UDC 336.717:005.334
336.717:004.78

Анали Економског факултета у Суботици, Vol. 50, број 31/2014, стр. 161-175
Датум пријема рада: 26.01.2013.
Датум прихватања рада: 10.12.2013.

Еволуција банкарских ризика од традиционалног до електронског банкарства

The evolution of banking risks from traditional to the electronic banking

Ненад Томић[*]
Економски факултет у Крагујевцу
Лазар Седларевић[**]
Економски факултет у Крагујевцу

Сажетак: Банкарском пословању својствена је пристуност ризика. Ризици имају своју позитивну страну, јер делују као брана превеликој банкарској похлепи за профитима, али и велику негативну страну, јер у случају игнорисања њиховог присуства, или лошег управљања изазивају велике финансијске губитке, како банци која је проузроковала неповољан догађај, тако и њеним клијентима и партнерима. У таквим условима јавља се опасност од ширења ризика на друге учеснике система. Током еволуције банкарског пословања, мењали су се појавни облици и стратегије управљања ризицима. У савременој економији, са једне стране, банкарски процеси су савршенији него икада, али је са друге стране то допринело ширењу нових категорија ризика, који у традиционалним условима нису долазили до изражаја. Еволуција банкарског пословања, стварање нових производа и услуга, нужно је довела до еволуције банкарских ризика, и стварања нових проблема за банке.
Кључне речи: банкарски ризици, електронско банкарство, електронски новац, еволуција ризика.

Abstract: The presence of risks is inherent to the banking industry. Risks can have positive side, when they act as a limit to the greed for high profits, but their negative side is dominant, because they can cause big loses for both banks and their clients and partners in the case of bad risk management or even ignorance of their presence. The danger of spreading the risks among the other participants in the financial system appears in that kind of situation. During the evolution of banking business, there has been significant change in the form of risks, and in the strategies for combating risks. In the modern economy, on one hand, banking processes are more efficient than ever, but on the other hand, it caused the diffusion of the new categories of risks, which were not significant in the traditional economy. The evolution of banking business and the creation of new products and services caused the evolution of banking risks, and creation of new problems for banks.
Keywords: banking risks, electronic banking, electronic money, evolution of risks.

Увод

Банкарски послови стари су већ неколико векова и од самих почетака повезани су различитим категоријама ризика. На путу ка већој профитабилности, банке се суочавају са повећаним обимом ризика, јер је опште правило пословања да без виших ризика не може бити ни виших профита. Неки од облика ризика са којима

[*] ✉ nenadtomic@outlook.com
[**] ✉ lazar_sed@hotmail.com

се банка среће својствени су свим пословним ентитетима, док су други карактеристични управо само за банке као посредничке финансијске установе. Традиционалан облик банкарског пословања, који се развијао од почетака банкарства у средњем веку, па све негде до Велике депресије тридесетих година прошлог века носио је са собом одређене форме банкарских ризика, и облике стратегија које могу бити предузете за борбу против њих. Након Другог светског рата, пословање банака се одвија у измењеном привредном амбијенту. Укрупњавање банкарског капитала, глобализација пословања, и нове технологије, мењају амбијент пословни амбијент, профитне функције банака, и наравно, облике ризика са којима се банка сусреће. У модерном окружењу практично ниједна традиционална категорија ризика није изгубила на значају, али су се зато уздигле нове претње по пословање банака, чинећи тако банкарско пословање још неизвеснијим.

Информационе технологије допринеле су развоју услуга електронског банкарства. Њима су отворене нове могућности за банке, како у традиционалним пословима, тако и у прилици за стварање нових банкарских производа и нуђење нових услуга, поправљању позиције конкурентности и снижању трошкова пословања. Коришћење нових технологија и стварање нових производа и услуга повезало је банке са неким новим категоријама ризика. Неке од њих били су од раније познати банкарској индустрији, али са неупоредиво нижим степеном значаја у традиционалном пословању, него што га имају сада; други облици ризика су нови и својствени само електронском пословању банака. Задатак банкарског менаџмента у идентификовању ризика, њиховој контроли и сузбијању није се променио у односу на традиционални концепт банкарства; данас је међутим, овај посао утолико већи, што банке електронизацијом свог пословања остају изложене притисцима по више основа. Не треба заборавити ни да је глобализација пословања банака резултирала постизањем све већих износа финансијских средстава који банке данас располажу, те је и са те стране присутан већи ризик у банкарском пословању.

У раду је извршен упоредни приказ традиционалних категорија банкарских ризика и њиховог испољавања у условима електронског банкарства, посебно у контексту активности издавања електронског новца, са новим категоријама ризика које су своју стварну претњу показале управо у условима електронског банкарства.

1. Традиционалне категорије ризика

Под традиционалним ризицима подразумевамо оне категорије које су својствене традиционалном комерцијалном банкарству, а које у условима електронског банкарства такође имају велику, али не и доминантну улогу. Суштина класичног комерцијалног банкарство састоји се у депозирно-кредитном процесу, тј. примању депозита и одобравању кредита. Ова класична кредитно-депозитна активност је инхерентно ризичан посао. Практично сви ови ризици су својствени банкарској активности уопште, а њихова интензивност у случају електронског

банкарства, и издавања електронског новца, може бити најчешће нижа у поређењу са класичним банкарством. У ту категорију можемо убројати ризик ликвидности, кредитни ризик, тржишне ризике који се огледају у променама каматне стопе и девизног курса, и неке од посебних категорија које су свој значај стекле у периоду након Другог светског рата, као што су ризик специфичне државе и стратешки ризик.

Након традиционалних ризика биће речи о категорији савремених ризика, која је до изражаја дошла управо у условима електронског банкарства, а нарочито у пословима везаним за издавање електронског новца. Такви су оперативни ризик, са наглашеним значајем технолошке компоненте, ризик репутације и правни (законски) ризик; ове категорије ризика чине нарочиту опасност и постављају нове изазове за успешан менаџмент ризицима.

Пошто се посао издавања кредита заснива принципу фракционих резерви, банке обично имају много више обавеза у депозитима, него што имају готовог новца. Уколико дође до изненадног таласа повлачења депозита банка може доћи у проблем са ликвидним средствима, те у недостатку истих зависити од скупог позајмљивања средстава. Скупо позајмљивање може озбиљно умањити профит банака, али то не мора да буде највећи проблем. Уколико се у јавности створи перцепција о проблему неке од банака са ликвидним средствима, међу депонентима ове банке може завладати паника и потреба да се средства повуку у целости. Такав јуриш на банке познат је у пракси већ вековима, и био је узрок многих банкарских криза. Нека општа превентива за овај облик ризика је такво управљање активом, да она буде спремна да поднесе овакве неочекиване ударе на депозитни потенцијал банке. То значи прерасподелу активе у корист што ликвиднијих финансијских инструмената, тј. тако да банка може без превеликих трансакционих трошкова, и у најкраћем року, да дође до средстава за одговарање на своје обавезе и да избегне скупо позајмљивање или суочавање са несолвентношћу.

Проблем ликвидности својствен је и активностима електронског банкарства, односно у овом случају пословима издавања електронског новца. Ризик ликвидности долази до изражаја у ситуацијама када корисници електронског новца журе са повлачењем сајбер новчаница и њиховом брзом конверзијом у трансакциони новац. Проблем је електронизација читавог процеса, и што корисници нису више у обавези да посете своју банку и усмено затраже повлачење новца, већ се све може учинити у само неколико једноставних команди преко рачунара. Олакшано управљање електронским новцем доводи до могућности брзог и лаког повлачења средстава, на које се никако не може припремити ниједном могућом стратегијом управљања активом. Одговор зато лежи у успоравању и компликовању процеса повлачења електронског новца: клијентима се кроз, рецимо, наплаћивање претплате за коришћење система електронског новца повлачење средстава може учинити скупљим. Guttmann (2003) сматра да се истим ефектом код клијената може развити осећај

припадности једном систему (стр. 157). Такође се може утицати стварањем неких аранжмана повољности за клијенте који систем користе у дужем периоду на формирање навике да се тај систем користи свакодневно, и да се код клијената елеминише потреба за размишљањем о повлачењу из конкретног аранжмана. Таргетирање група потрошача и праћење учесталости коришћења пожељне су активности уколико се размишља о решавању ризика ликвидности на дуге стазе.

Даље, банке се увек суочавају са могућношћу да неки од ентитета који су узели кредит неће бити у могућности да га отплате (Вуксановић, 2009, стр. 10). Губици који настану по том основу отписују се на терет банкарског капитала. С обзиром да база банкарског капитала није велика, банке не могу поднети нарочито велике губитке а да не буду гурнуте у правцу несолвентности. Овај облик ризика, кредитни ризик (дефаулт риск) заслужује посебну пажњу да би се избегло остварење ризичног догађаја. Банке спроводе сложен процес евалуације кредитне способности подносилаца кредитних захтева пре него што им одобре зајам. Проблем је што овај процес није савршен – у тренуцима полета економске активности, банке теже да релаксирају услове кредитне анализе у потрази за већим профитима. Оптимистично очекивање услед наглог раста захтева за кредитима и повољног стања у привреди вуче банке да одговоре на повећану тражњу да би избегли одлазак клијената код конкуренције. Мањак опрезности у оваквим тренуцима веома често у каснијем периоду резултира великим бројем неперформансних зајмова, који могу угрозити стабилност целокупне банке. Зато је неопходно одржавати високи ниво стандарда кредитне анализе у свим фазама привредних циклуса, а одлуке о давању кредита треба буду под сталним надзором интерне ревизије. Кредитни ризик висок значај има и у условима електронског банкарства. Издаваоци електронског новца морају бити нарочито опрезни у случајевима давања кредита, јер је у овом облику банкарства на даљину често немогуће утврдити све неопходне чињенице о зајмотражиоцу. Као тражиоци зајма се често појављују појединци и ентитиети који не би могли добити кредит у уобичајеном поступку, те за њих нема релевантних података који би се могли анализирати.

Следећи значајни облик традиционалних ризика је тржишни ризик, који обухвата две широке категорије тржишних фактора – промене каматних стопа, и промене девизних курсева. Ризик од промене каматних стопа јавља се услед рочне неусклађености активе и пасиве. Ritter, Silber и Udell (2009) наводе да је просечна рочност пасиве знатно дужа него активе, те раст каматних стопа доводи до смањења каматне марже банака, јер ће банка раније морати да обнови депозитни потенцијал по вишим каматама, у односу на пласирану активу (стр. 244). Начин да се банка избори са овим проблемом је уграђивање флексибилних каматних стопа у одобрене кредите, које омогућавају да се каматне стопе на одобрене кредите мењају заједно са променом тржишних каматних стопа. Ове каматне стопе најчешће се формирају тако што се на неку референтну каматну стопу дода одређени број процентних поена (у зависности од процене бонитета клијента). Тако процентна премија остаје фиксна, али укупна каматна стопа

прати промене референтне каматне стопе. Прилагођавање се врши у следећем обрачунском периоду у односу на насталу промену (при чему то може бити полугодишње или годишње).

Банке она средства која не пласирају у кредите инвестирају у хартије од вредности, чешће обвезнице него акције. Услед оваквих инвестиција, изложене су ризицима да ће изненадне промене каматних стопа довести до промене вредности хартија од вредности у њиховом власништву. Кретање каматних стопа и цена обвезница је инверзно, па у случају раста тржишних каматних стопа долази до пада цена обвезница. Проблем је што ово доводи до промене вредности активе и обавеза, па се тако вредност активе може смањити у односу на обавезе, изискујући смањење капитала ради уравнотежења активе и пасиве. Крајњи исход може бити да банка дође у ситуацију да се више не уклапа у стандарде о банкарском капиталу, након чега мора да предузме корективне акције докапитализације. Сам тржишни ризик опасан је и по томе пто може бити увод у ризик ликвидности, јер у случају да банка мора да предузима корективне акције, може доћи до панике и јуриша на банку, што може изазвати проблем ликвидности. Постоје начини да се банка осигура од опасности нагле промене каматних стопа, а један од најчешће коришћених је стратегија са дериватима. Куповањем деривата на обвезницу, банка може лимитирати максималан износ губитка у случају промене каматних стопа.

Тржишни ризици не заобилазе ни издаваче електронског новца. Наиме, сва је прилика да ће се хартије од вредности налазити све чешће и на страни активе и на страни пасиве у билансима ових институција. Средства добијена од продаје услуга својих система инвестираће у тржиште новца; са друге стране, и мањак средстава ће се највероватније надоканђивати на овом тржишту. Улога каматне стопе и ризик од њених хировитих промена ће стога бити велики.

Поред кретања каматних стопа, значајни тржишни ризик који може веома негативно утицати на банкарско пословање је валутни ризик, односно ризик од промене девизних курсева у случајевима када банка има значајан ниво активности у страној валути, или са партнерима из иностранства. Валутни ризик имао је растући значај почев од педесетих година прошлог века, захваљујући глобализацији светске привреде, и сталне потребе банака да обављају плаћања у различитим валутама. У историји пословања банака већ су забележени и случајеви пропасти услед неадекватно менаџмента валутним ризиком (случај Hersttat банке 1974. године). Подједнако велики значај имаће валутни ризик и у условима електронског бакарства, пошто је мотив оваквих институција да послују глобално, те да сервисирају клијенте који се служе различитим националним валутама. Изазов за банке у условима електронског новца биће успоставити курсеве размене законских средстава плаћања у инструменте електронског новца, али и касније управљање овим курсевима. Неки пројекти електронског новца, као Beenz.com, омогућавали су размену средстава између различитих аранжмана електронског новца (у сарадњи са Flooz.com), зарађујући

и на разлици куповног и продајног курса свог новца за доларе (Guttmann, 2003, стр. 129).

Глобализација финансијског пословања је трансформисала банке у транснационалне организације, које су своју активу проширile на финансијске секторе многих земаља света. Интернационализација пословања имала је двоструки утицај на менаџмент ризиком: са једне стране помогла је смањењу тржишног ризика услед увећане диверсификације банкарских портфолија, али у исто време, ствара се нови вид ризика, несвојствен пословању банака унутар националних граница. Појединачне земље, или читави региони, могу бити изложени економским, социјалним или политичким потресима, који могу умањити вредност банкарске активе везане за ту земљу, или угрозити пословање у том подручју. Овај облик ризика, ризик земље, се процењује на континуираној основи, јер у себи садржи јаку црту динамичности. У случају електронског новца ризик земље укључује могућности да прекогранични партнер постане неспособан да сервисира своје обавезе према распореду. Институција која управља системом онда мора да нађе начин да се побрине за криснике у тој земљи, док не нађе другу институцију која ће пружати њене услуге локалним корисницима.

Ghosh (2012) наводи ризик оперативног окружења, и дефинише га слично као што други аутори дефинишу ризик земаља: као опасност да банкарска стратегија не буде одговарајући за дати систем пословног окружења, које зависи од законских, економских, политичких и социјалних елемената датог подручја (стр. 10). План пословања врло лако може бити неостварив уколико се у одређеној земљи, или региону, пракса банкарског пословања битно разликује од стандарда на које је банка навикла. Висока инфлација, ограничења у приступу тржишту новца и капитала, високе каматне стопе, и други поремећајни фактори могу допринети томе да банка не може у пракси да се држи предвиђеног плана. Изненадне промене у законским ограничењима могу бити велики потрес за пословање банака. О тој роблематици писао је Gkoutzinis (2010), наводећи као нарочит проблем ситуацију у којој се доносе законска решења која домаће банке већ испуњавају, са жељом законодаваца да на тај начин створе предност домаћих у односу на стране банке (погл. 3).

Неки аутори као Kondabagil (2007) наводе и стратешки ризик, приписујући овом облику опасност од погрешних одлука управног одбора банке, које би могле да банку доведу до губитка, испусте потенцијалну прилику или умање тржишни удео банке (стр. 11). Значај овог облика ризика може заиста бити изузетан, ако се узме у обзир да погрешна процена, недоступност правих података у правом тренутку, и непридавање адекватног значаја неким претњама или могућностима често доводе до погрешних одлука, које могу скупо коштати пословни ентитет. Стога је овај облик ризика присутан и код традиционалног банкарства, али и код електронског банкарства. Погрешна одлука управног одбора у вези планирања активност електронског пословања може довести до великих пропуштених могућности и појаве губитака уместо раста компаније. Спектар одлука које могу довести до губитака је широк, и подразумева одлагање

замене технологије, преурањеност иновације која још није сигурносно тестирана, превелику зависност од оутсорсинга у дизајну активности, лош дизајн апликација лош поступак кадрирања особља, и многе друге. Базелски комитет за супервизију (2003) у документу посвећеном односу према ризицима у контексту електронског банкарства, наводи да је на управном одбору одговорност не само за праве одлуке у кључним тренуцима, већ и за контролу и борбу против свих осталих врста ризика. Управни одбор мора поставити здраве основе за контролу сигурности и ефикасности система, а на њему лежи и директна одговорност за спречавање остваривања оперативних ризика.

2. Категорије банкарских ризика својствене електронском банкарству

Сви ови побројани ризици својствени традиционалном банкарском присутни су и у пословању електронског издавања новца и банкарства на даљину. Нова категорија ризика, својствена само електронском банкарству, или боље рећи, са далеко већим значајем у контексту електронског банкарства него код традиционалног, представља додатне облике ризике за издаваче електронског новца и банкарских услуга на даљину. Један од разлога је што услуге које се у контексту електронског банкарства пружају зависе од напредних технологија, које саме по себи намећу проблем оперативних ризика.

Оперативни ризици јављају се у различитим облицима, а тичу се проблема који могу настати употребом и злоупотребом високотехнолошке основе неопходне за пружање и примање услуга електронског банкарства. Комитет Банке за међународна поравњања за електронски новац (1998) наводи три облика оперативних ризика: ризици који настају услед повреде безбедности, ризици који настају услед дизајна система, и ризици који настају услед злоупотребе корисника (неки други аутори дајући другачију класификацију).

Акутан проблем међу овом групом је неовлашћен приступ систему од стране хакера са криминалним намерама, најчешће са циљем крађе средстава. Неовлашћен приступ најчешће настаје по основу пресретања поверљивих корисничких информација, што резултира крађом дигиталног идентитета корисника. Сајбер-тероризам се може извести и убацивањем вируса у компјутерски систем банке, чиме се уништавају и/или оштећују подаци које поседује издавалац електронског новца, или се онемогућава функционисање инфраструктуре система. Трошкови које оваква активност изазове могу бити веома високи, не само по основу трошкова враћања система у пређашње стање, исправљања технолошких аномалија и повратка изгубљених или оштећених података, већ и по основу трошкова који настају услед немогућности корисника да користе систем у току трајања оштећења, потребе за враћањем изгубљених средстава корисника, или губитака који ће настати услед напуштања система од стране корисника који су сличну непријатност доживели више пута или страхују од њеног понављања. Могући одговор на овакве претње је активно коришћење

софтверске технологије које онемогућава пресретање корисничких информација, или веома отежава извођење оваквих напада. Како Радојевић и Радовановић (2010) наводе, за потребе преноса података преко интернета развијају се различите варијанте стандарда енкрипције за шифровања података, док се системи институција чувају јаким антивирус програмима и тзв. фиревалл механизмима, који онемогућавају улазак нежељених компјутерских фајлова у систем. Механизми заштите се констатно морају надгледати и тестирати на отпорност према новим могућим претњама, да би се стално знала рањивост система.

Поред овога, издавачи сајбер новца морају констатно да надгледају и употребу њихових производа од стране корисника, да би се брзо реаговало у случају детекције аномалија. Примера ради, након формирања циљних група са уобичајеним шаблонима коришћења, свака употреба електронског новца која веома одскаче од шаблона (по рецимо, неуобичајено високом износу, и према партнерима са географског подручја где их до тада није било) морала би да затражи додатну потврду идентитета корисника, односно да је корисник „онај који тврди да јесте“; другу могућност Guttmann (2003) види у спречавању аутоматског одобравања трансацкија преко одређених износа, и чекање на одобрење од стране оператора система (стр.159). Модерни контекст функционисања електронског новца повлачи са собом немогућност постављања стандарда, и потребу да се ризицима стално управља.

Издаваоци електронског новца могу да се суоче и са преваром изведеном од стране неког од њихових корисника, који најпре изврше трансакцију плаћања, а потом негирају да је до трансакције дошло и захтевају обештећење за дати износ. Трошкови који настану ради доказивања ауторизованости спорне трансакције могу бити веома високи, и њихова се редукција може постићи почетним улагањима у механизме ауторизације корисника, као што је употреба ПИН бројева. У овим условима, издаваоци електронског новца се суочавају са опасношћу да неко фалсификује цертификате које издају, чиме може да превари остали кориснике, или са могућношћу да цертификат буде издат неком лицу за које се касније испостави да је ангажовано у криминалним активностима, а за које нису постојали адекватни подаци од стране његове банке у време издавања. Трошкови поништавања и поновног издавања оваквих цертификата могу бити високи.

Оперативни ризици подразумевају и опасности да превару изврше запослени у институцији која издаје електронски новац. Они могу украсти поверљиве податке везане за кориснике, и искористити их у покушају да извуку средства са рачуна клијената. У таквим случајевима, губици клијената морали би да буду надокнађени, а подаци поново сачувани. Губитак се може јавити и по основу тога што несавесни запослени могу на свом рачуну, или у договору на рачуну другог корисника, креирати електронски новац за који није начињена уплата, и чија ће исплата у будућности повући чист губитак компаније. Ако информација да институција која издаје електронски новац има проблема са

запосленима процури у јавност, компанија може имати додатних проблема због лошег публицитета, одлива старих корисника и избегавања од стране нових, могућности тужби и додатних ревизионих корака надлежних органа власти. Да би се избегле овакве непријатности, компаније би требало да своје запослене бирају пажљиво, по могућству уз мишљење или препоруку спољњих институција, да спроводе унутрашњу контролу и деле дужности тако да запослени не дођу у могућност да сами изведу превару и прикрију је, те да податке чувају тако да остану ван домашаја већег дела запослених.

Даље, оперативни ризици у контексту електронског новца могу бити повезани са могућношћу фалсификовања, односно дуплирања, где криминалци покушавају да дуплирају износе електронског новца са циљем да обаве плаћања за роба и услуге. Издавалац електронског новца је у оваквим ситуацијама одговоран за дуплирани новац који није адекватно уплаћен, и поред ових губитака мораће и да исправи аномалије у систему које су створиле могућност дуплирања новца. Издаваоци електронског новца који се баве сервисирањем микроплаћања могу постављати низак лимит за допуну, чиме се фалсификовање чини неатрактивним. Праћење појединачних трансакција и прављење кумулативних извештаја у централној бази података омогућава улазак у траг изворима фалсификованог новца.

Још један узрок оперативних ризика је комплексна структура система издавања електорнског новца, у којој се институција издавалац често одлучује да део услуга повери специјалистима. Тако се ствара вишестрана алијанса у којој пре свега институција издавалац мора да предузме велику бригу око избора поузданих партнера, јер је управо она одговорна у име целе групе према корисницима. Неуспех у пружању услуга неком од корисника није само индивидуални проблем, јер се последице могу брзо пренети и угрозити функционисање читавог система. Своје незадовољство лошим функционисањем могу показати све стране укључене у трансакцију неуспелу због грешке система, а такође и корисници који су раније искусили сличне проблеме, или који су уплашени могућности да у будућности доживе исто. Сем што пажљиво бирају пертнере за алоцирање неких функција, институције издаваоци треба и да пажљиво сачине уговор о преузетим обавезама, те да изврше планирање редоследа и износа акција које треба да буду предузете. Посебно је битно прављење резервних планова, што укључује могућност да се неки пружаоци услуга промене по кратком поступку.

Велики извор оперативне ризичности електронског новца долази услед превелике зависности од компјутерских и информационих технологија. У свету у коме ове технологије еволуирају брзином која ће се увећава, издаваоци електронског новца послују са ризиком да ће користити погрешну или застарелу технологију. Guttmann (2003) прави разлику технолошког ризика у односу на оперативни, наводећи технолошки ризик као ризик инфраструктуре, а оперативни ризик као ризик управљања том инфраструктуром (стр. 160).

Технолошки ризик подразумева опасност да ће се издаваоци електронског новца служити технолошким системима који су застарели и превазиђени, или да им особље неће бити у стању да прати најновије технолошке трендове, што може довести до пада система или лошег функционисања. За борбу против ове врсте ризика неопходно је на примарно место поставити праћење нових трендова у информационим и комуникационим технологијама. Овим проблемима би требало да се бави тим стручњака, који би пратио трендове, тестирао нова програмска и компонентна решења, вршио тестирање сигурности и отпорности система, те брзине опоравка и повраћаја на претходно стање. Овај тим би био одговоран и за застарелост хардвера и софтвера, те требало да иницира адекватну надградњу онда када је неопходна. Подразумева се да једна озбиљна институција себи неће допустити тај луксуз да технолошка застарелост омета функционисање читавог система. Проблем функционисања услед технолошке застарелости открива несумњиво постојање и других проблема у организацији мимо технолошких. Међутим, додатан разлог праћења технолошке еволуције је сигурност и приватност крајњих корисника. Наиме, поред оператора система, нова достигнућа занимају и оне који би потенцијално такав систем угрозили – дакле, криминалце и сајбер-терористе. Зато би са сваким технолошким напретком који омогућава да шири круг корисника дође у посед напредне технологије, требало освежити сопствени дефанзивну базу, како се однос снага не би помакао у корист оних којима је приступ систему неовлашћен. Ново софтверско решење који омогућава обилажење firewall-a, олакшава упад у сигурносне системе, или може да дешифрује комуникацију са клијентима која је скремблована, захтева нове напоре оператора система да поново успоставе стабилан фиревалл или сигурније шифрују комуникацију са клијентима. Праћење трендова стога је неопходно да би се идентификовао извор проблема и усмерила технолошка иновирања.

Све до сада побројане категорије ризика могу да озбиљно угрозе функционисање система електронског новца, угрожавајући му и репутацију. Репутациони ризик озбиљно штети институцији. Пре свега, корисници који су искусили директно неке проблеме у вези са функционисањем система ће највероватније напустити систем. Када проблем буде познат широј јавности, њих могу следити и они корисници који нису директно искусили проблем, али страхују да би се слична ствар могла догодити и њима. Поверење јавности у погледу новца изузетно је важна ствар. Много времена је протекло док се поверење није изградило у данашњи систем папирног новца, са монетарном вредношћу одвојеном од предметне вредности. Изградња поверења у електронски новац ће, како се претпоставља, трајати много краће, али сваки потрес може озбиљно да наруши све до тада створено. Када се ради о новцу, поверење се тешко стиче, а лако губи. Најбољи начин за борбу против губитка репутације је избегавање пропуста, и спречавање губитака и угрожавања корисника. Да би се то извело, неопходан је стални менаџмент ризика, стално тестирање система и симулирање стресних ситуација. Када проблеми настану, неопходно је имати план за решавање кризне ситуације, избегнути стихијско

ширење проблема и спречити настајање панике. Треба перманентно водити рачуна о корисницима система и како спречити њихову изложеност непријатностима и губицима, јер од поверења корисника и зависи стабилност система.

Пример пада система Flooz.com услед губитка поверења корисника у систем најбољи је пример опасности репутационог ризика за електронски новац. Flooz.com је пример такозваног система купонског новца. У почетку је сервис успео да постигне одређене успеху, и заинтересује (махон млађу) популацију за коришћење. Успех није био дугог века, па су убрзо дошли и проблеми. Wearden (2001) наводи да је систем захтевао велика почетна фиксна улагања и велике издатке за одржавање, али није успео да обезбеди довољно брз прилив средстава да би постао профитабилан. Но и поред тога, систем је функционисао, све док није откривено да је група руских хакера преко њега „опрала“ 300 000$ са украдених кредитних картица куповином Flooz-ових купона. Оператори система решили су да блокирају коришћење кредитних картица за плаћање да се не би изложили још тежем губитку и опасности од рефундирања, а то је била кап која је прелила часу. Чак и они корисници који нису оштећени напустили су систем због привременог блокирања плаћања, и опасности од понављања крађа. Систем је престао да функционише у августу 2001. након мање од 3 године рада.

Поред тога што различити проблеми који могу настати у функционисању система електронског новца могу угрозити репутацију система, може доћи и до настанка правних ризика. Ови ризици се огледају у изложености могућим правним тужбама, којима корисници система траже компензацију за штету коју су претрпели услед лошег функционисања или пада система. Међутим, законска проблематика у контексту интернета значи и више од просте опасности од тужби. Виртуелна природа интернета која шири банкарски утицај глобално на све којима је интернет доступан отвара посебну групу правних питања. Ова питања нису решена, не само у контексту издавања електронског новца, него ни у ширем смислу у контексту пословања на интернету. Окружење у коме послују интернет компаније је добрим делом још правно нерасветљен, и у ситуацији у којој правно окружење перманентно еволуира, све што фирме легално раде данас, сутра може бити забрањено. У оним сферама у којима не постоји законско решење, све што законски није забрањено, дозвољено је. Често није најјасније како се нека законска решења, дизајнирана за случајеве традиционалних банака требају имплементирати у окружење које зависи од технологије која се перманентно мења. Као што постоји потреба за праћење промена у технологијама, тако је неопходно бити у току и са еволуцијом законских решења.

Додатан проблем је што интернет пружа глобалну доступност, а већина законских решења и даље долази у националним оквирима, па се посебно пажња мора обратити и на решења по појединим земљама и подручјима. Правни ризици настају услед неусаглашености са законима, правилима, препорученим мерама

или етичким стандардима одређеног националног оквира. Kondabagil (2007) каже да је могућност њиховог настајања већа што су нејасније обавезе, и слабије дефинисана права сваког од учесника у трансакцији (стр. 13). Последице лошег управљања правним ризицима могу бити финансијске казне, тужбе клијената и партнера, опадање репутације, суспензија компаније или у екстремним случајевима одузимање лиценце за рад.

Изазови из сфере правних ризика су нарочито тешки, зато што пословање издаваоца електронског новца има додира са мноштвом контроверзних питања из домена законодавства – од опорезовања електронског пословања, преко дигиталних потписа, приватности и сигурности корисника, до прања новца и других типова електронског криминала, и коначно, самог питања новца. Посебну пажњу треба обратити на приватност корисника, због одговорности коју институције имају према јавности. Како су ове компаније глобалне у смислу доступности корисницима, морају бити добро информисане о законским разликама од земље до земље, и о надлежностима различитих државних органа. У случају наступања кроз вишестране алијансе, издаваоци електронског новца морају такође бити спремни да преузму одговорност услед превара које начине њихови партнери.

Као посебне категорије ризика, Ghosh (2012) наводи ризике од прања новца и offshore банкарства (стр. 12-15). Наше је мишљење да би се и ови ризици могли сматрати варијатном правних ризика. Проблем прања новца веома је изражен у међународним условима, а националне и интернационалне организације које се баве овим проблемом често се боре и против финансирања тероризма као комплементарне активности прању новца. Иако између ове две активности не стоји потпуни знак једнакости, у последње време веома је честа појава да новац стечен криминалним активностима иде у легалне токове, и/или се користи за финансирање терориста. Offshore банкарство је идеално средство за постизање оба ова циља, будући да су принципи offshore финансијских услуга, поред обезбеђивања „пореског раја“ за кориснике, и обезбеђивање потпуне дискреције и тајности, како у погледу власништва над рачунима, тако и у погледу употребе средстава која се на њима налазе. Електронско банкарство је корак даље у том правцу – погодно је за коришћење криминалних група и убацивање новца стеченог криминалом у легалне токове, будући да се код отварања рачуна и издавања електронског новца не врши провера стечених средстава којима се електронски новац купује. Помоћу електронског новца лакше је вршити финансирање терористичких активности даљину, а могуће је и користити фискалне повластице offshore рачуна без икакве потребе да се са овим центрима остварује дубљи контакт.

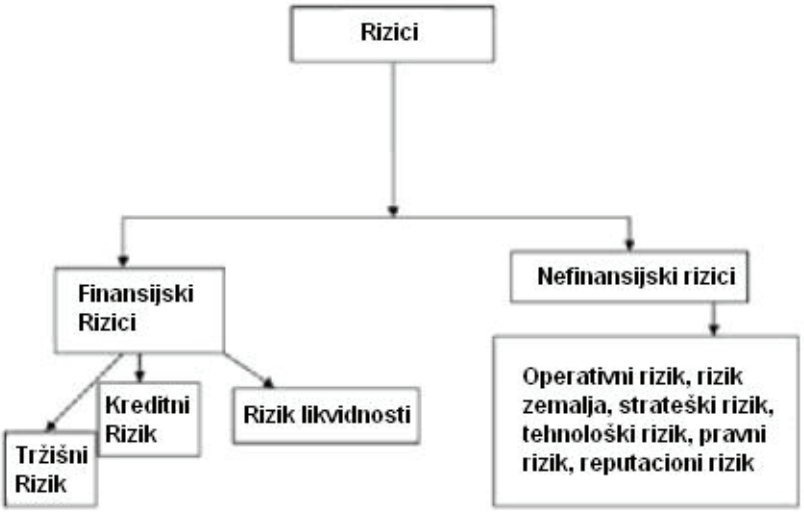
3. Оцена тенденција у еволуцији банкарских ризика

За ентитет способан да креира електронски новац, менаџмент ризицима је активност од суштинског значаја. Балансирање са високим приносима са једне стране и значајним ризицима са друге, биће пре или касније кажњено од стране

јавности. Када дође до грешке у менаџменту ризицима, поверење јавности у неки систем електронског новца постаће виртуелнија од самог електронског новца. Последице губитка поверења јавности најчешће могу бити погубне по функционисање система. Док корисици и инвеститори напуштају компромитовани систем, остају високи фиксни трошкови оваквог начина пословања; и најмање смањење обима трансакција у тим условима може значити велике оперативне трошкове. Како се криза репутације продубљује, а број трансакција смањује, губици нарастају на ниво на коме не могу бити компензовани, те систему прети затварање. И поред овакве опасности, банке и други провајдери услуга електронског новца често не желе да пропусте прилику да уберу високе профите због високих трошкова управљања ризицима.

Може се видети да је током еволуције са традиционалних облика банкарства на електронске форме, дошло до промене, не само категорија ризика, већ и сфере у којима ризици погађају активности банака. За традиционално комерцијално банкарство карактеристични су финансијски ризици, односно ризици који погађају финансијску сферу банкарског пословања (за пример можемо узети тржишни ризик – до кога долази услед промена каматне стопе и девизног курса, дакле финансијских флуктуација). Са друге стране, значај финансијских ризика се релативизује у условима електронског банкарства, када услед специфичности активности електронског банкарства значај добијају неки нови контексти пословања – законска решења или технолошке основе. Важно је имати у виду да се од нефинансијских ризика банка не може заштити на начин на који је могла од финансијских – коришћењем деривата или постављањем лимита.

Слика 1. Класификација финансијских и нефинансијских ризика



Према: Ghosh (2012)

Закључак

Ризици су саставни део банкарске активности. Коришћење нових технологија, које су допринеле стварању нових банкарских производа и услуга, што једним именом називамо електорнским банкарством донело је много предности, како клијентима, тако и самим банкама. Електронско банкарство даје могућност превазилажења канцеларијске ограничености, и омогућује корисницима удаљени приступ и сталну доступност жељених услуга. Ово је довело до диверсификације банкарских услуга и проширења базе корисника, али је са друге стране допринело и ширењу базе ризичних активности банке.

Управљање ризицима у данашњим условима важније је него икад. Сведоци смо да је претерана тежња за профитима, и прелагодно схватање ризика и опасности код неких банкарских (и не само банкарских) институција изазвало највећу кризу у последњих 80 година, која се са финансијског сектора пренела на реални сектор. Ово је време информатичког друштва, у коме иновације информационих и комуникационих технологија постају перманентне, стварајући окружење у коме императив ићи у корак са променама. Такво окружење не дозвољава сталне дефиниције и непроменљиве стратегије за борбу против ризика. Постоји потреба за сталним праћењем ризика, и за процењивање релативног значаја опасности које прете. Нови производи и услуге са собом носе и нове облике ризика; издавање електронског новца минимизирало је значај неких претходних категорија ризика, стављајући у први план ризике против којих тренутно не постоји адекватна стратегија за борбу, осим сталног и свеприсутног мониторинга.

Електронски новац још увек није опште прихваћен, а бројне солуције електронског новца биле су кратког даха. Иако је у тим почетним решењима показана сва слабост концепта електронског новца, нема сумње да нас у будућности чекају нова оперативна решења овог концепта, који показује високи експлоатациони потенцијал. Претходња решења управо служе као пример који демонстрира значај нових категорија ризика, и као модел на чијим грешкама треба учити.

Литература

1. Basel comittee on banking supervision (1998), *Risk management for electronic banking and electronic money activities*, Basel: Bank for international settlement

2. Bank for international settlement (2003) *Risk management principles for electronic banking*, Basel

3. Ghosh, A. (2010). *Managing risks in commercial and retail banking*, Singapore: John Wiley & Sons

4. Gkoutzinis, A. (2010). *Internet banking and the law in Europe* (2nd edition), Cambridge: Cambridge university Press

5. Guttmann, R. (2003). *Cybercash – The coming era of electronic money*, New York: Pallgrave Macmilan

6. Kondabagil, J. (2007). *Risk management in electronic banking*, Singapore: John Wiley & Sons

7. Радојевић, Т., Радовановић, Д. (2010). *Managing risks of electronic banking*, Interntional scientific conference, Gabrovo

8. Ritter, L., Silber, W., Udell, G. (2009). *Principi novca, bankarstva i finansijskih tržišta*, 11th edition, Boston:Pearson Education, prevod na srpski jezik Udruženje banaka Srbije

9. Вуксановић, Е. (2009). *Електронски системи плаћања*, Крагујевац: Економски факултет

10. Wearden, G. (2001). Flooz.com collapse linked to massive credit card fraud, *ZDNET News*, August 28th

Resume

In the context of electronic banking, the importance of banking risks migrated from the financial to the non-financial ones. It does not mean that financial risks become irrelevant in the world of electronic banking; their importance remains high, and they are still dominant category of risks for banking corporations. Regarding only electronic banking activities, some non-financial categories, such as legal regulations, and technological basis of the bank, increase their influence and possible dangers for the banks. New products and services initiated new possible sources of revenue, and new possible obstacles and problems for banks. Problems with inadequate laws, weak operational platforms and bad job done in outsourcing activities, would have significantly larger impact in issuing of electronic money activities, than the classical credit risks. Loss of reputation increases its importance in context of advanced ICT tehnology, where information travel a lot faster than in the traditional banking. The classification of banking risks can hardly be final, as ahe categories of risk are evolving permanently, and the list is never complete.