искључиво продаји ових картица, као и Интернетове сајтове за аукције где је дозвољена ограничена продаја ових картица. Ово су само неки од начина на које се припејд картице могу искористити за прање новца.

Карактеристике припејд картица које доприносе знатној користи, ефикасности и приступачности методу прања новца:

– Према прописима неких земаља (нпр. САД) ове картице не могу бити предмет одузимања јер не представљају монетарни инструмент, па се због тога и лакше преносе преко границе.

– Отворен систем картица омогућава глобалан АТМ приступ без рачуна у банкама и тиме се омогућава електронски трансфер новца веома сличан оном трансферу који се врши преко регуларних банкарских рачуна.

– До ових картица се долази веома лако, најчешће преко Интернета без обавезе идентификације држаоца картице, најчешће само на основу фотографије и попуњеног обрасца.

– Многи програм менаџери одобравају неограничен дневни лимит који се може подићи са рачуна.

Припејд картице представљају један од најновијих достигнућа у свету потрошача који користе електронске начине плаћања. Прво је настала тзв. gift card као замена за вредносне папире. Најновије иновације припејд картица су задржале исте карактеристике као и раније картице, с тим што је значајно проширено подручје употребе ових картица и оне данас представљају значајну замену за традиционалне начине плаћања, слање прекограничних новчаних пошиљки и сл.

Међутим, припејд платне картице су веома брзо показале бројне слабости у смислу да су се неке од карактеристика ових картица веома брзо показале као погодне за прање новца и немогућност улажења у траг перачима новца.

Многе владе и надлежни државни органи су прање новца идентификовали као значајан проблем. По својој природи, прање новца користи све рањивости система плаћања као своје предности којима се прикрива порекло новца. Традиционални механизми плаћања као што су кеш, чекови и кредитне картице су веома вешто коришћени од стране криминалаца све док нису пооштрени прописи којима се банке и друге финансијске институције обавезују већим стандардима на утврђивање идентитета својих клијената и обавезност пријаве надлежним властима свих сумњивих трансакција, као и порекла новца којим располажу, чиме су злоупотребе ових механизама плаћања знатно ограничене. Осим тога, органи откривања и гоњења су значајно развили начине улажења у траг сумњивим финансијским трансакцијама. Међутим, криминалци су веома досетљиви у погледу злоупотребе свих слабости система плаћања, нарочито онда када они потичу од нових и мање познатих начина плаћања. Припејд картице су пример новог начина плаћања који представља потенцијално атрактивно средство које омогућава трансакције прања новца.

Припејд картица (унапред плаћена картица) је картица на којој је похрањена вредност за коју је ималац платио издаваоцу унапред. Када говоримо о припејд картици неопходно је првенствено дефинисати одређене појмове који стоје у вези са овом врстом картице као што су:

– ***limited-purpose prepaid card*** – унапред плаћена картица за ограничене сврхе, она може бити коришћена за ограничен број тачно одређених намена. Њена употреба је често ограничена на одређен број тачно одређених продајних места на одређеној локацији (нпр. града, удружење, универзитет). У случају унапред плаћениих картица са једном наменом,

издавалац картице и давалац услуге може бити исти (нпр. картице за јавне телефоне).

– ***multipurpose prepaid card*** **–** унапред плаћена картица са вишеструком наменом. Овде постоје најмање три стране: издавалац, власник и акцептант картице.

– ***stored value card*** – је картица са похрањеном вредности, унапред плаћена картица на којој се евиденција средстава може и повећати и смањити. Назива се такође и електронски новчаник (electornic purse).

Припејд картица је релативно ново средство плаћања. Као кредитне или дебитне картице, то су пластичне картице које имају одређену вредност. Док се код кредитних картица „плаћа касније“, а код дебитних „плаћа одмах“, код припејд картица се „плаћа унапред“ јер су на рачуну унапред похрањена средства.[4]

Потрошачима су доступне две врсте припејд картица које се разлукују по томе где и како се оне могу користити. Прва врста картица су тзв. затворен систем припејд картица. За овај систем су карактеристичне малопродајне картице (***retail gift cards) -*** издаје их небанкарска институција да би се користила у одређеним радњама. Имаоцу картице се обично одобрава кредитна линија. Други систем картица је тзв. отворен систем картица. О оба ова система је већ раније у тексту било речи.

За потребе откривања и доказивања прања новца припејд картицама најважније је да се уочи разлика између две наведене врсте ових картица, односно два система. Ево два примера како се тзв. малопродајна картица може користити за прање новца. Оба примера су из праксе. У првом случају, криминалци су куповали велики број ових картица у читавом ланцу продавница (малопродаје) ван САД-а и то обично по највећем курсу америчког долара, а онда су те картице слали својим „ортацима“ у другим државама где су их ови продавали по средњој вредности курса. У другом случају, дилери дрогом су готовински новац који су стицали продајом наркотика куповали ове картице и давали их у компензацију својим добављачима. На ове поменуте начине, картице су коришћене као средство за прање новца.

Међутим, пошто је могућност искоришћавања ових картица у сврхе прања новца ограничена, много више пажње се посвећује отвореном систему припејд картица и много софистицираније начинима прања новца у овом систему.

---

[4] О овоме више видети: Prepaid Card Models:A Study in Diversity, http://www.philadelphiafed.org/pcc/PrepaidCardModels_Palmer_FINAL.pdf < ConFerence Summary „Prepaid Cards:How Do They Function? How Are They Regulated?, http://www.philadelphiafed.org/pcc/confernences/PrepaidCards_062004.pdf

До Јуна месеца 2006. године преко Интернета се могла набавити припејд картица (анонимно, са могућношћу подизања готовог новца на банкоматима, без ограниченог лимита, са максималним дневним износом готовог новца који се могао подићи са овог рачуна у износу од 5 000$, и то за само 35$). На једној веб страници[5] се рекламирала продаја ових картица. За куповину исте није била потребна идентификација купца и анонимност је била загарантована. Због свега овог су банке и други учесници у програмима припејд картица модификовали своје захтеве који се односе на обавезно давање информација за личну идентификацију ради активирања, као и могућности трансакција картицом.

Међутим, иако је идентификација лица у САД-у сада основни услов за добијање и коришћење припејд картице, исте се анонимно могу добити на великом броју тзв. *off-shore локација*. На Интернету се рекламирају бројне компаније преко којих свако физичко лице може набавити припејд картицу без давања личних података, а која се може платити готовином или трансфером одређеног новчаног износа на рачун компаније при чему се најчешће препоручује да се овај трансфер обави преко неких банака које имају висок степен дискреције клијената.

Услови и начин добијања припејд картице преко тзв. off-shore компанија[6]

ВИЗА дебитна картица је једина међународна картица за глобално тржиште. Картицу могу да користе физичка и правна лица. То значи да је картицу могуће регистровати на име предузећа или фирме и када новац треба да „лети" на рачун ове картице, име физичког лица овлашћеног за коришћење картице не мора да се открије. То значи да се картица може одлично користити за off-shore компаније на подручју САД-а, као и за предузећа у европским земљама.

Предности ВИЗА дебитне картице:

- Нема иницијалног износа за добијање картице;
- Нема компликованих захтева јер се пријава врши путем Интернета или факса;
- Није потребна овера потписа приликом пријаве;
- Од докумената је довољна само лична карта;
- Картица се може користити у било којој земљи;
- Картицом се може куповати преко Интернета, факса, писма или путем телефона;

[5] www.evergreen-cards.com *сајт више није активан*

[6] http://www.poslovne-usluge.com

- ВИЗА дебитна картица се може користити на свим АТМ банкоматима који носе ВИЗА или ПЛУС знак;
- ВИЗА дебитна картица има свој јединствени рачун са банком у Панами;
- Рачун ВИЗА дебитне картице је осигуран строгом банкарском тајном, а Панама нема уговор са било којом другом земљом о размени информација;
- Постоји могућност слања новца путем банковног трансфера на картицу (wire transfer);
- Нема провере бонитета клијента;
- Гарантовано је добијање ВИСА дебитне картице;
- Свако може да добије ову ВИЗА дебитну картицу са једноставним захтевом;
- Не плаћају се камате на коришћење картице;
- Новац са рачуна једне картице може се брзо пребацити на рачун друге картице путем Интернета;
- Износ на картици се може допуњавати на много начина.

За добијање Виза картице потребно је само да се попуни пријава са адресом, телефоном и потписом и достави копија пасоша или личне карте. Достављање захтева за Виза дебитну картицу може се извршити путем Интернета или e-mail-a, факса или поште.

Сама чињеница да нема потребе за нотаризацијом потписа и да се документа не проверавају омогућава максималну злоупотребу. Подаци о власнику Виза дебитне картице су строго чувана банкарска тајна. На картици није уписано име клијента ради лакше продаје самих картица, као и ради сигурности и дискретности у пословању са истом. Уколико је банка у држави која нема уговор са другим државама о размени информација о картицама (нпр. Панама), немогуће је ући у траг новцу који на овај начин циркулише. Овакве картице су најчешће лимитиране на износе од 10000$. Међутим, банке и ту излазе у сусрет клијентима, тако да ако уплате веће суме од максималне, остатак суме се ставља на рачун Виза дебитне картице и аутоматски се износ на картици допуњава на максималан по подизању новца. Уз све ове погодности, сами трошкови картице су минимални: око 200$ за отварање и око 15 $ годишње за одржавање рачуна и картице.

Картица се најчешће допуњава на један од следедећих начина:

- путем банковног трансфера на један од рачуна у Европи, обично некој мањој држави са неразвијеним сектором контроле банкарских трансакција;
- директним банковним трансфером на рачун картице у држави у којој је седиште банке која је издала картицу;

- путем e-gold-a,
- путем e-bullion-a,
- путем EMO система;
- поштанском уплатницом;
- путем Western Union ili MoneyGram,
- другом кредитном картицом преко матичне банке и слично.

Банке треба да прихвате ризик својствен издавању припејд картица без посебног припејд програма. Уколико се у самим банкама не врши строга контрола свих операција са припејд картицама, то ће неминовно довести до пораста криминалних активности. Ескалација ризика са припејд програмом иде у правцу анонимног коришћења картица и слабије контроле. Припејд програм са релативно ниским ризиком укључује контролу која ће га учинити мање привлачним перачима новца. Уколико банка увек може да утврди идентитет купца и држаоца картице, као и „спонзора" односно лице које уплаћује одређени новчани износ на рачун картице, постоји веома мали ризик за прање новца, и обрнуто. Такође су веома значајни извори куповине и допуне ових картица. Уколико се вредност картице допуњава трансфером новца из неке банке од стране клијента који је банци познат, тиме се постиже највећи степен сигурности. И супротно, највећи ризик постоји када се вредност картице повећава готовинским новчаним улогом или другом картицом на рачун припејд картице.

Законске мере за спречавање прања новца припејд картицама

Поред већ постојећих законских мера за спречавање прања новца (обавеза банака и других финансијских институција да све сумњиве трансакције пријаве надлежном органу, идентификација извора, обима и тзв. „транзитних тачака" уласка и изласка новца из финансијских институција, као и идентификација лица директно укључених у ове трансакције, прикупљање релевантних финансијских информација, њихово похрањивање у базе података и аналитичка обрада), у великом броју држава је прописана обавеза банака и других финансијских институција да поставе посебне програме против прања новца – AML (Anti-Money Laundering) програме, да их имплементирају, развију и одржавају. Ову обавезу имају и нефинансијске институције укључујући ту и оператере система кредитних и дебитних картица. Такође се препоручује и прихватање и успостављање CIP програма за идентификацију потрошача. Прихватање и имплементација овог програма је посебно значајна за нефинансијске институције које издају, продају или врше откуп припејд картица. У вези са применом овог програма је нејасно да ли се примењује и на банке које издају припејд картицу, али чији рачун није директно везан за сваког држаоца картице.

Друге мере за спречавање прања новца припејд картицама

Поред законских мера, банке и други учесници програма припејд картица су развили различите стратегије и инструменте којима смањују ризик злоупотребе односно коришћења припејд картица у процесу прања новца. Најзначајније мере су ограничавање лимита – новчаног износа који се може уложити на рачун картице. Међутим, препознајући могућност прања новца на тај начин што се повлачењем максималног износа новца са рачуна који је одобрен, на исти може поново уложити максимално дозвољена сума новца, уведена су и додатна правила. Наиме, за нови прилив средстава на рачун неопходно је да држалац картице оператеру (телефонски или on-line аутоматским системом) проследи одређене идентификационе податке.

На нивоу издавања картица и менаџмент програма, компаније су развиле одређене стратегије за мониторинг коришћења картица ради откривања „примерака" – „узорака" за идентификацију високо ризичних ситуација. Позната америчка фирма Epoch Data Inc[7] је конструисала посебну технологију ***„правовремени мониторинг трансакција"*** ради идентификације сумњивих или високоризичних трансакција које указују на могућу активност прања новца. Ова технологија омогућава истраживање куповине, улагање средстава на рачун, повлачење готовог новца са банкомата на свим локацијама, откривајући неправилне „узорке". Суштина овог аутоматског система је у томе што он садржи огроман број – читав сет индиција за разоткривање сумњивих трансакција прања новца.

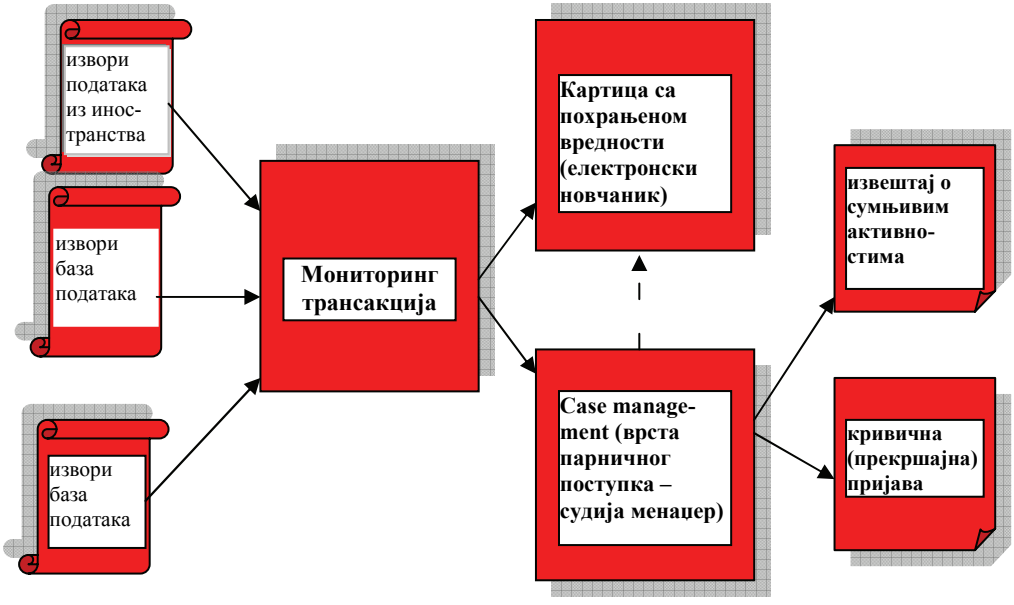
Одређене врсте трансакција треба да „алармирају" финансијску институцију о могућности вршења сумњивих трансакција од стране клијента. То могу бити неекономске, незаконите или некомерцијалне трансакције, као и оне које имају велики проток готовог – кеш новца и нису у складу са нормалним или очекиваним трансакцијама клијента. Веома висок преокрет рачуна који није у складу са сумом која је била нормално на рачуну може представљати индицију да су фондови „опрани". Специфични примери банкарских сумњивих активности могу бити од велике помоћи финансијским институцијама и било би неопходно да буду саставни део тзв. тренинг активности.

Сумњив акт или трансакција је најчешће она која није у складу са познатим клијентовим легалним послом или личним активностима, или нормалним бизнисом за ту врсту финансијског производа. Због тога свака финансијска институција треба да прикупи информације које се односе не само на клијента, него и на посао којим се бави, а да би се олакшало препознавање сумњивих финансијских трансакција.

[7] http://www.epochdata.com

EDI ПЛАТФОРМА

Технологија откривања сумњивих трансакција



Питања која финансијска институција узима у обзир приликом одређивања да ли је одређена трансакција сумњива су:

- да ли је величина трансакције у складу са редовним активностима клијента;
- да ли је трансакција рационална у контексту клијентовог посла или личних активности;
- да ли је промењен образац трансакција које врши клијент;
- да ли клијент има посебан разлог да ради са иностранством (уколико је трансакција по природи међународна).

Главни индикатори могућег прања новца су*[8]*:

- Трансакције чија структура наглашава неку илегалну сврху, комерцијална сврха је нејасна или се чини апсурдном са комерцијалне тачке гледишта.
- Трансакције код којих је разлог клијента за одабиром ове финансијске институције или филијале за реализацију односне трансакције нејасан.

[8] http://www.sourcewatch.org

- Трансакције које нису у складу са финансијским знањем посредника и искуства клијента и наглашеном сврхом бизнис односа.[9]
- Клијенти који дају лажне или непотпуне информације финансијској институцији или одбију због некридибилног разлога да дају информације или документекоји су затражени и рутински обезбеђени у вези са релевантном пословном активношћу.
- Трансакције са земљом или јурисдикцијом које се од стране FATF/a сматрају некооперативном, као и пословни односи са странкама чије место боравка је у овим земљама.
- Извршавање вишеструких трансакција кеша на граници норме за коју је потребна идентификација клијента или извештај о трансакцији.
- Трансфер великих сума или чести трансфер у/из земаља које илегално производе наркотике или су познате по терористичким активностима.
- Трансакције које неочекивано резултирају нулом на билансу клијента.
- Клијент захтева да пословни однос буде затворен и да отвори нови однос на његово име (или име члана породице) без остављања трага на папиру.
- Клијент је осуђен на кривично дело (корупцију или незаконито коришћење јавних фондова).
- Било која предложена трансакција која укључује неку непознату страну.

Специфични индикатори за банке и финансијске институције:

- Трансакције које укључују повлачење средстава брзо након што су била депозирана у банци (пролаз – кроз рачуне).
- Размена великих сума у малим апоенима банкнота (ЕУР или страним) за банкноте у великим апоенима.
- Чести депозити или повлачења великих новчаних свота које се не могу објаснити бизнисом клијената.
- Кеширање чекова великих сума, укључујући путничке чекове ван уобичајеног пословања клијента.
- Инструкције за прекогранични трансфер од стране случајних клијената без ваљаног легитимног разлога.
- Трансфери великих сума новца уз инструкције да се сума исплати бенифиционару у кешу.
- Честе необичне трансакције између клијентовог личног и пословног рачуна.

---

[9] Бизнис однос са банком или финансијском институцијом значи ангажовање у финансијским услугама банке или финансијске институције више него за обичну трансакцију/је.

Специфични индикатори за дилере обвезница:

- Неактивни бизнис односи који одједном доживљавају велике инвестиције које нису у складу са нормалном инвестиционом праксом клијената или њихових финансијских могућности.
- Клијент користи обвезницу или фирму брокера као место где држи фондове који се не користе у трговини обвезница за дужи период времена и таква активност није у складу са уобичајеном праксом клијената или њихових финансијских могућности.
- Велика или необична поравнања обвезница у кешу од стране клијента.
- Трансфер фондова или обвезница између рачуна који нису повезани са клијентом.

Закључна разматрања

Док напори у борби против прања новца остају приоритет за надлежне органе и финансијске институције, са друге стране, криминалци настављају са својим напорима да пронађу пут и начин да искористе, односно злоупотребе финансијске системе плаћања, да преместе и да прикрију незаконито стечен новац. И док су сви начини (средства) плаћања – од плаћања готовим новцем па све до платних картица, предмет незаконитог коришћења, време је показало да су надлежни органи за борбу против прања новца били способни да изграде различите системе и механизме ради превазилажења слабости финансијских система и ограниче или у потпуности онемогуће њихову злоупотребу.

Нови методи плаћања су се ипак показали као посебно погодни за злоупотребу, али док финансијски експерти и други надлежни органи полако улазе у траг новом инструменту прања новца, криминалци су, као и увек корак испред, јер је увек за откривање новог начина прања новца, изналажења бољих законских решења којима би се то онемогућило и њихову имплементацију у позитивноправне прописе, потребно време, које криминалци обилато користе за несметано прање новца.

Данас највећу бригу представљају припејд картице које великим бројем својих карактеристика омогућавају најразличитије начине за прање новца, уколико се над њима не спроводи строга контрола. Висок степен анонимности који је карактеристичан за многе припејд картице, учествовање многих небанкарских и нерегуларних страна у овом процесу, чињеница да се до платних картица лако долази и могућност плаћања у више наврата, чине ове картиве рањивијим, односно погоднијим за потенцијалне злоупотребе више него друге, више „укорењене“ методе плаћања, укључујући овде и традиционалне дебитне и кредитне картице. Ипак,

стручна лица надлежних органа су на време схватили ове ризике коришћења картица и изнашли различите начине обезбеђења које интензивно развијају у намери да ограниче потенцијалне злоупотребе.

Ради онемогућавања коришћења припејд картица мимо њихове основне законске сврхе, бројни стручњаци у САД-у који су први и указали на ову проблематику, а ради превазилажења исте, предлажу да правна лица усвоје и користе програме који се фокусирају на поступак „познавање муштерије“ и којима се ограничава брзина прилива и одлива новчаних средстава са картица, стицање већег броја картица везаних за један рачун и контролу броја подизања готовог новца са банкомата. Такође се предлаже и увођење посебно направљеног мониторинг система који сам истражује такве активности у својој мрежи и открива сумњиве трансакције, скоро на исти начин као и што се користе посебни софтвери посебно намењени за откривање превара у плаћању.

Можемо закључити да не постоји условно речено тзв. „сребрно дугме“ које ће у потпуности зауставити прање новца припејд картицама. Међутим, законска регулатива у комбинацији са одређеним правилима плаћања путем мреже и праксом смањивања пословног ризика, може се значајно допринети редуковању крминалних активности и промоцији једног здравог и снажног тржишта за законит програм припејд картица. Само време може показати да ли се на овај начин може спречити да припејд картице не буду омиљено средство за прање новца стеченог најразличитијим криминалним активностима.

Tatjana Lukić, Ph.D., Assistant professor
Law Faculty, Novi Sad

THE PREPAID CARDS – NEW TOOL FOR MONEY LAUNDERERS

Abstract

Prepaid cards are one of the newer developments in the world of consumer electronic payments. Beginning as an electronic replacement for paper gift certificates (so-called gift cards), now recent innovations to prepaid cards have incorporated the same pre-funding characteristic but are integrated into Master Cards, Visa and other payment card networks. These network-branded prepaid cards programs are now gaining traction as attractive alternatives for traditional paper-based solutions such as cross-border remittances, government assistance programs and many other emerging applicatins.

Over the past few years a lot of government agencies in many countries identifies a number of vulnarabilities particular to prepaid cards and emphasized the threat to the financial systems the use of prepaid cards by money launderers, stating that prepaid cards provide an ideal money laundering instrument to anonymously move monies associated with all types of illicit activity.

In this article the author deals with prepaid cards and how they could be abused, outlines how both the government and the payment sectors have responded to mitigate risks. Also, in this article the author describes how money laundering take place, explores prepaid cards` vulnerability to criminal use and differentiates these criminal acts from more traditional payment card fraud. In this article the author also describes how some government`s and payment industry`s responses to the challenge have helped mitigate risks while still supporting payment innovations.