НАРОДНА БАНКА СРБИЈЕ

СЕКТОР ЗА ПЛАТНИ СИСТЕМ

ФУНКЦИЈА НАДГЛЕДАЊА ПЛАТНОГ СИСТЕМА

друга половина 2016. год.

Садржај:

Увод

Народна банка Србије обавља функцију надзора/надгледања платних система у складу са Законом о Народној банци Србије, Законом о платним услугама и прописима донетим на основу тог закона, руководећи се принципима транспарентности, примене међународно признатих стандарда за функционисање платних система и конзистентности у примени захтева и стандарда на упоредиве платне системе.

Делокруг надзора/надгледања чине првенствено платни системи и активности у оквиру ове функције усмерене су на рад тих система у целини, а не на индивидуалне учеснике у њима.

Са друге стране, у делокругу надгледања су и платни инструменти чијим се коришћењем иницирају платне трансакције које се извршавају у платним системима – ако је употреба тих инструмената уређена посебним правилима договореним између њихових издаваоца. Надгледање инструмената плаћања представља важан део надгледања платних система у којем се извршавају платне трансакције инициране тим инструментима и укључује првенствено разматрање сигурности њихове употребе што је од значаја за одржавање поверења јавности у националну валуту.

Активности Народне банке Србије у обављању функције надзора/надгледања у другој половини 2016. години биле су усмерене су на завршетак провере испуњености прописаних услова за давање дозвола за рад платних система – правном лицу које је управљало радом платног система у складу са одредбама Закона о платном промету и прописа донетих на основу тог закона, као и новим учесницима на тржишту Републике Србије.

1. Учесници на тржишту

У поступцима по захтевима за давање дозволе за рад платних система Народна банка Србије утврђује испуњеност услова прописаних Законом о платним услугама и подзаконским актима донетим на основу тог закона, а који се односе на организационе, кадровске, техничке и друге услове, систем управљања и унутрашњих контрола, као и управљање ризицима у платном систему. Као резултат спроведених поступака, Народна банка Србије је позитивно решила два захтева и крајем 2016. године донела решења о давању дозволе Удружењу банака Србије п.у. за рад платних система – Клиринг чекова УБС и Клиринг директних задужења УБС, а један захтев за давање дозволе за рад платног система је одбијен с обзиром на то да је утврђено да нису испуњени прописани услови.

У Републици Србији на крају 2016. године послују два оператора платних система – Народна банка Србије која управља радом четири платна система (RTGS НБС систем, Клиринг НБС систем, Међубанкарски клиринг систем у девизама НБС и DinaCard клиринг систем) и Удружење банака Србије п.у. које управља радом два платна система (Клиринг чекова УБС и Клиринг директних задужења УБС). Платни системи за које је Удружење банака Србије п.у. добило дозволе за рад у складу са Законом о платним услугама, пословали су и пре почетка примене овог закона у складу са одредбама Закона о платном промету и прописа донетих на основу тог закона.

У табели 1. дат је преглед наведених платних система, врсте налога за пренос који се у тим системима извршавају и начин на који се обавља поравнање по основу тих налога.

RTGS систем Народне банке Србије и Клиринг систем Народне банке Србије утврђени су у складу с прописима као битни платни системи – системи од значаја за стабилност финансијског система, те се на њих, поред захтева прописаних за све платне системе, примењују и одредбе Закона о платним услугама којима се уређује коначност поравнања у битном платном систему, као и додатни захтеви утврђени подзаконским актима. То се нарочито односи на дефинисање тренутка прихватања налога за пренос у систему и тренутка од када учесник и треће лице не могу опозвати тај налог (тренутак неопозивости) – што је од значаја за смањење правног и системског ризика при извршавању трансакција у битном платном систему. Поред тога, један од захтева је и да оператор битног платног система треба да предузме све разумне мере за обезбеђивање наставка кључних пословних процеса у вези с радом битног платног система најкасније два сата после наступања догађаја који онемогућавају редован рад тог система, односно све разумне мере за осигурање завршетка поравнања на основу налога за пренос најкасније до краја дана на који се то поравнање мора обавити.

Табела 1. Преглед платних система у Републици Србији

Назив платног система	Налози за пренос који се извршавају у платном систему	Начин на који се обавља поравнање
RTGS НБС	Налози по основу трансфера одобрења којима учесници иницирају пренос новчаних средстава, у своје име и за свој рачун, као и ради извршавања платних трансакција својих корисника платних услуга; налози за извршавање платних трансакција с циљем спровођења монетарне политике Народне банке Србије; налози за поравнање новчаних обавеза, односно потраживања насталих у другим платним системима и системима за поравнање финансијских инструмената; налози који проистичу из снабдевања банака готовим новцем и преузимања од банака готовог новца, у складу са прописима Народне банке Србије; остали налози у складу с правилима рада система	У реалном времену по бруто принципу
Клиринг НБС	Налози по основу трансфера одобрења којима учесници иницирају пренос новчаних средстава, у своје име и за свој рачун, као и ради извршавања платних трансакција својих корисника платних услуга, у појединачном износу до 300.000,00	У одложеном времену по нето принципу
Међубанкарски клиринг систем у девизама НБС	Налози по основу трансфера одобрења у еврима у Републици Србији, у складу с прописима	У одложеном времену по нето принципу
DinaCard клиринг НБС	Налози који проистичу из платних трансакција обављених употребом DinaCard платних картица	У одложеном времену по нето принципу
Клиринг чекова УБС	Налози који проистичу из платних трансакција обављених чековима	У одложеном времену по нето принципу
Клиринг директних задужења УБС	Налози који проистичу из извршавања платних трансакција директним задужењем УБС, у смислу Закона о платним услугама, у појединачном износу до 300.000,00 динара.	У одложеном времену по нето принципу

Осим RTGS НБС система у којем се налози за пренос извршавају у реалном времену по бруто принципу, у свим осталим системима налози за пренос извршавају се у утврђеном времену по нето принципу тј. обавља се поравнање нето позиција насталих као резултат нетирања по основу налога за пренос у овим системима у смислу Закона о платним услугама, а у складу са правилима рада тих система и RTGS НБС система.

Поред тога што је оператор платних система, Народна банка Србије је истовремено регулатор платних система, има улогу агента за поравнање, а са друге стране обавља функцију надзора/надгледања платних система и издаје и одузима операторима платног система дозволе за рад овог система. Оваква специфична позиција централне банке на тржишту платних система није карактеристична само за Републику Србију. Централне банке свих земаља чланица Европске уније оператори су ТАРГЕТ2 компоненти, а поједине националне централне банке су оператори и система за плаћања мале новчане

вредности (*Retail Payment Systems*)[1]. Функција надзора/надгледања подељена је између Европске централне банке и националних централних банака земаља чланица Европске уније, у зависности од значаја платног система – Европска централна банка има водећу улогу у надзору/надгледању ТАРГЕТ2 компоненти, као и других платних система који су од системског значаја за тржиште Европске уније. Са друге стране, Европска централна банка и националне централне банке су такође, регулатори тржишта платних система.

Све наведене улоге централних банака појавиле су се као одговор на промене до којих је дошло у области платних система – повећања значаја платних система услед све већег броја и вредности трансакција које се у њима извршавају и нових техничко-технолошких решења, али и као резултат немогућности субјеката на тржишту да развију решења која би осигурала несметано функционисање платних система, односно која би одговарала потребама економије. Своју улогу централне банке су препознале и у актуелним дешавањима на глобалном нивоу по питању брзих плаћања тзв. „инстант плаћања“ (*Fast payments, Instant payments*). Већина централних банака сматра имплементацију „инстант плаћања“ стратешким опредељењем у области платних система са циљем модернизације националне инфраструктуре, стварања основе за развој иновативних решења у области инструмената плаћања, унапређења брзине плаћања, обезбеђивања јединственог решења и подстицања финансијске инклузије.[2] Према студији BIS-а[3] ниво подршке и приступ који ће централне банке прихватити у домену развоја инстант плаћања обухвата различите сценарије.[4]

Имајући у виду напред наведено, у домену надзора/надгледања платних система нарочито је од значаја конзистентност у примени захтева и стандарда на упоредиве платне системе.

2. Регулаторни оквир

У претходном извештају разматрани су аспекти регулаторног оквира за платне системе који се односе на послове који се обављају у платном систему, специфичности ризика који се могу појавити у њему и значај правила рада платног система.

[1] нпр. централна банка Италије – Bi-Comp, CABI clearing system, централна банка Литваније – SEPA MMS, централна банка Немачке – RPS, централна банка Грчке – ACO, централна банка Португалије – SICOI.

[2] Fast payments – Enhancing the speed and availability of retail payments, BIS, 2016.

[3] Ибид

[4] Сценарији представљени у BIS студији са примерима су: „Business as usual“ – Италија, Индија, „Moderate support“ – Шведска „24/7 RTGS or special settlement services“ - Аустралија, „Central bank as fast payment system operator“ - Мексико.

Како би се кључни аспекти регулаторног оквира заокружили у суштинском смислу, у овом извештају посебан акценат је стављен на систем управљања и систем унутрашњих контрола. У складу са прописима којима се уређује пословање платних система, оператор је дужан да успостави, одржава и унапређује поуздане, ефикасне и свеобухватне системе управљања и унутрашњих контрола који обезбеђују стабилан, сигуран, ефикасан и делотворан рад платног система и одговорно и поуздано управљање радом тог система. Јасно је да се ови системи првенствено успостављају у сврху управљања ризицима и сматрају се поузданим, ефикасним и свеобухватним ако оператору омогућавају да управља ризицима којима је рад платног система изложен или би могао бити изложен, укључујући и када је оператор поједине оперативне послове у вези с радом платног система поверио другом лицу.

Систем управљања код оператора заснован је на односима између различитих субјеката у чијем је интересу пословање платног система. Имајући у виду да овај систем оператору пружа основ за постављање циљева у вези с радом платног система, утврђивање начина за остваривање тих циљева и праћење њиховог остваривања[5] – систем управљања мора се посматрати у непосредној вези са осталим захтевима прописаним за функционисање платних система.

Законом о платним услугама утврђене су правне форме субјеката који могу бити оператори платног система и с тим у вези, могуће су разлике у начину успостављања система управљања платним системом.

У наведеном систему од значаја је да у организационој структури оператора подела и разграничење послова, као и дужности и одговорности које се односе на рад платног система и управљање ризицима у платном систему буду прецизно и јасно утврђени (документовани), транспарентни и доследни, на начин да се избегне сукоб интереса. То подразумева јасно дефинисање унутрашњим актима оператора поделе дужности и одговорности између органа управљања, руководиоца платног система и других запослених код оператора – у вези с радом платног система и управљањем финансијским, оперативним и осталим ризицима којима је изложен или би могао бити изложен рад овог система. Такође, делокруг свих организационих целина код оператора релевантних за рад платног система и управљање ризицима у овом систему треба да буде јасно дефинисан са јасним линијама одговорности. Поред тога, систем управљања ће оператору омогућити да на одговарајући начин управља ризицима у платном систему и ако је:

- обезбеђена независност функцијама управљања ризицима и интерној ревизији, укључујући и њихова овлашћења и приступ органима управљања;
- делотворна комуникација и сарадња на свим организационим нивоима којима су додељене одређене одговорности у вези с радом платног система и

[5] Principles for financial market infrastructures – CPSS-IOSCO, BIS, 2012.

управљањем ризицима у овом систему и ако је проток информација одговарајући тј. ако је се релевантне информације преносе ефикасно на хоризонталном, а нарочито на вертикалном нивоу;

- обезбеђен јасан и документован процес доношења одлука у вези с радом платног система и управљањем ризицима у овом систему.

Системом унутрашњих контрола оператор води рачуна о спречавању прекомерне изложености ризицима, обезбеђује усклађеност пословних операција са прописима и може спречити, односно отклонити различите неправилности. Као што и сам назив указује, унутрашње контроле се успостављају у унутрашњем пословању оператора и обухватају различите сегменте пословања. За функционисање платног система од нарочитог значаја су контроле које се односе на обезбеђивање усклађености пословања оператора с прописима, али и правилима рада платног система којим управља, као и унутрашњим актима. Такође, од значаја су и контроле које се односе на спровођење процедура и утврђивање неправилности у њиховом спровођењу, обезбеђивање исправности података и информација у извештајима, правовременог и тачног објављивања података о платном систему у складу с прописима, физичке и логичке контроле приступа информационом систему, као и провери адекватности информационог система природи, обиму и сложености послова у платном систему. Поред наведеног, системом унутрашњих контрола оператор треба да заштити и интересе учесника у платном систему којим управља.

Имајући у виду да унутрашње контроле треба да буду део свакодневних активности свих запослених код оператора, њиховим спровођењем они дају важан допринос унапређењу система унутрашњих контрола кроз правовремено уочавање евентуалних недостатака и благовремено информисање на вертикалном нивоу, због чега је важно и контролно окружење и подршка руководства.

Интерна ревизија (унутрашња ревизија) код оператора је од значаја због пружања независне и свеобухватне процене адекватности система управљања платним системом, а нарочито система унутрашњих контрола и управљања ризицима у платном систему.

Поред кључних циљева стабилности и сигурности, рад платног система треба да буде ефикасан и делотворан, нарочито у домену потреба његових учесника, у ком случају оператор треба активно да сарађује са учесницима и потенцијалним учесницима (консултације са учесницима али и евентуално анализирање тржишта, техничко-технолошких решења, трошкова коришћења система и др.). Ако платни систем није ефикасан и делотворан, може нарушити финансијску активност и изложити ризицима своје учеснике, као и њихове клијенте.

3. Преглед дешавања у области надгледања платних система - Банка за међународна поравнања и Европска унија

3.1. Банка за међународна поравнања – Смернице за „сајбер“ отпорност инфраструктуре финансијског тржишта[6]

У настојању да се испуне очекивања корисника финансијских услуга и понуди што шири спектар лако доступних производа и услуга, финансијски сектор испољава све веће захтеве за брзином испоруке производа и извршавањем финансијских трансакција. С тога, инвестирање у нову технологију представља окосницу конкурентске предности која омогућава да се подрже захтеви тржишта. Међутим, упоредо са развојем нове технологије и дигитализацијом финансијских услуга долази и до развоја „сајбер“ криминала и повећања ризика од „сајбер“ претњи и напада (*social engineering, skimming, phishing, identity fraud, hacking, ransomeware*).

Према извештају Организације за економску сарадњу и развој (ОЕЦД) за Г7 групу[7], забележен је значајан раст у броју „сајбер“ инцидената и компанија које су истима погођене. Због тога је на Светском економском форуму 2017, у годишњем Глобалном извештају о ризицима *(„Global Risks Report“, the World Economic Forum 2017*) „сајбер“ ризик идентификован као један од најзначајнијих ризика са којим се суочавају компаније у пет земаља групе Г7. ОЕЦД је препознао да су на глобалном нивоу државе претежно у својим националним оквирима усвојиле стратегије за информациону безбедност које би требале да унапреде свест о управљању ризицима у дигиталном пословању, али не третирајући „сајбер“ безбедност као питање управљања економским и општедруштвеним ризицима.

Пратећи трендове у оба правца (безбедност и финансијске иновације), међународна регулаторна тела су усмерила пажњу ка стварању услова за што сигурнији пословни амбијент, и то за све учеснике у ланцу плаћања, што је и резултирало предузимању низа активности и доношењу конкретних мера и аката којима се уређује област информационе безбедности генерално за платне услуге, а самим тим и за платне системе који подржавају те исте услуге.

Како инфраструктуре финансијског тржишта, међу којима су и платни системи, имају важну улогу у промовисању стабилности финансијског система, Банка за међународна поравнања поравнања (*BIS – Bank for International*

[6] „Guidance on cyber resilience for financial market infrastructures“, Committee on Payments and Market Infrastructures, Bank for International Settlements, June 2016. http://www.bis.org/cpmi/publ/d146.pdf
[7] „Supporting an effective cyber insurance market“, OECD, May 2017

Settlement) је 2016. године објавила Смернице за „сајбер“ отпорност инфраструктура финансијског тржишта (у даљем тексту: Смернице). Наведеним Смерницама „сајбер“ отпорност се дефинише као „способност организације да предвиди, издржи, задржи и брзо опорави одређену инфраструктуру финансијског тржишта од сајбер напада.“ С тога, BIS „сајбер“ отпорност, у смислу оперативне поузданости рада финансијске инфраструктуре, ставља у функцију остваривања циљева финансијске стабилности због чега је веома важно постизање конзистентности у надгледању/надзору инфраструктура и њихових учесника од стране различитих надлежних тела.

Руководећи се основним циљевима усмереним ка достизању што већег степена сигурности и ефикасности финансијске инфраструктуре уз ограничавање системског ризика, BIS је „сајбер“ ризик препознао као кључни ризик у оквиру оперативног ризика са којим се суочавају све финансијске инфраструктуре данас. BIS овај ризик види као јединствени изазов који се намеће традиционалним оквирима за управљање оперативним ризицима у инфраструктури с обзиром на специфичности које га издвајају од других врста оперативних ризика, и које се огледају у следећем:

- „Сајбер“ нападе је тешко предвидети, идентификовати, проценити тачан обим губитка и потпуно их „искоренити“. Често су неприметни и шире се великом брзином унутар мреже система;
- „Сајбер“ напади могу доћи кроз различите „улазне“ тачке инфраструктуре финансијског тржишта због присуства међусобно повезаних различитих субјеката у ланцу извршавања плаћања, повезаних субјеката, пружалаца техничких услуга којима се подржава рад инфраструктуре али „улазна“ тачка могу бити и сами запослени;
- „Сајбер“ напади у значајној мери доприносе неефикасности система управљања ризицима и континуитетом пословања.

Имајући у виду наведене специфичности „сајбер“ ризика, BIS сматра да је неопходно успоставити један свеобухватан оквир за управљање оперативним ризиком који ће укључити и „сајбер“ ризик – дефинисањем јасне стратегије и циљева „сајбер“ отпорности.

Смерницама утврђен оквир за управљање „сајбер“ отпорношћу састоји се од пет кључних фаза (Управљање – Идентификација – Заштита – Откривање – Опоравак) и тим фазама три заједничке компоненте (Тестирање – Безбедносна упозорења – Учење и развој).

- Управљање

Ефикасан систем управљања „сајбер“ ризиком сматра се суштински значајним за реализацију системског и проактивног приступа управљању постојећим и новим претњама са којима се одређена инфраструктура суочава.

Системом управљања треба обухватити све нивое једне организације и обезбедити одговарајуће ресурсе и стручност кадрова који би се бавио овим ризиком. Због тога се под ефикасним управљањем „сајбер“ отпорношћу подразумева дефинисање, пре свега, јасног и свеобухватног оквира који укључује информациону-комуникациону опрему, људе, процесе и захтеве које намећу нове технологије, као и правовремену комуникацију са свим интересним групама како би се обезбедила ефикасна реакција и опоравак од „сајбер“ напада. Поред тога, оквир треба да буде усклађен и са дефинисаном стратегијом постизања „сајбер“ отпорности и циљевима које треба у том смислу остварити.

- Идентификација

Испољавање сваког типа оперативног ризика у инфраструктурама финансијског тржишта потенцијално може да угрози финансијску стабилност, с тога је за ефикасно управљање „сајбер“ отпорношћу веома важна идентификација и класификација свих кључних пословних процеса, информационих добара и екстерних субјеката од чијег пословања зависи одређена инфраструктура финансијског тржишта, а који ће бити приоритет у заштити од злоупотреба.

- Заштита

Системи безбедности, унутрашњих контрола и процеси треба да буду дефинисани на тај начин да штите поверљивост, интегритет и доступност информационог система инфраструктуре финансијског тржишта. Контроле треба да буду сразмерне улози коју одређена инфраструктура има у финансијском систему и претњама којима је изложена, уз адекватно дефинисану толеранцију ризика.

- Откривање

Суштина имплементације оквира за управљање „сајбер“ отпорношћу је способност препознавања раних знакова потенцијалног „сајбер“ напада или што ранијег откривања да је стварно и дошло до повреде система. Рано откривање преварних радњи омогућава проактивно деловање ради спречавања повреде система или ублажавања утицаја напада кроз онемогућавање приступа поверљивим подацима и „извозу“ (*export*) истих. С тога се Смерницама указује на значај успостављања ефикасног система за континуирано праћење неуобичајених радњи и дефинисања потребних активности у случају да дође до инцидента.

- Одговор и опоравак

У овој фази управљања „сајбер“ отпорношћу акценат је на развоју способности адекватног реаговања и предузимање мера опоравка система од „сајбер“ напада. У том смислу, потребно је обезбедити да се кључне функције успоставе брзо, сигурно и са прецизним подацима како би се ублажио потенцијални системски ризик. С тога су добро дефинисани планови одговора на инциденте, планови континуитета и опоравка система од велике важности.

Имајући у виду наведене фазе, Смерницама се указује на значај тестирања сваког од елемената система управљања „сајбер“ отпорношћу пре имплементације унутар инфраструктуре финансијског тржишта, како би се проценила његова укупна ефикасност и како би се иста пратила током редовног рада инфраструктуре. Поуздано и детаљно тестирање доприноси идентификацији недостатака у постављеним циљевима „сајбер“ отпорности и обезбеђује кредибилне и значајне податке неопходне за процес управљања овим ризиком. Са друге стране, анализом података добијених кроз тестирање проактивно се долази до начина на који се уочене слабости и недостаци могу исправити, смањити или у потпуности отклонити. Поред тестирања, од значаја је познавање и редовно праћење ситуације у окружењу у вези с могућим „сајбер“ претњама, као и потенцијалних последица проузрокованих пословањем инфраструктуре у таквом окружењу. За креирање свести о „сајбер“ претњама веома је важно успоставити ефикасан систем информисања који би омогућио правовремену и брзу реакцију како би се „сајбер“ напади предухитрили или што раније открили. С тога је неопходно активно учешће у размени информација и сарадња са свим интересним групама, и то не само у домену пословања финансијске инфраструктуре већ и у ширем кругу субјеката. Исто тако, неопходно је обезбедити и континуирано учење и ангажовање запослених на проналажењу адекватних решења за прилагођавање динамичној природи „сајбер“ ризика, као и развоју способности за правовремену идентификацију, процену и управљање претњама и откривање рањивости система.

Смерницама се такође указује и да организација која управља радом инфраструктуре финансијског тржишта треба да имплементира организациону „сајбер“ културу која нарочито обухвата ширење свести о овом ризику и континуирано унапређивање знања и компетенција запослених у овој области.

3.2. Инстант плаћања

Према Европском одбору за мала плаћања (ERPB – *Euro Retail Payments Board*) – „Инстант плаћања“ представљају решења за електронска плаћања мале новчане вредности која су на располагању корисницима платних услуга по моделу 24/7/365 и која резултирају тренутном или скоро-па-тренутном одобрењу

рачуна примаоца плаћања.[8] Наиме, прелазак пословања у електронску сферу, а нарочито електронска трговина и коришћење дигиталних комуникација условили су да корисници платних услуга очекују да им на располагању буду решења која ће им омогућити брзо обављање плаћања.

Коришћење „паметних" телефона и интеграција продајних канала отворених 365/24/7 од стране трговаца, заједно су створили услове да потрошач може извршавати плаћања у било које време и са било којег места, и то не само на релацији потрошач-пословни субјект (person-to-business) већ и на релацији потрошач-потрошач (person-to-person). Потенцијале тржишта и технолошке иновације треба подржати што је и резултат усвајања SCT Inst шеме у Европској унији.[9] Приликом припреме наведене шеме Европски савет за плаћања имао је у виду пословне захтеве који се, између осталог, односе на: доступност услуге инстант плаћања за кориснике платних услуга, расположивост новчаних средстава за примаоца плаћања, разумевање концепта извршавања инстант плаћања у року од "неколико секунди" од стране свих учесника, успостављање поузданог система идентификације корисника платних услуга како не би долазило до грешака, успостављање стандардизованих финансијских и нефинансијских порука и др. „Инстант плаћања" отварају простор за конкуренцију у домену инструмената којима се могу иницирати безготовинска плаћања и искоришћење потенцијала мобилних плаћања, а све то би требало да допринесе даљем развоју електронске трговине.

С обзиром на то да је крајем новембра 2016. године усвојена SCT Inst шема, Евросистем је у истом периоду спроводио низ активности усмерених на анализу потреба тржишта за услугама поравнања инстант плаћања по моделу 24/7/365.

Посебна Радна група, на чијем челу су представници Европске централне банке припремила је спецификацију корисничких захтева за нове услуге TARGET инстант плаћања. Наведена иницијатива је резултат циља Евросистема да се одговори на раст тражње за „инстант плаћањима" на европском тржишту и да се избегну национална решења која би уместо обезбеђивања јединственог тржишта довела до његове фрагментације.

Препознајући да се ради о значајним иновацијама на тржишту плаћања мале новчане вредности и BIS је у новембру 2016. године, као резултат спроведеног истраживања, објавила студију под називом Брза плаћања – Побољшање брзине и доступности плаћања „мале" новчане вредности.[10]

Из угла надгледања/надзора над пословањем платних система, увођење „инстант плаћања" може позитивно утицати на ефикасност. Међутим, ако се сагледава сигурно и стабилно пословање платних система за инстант плаћања,

[8] Pan-European instant payments in euro: definition, vision and way forward, ERPB, 2014.
[9] Европски савет за плаћања (EPC – European Payment Council) усвојио је шему инстант трансфера одобрења за јединствено европско тржиште за плаћања (SCT Inst Scheme).
[10] Fast payments – Enhancing the speed and availability of retail payments, BIS, 2016.

иако су ризици којима су платни системи изложени исти, они добијају нову димензију у условима пословања 24/7/365 и у оквиру правила да примаочев пружалац платних услуга унапред мора ставити на располагање средства примаоцу плаћања, а да новчана средства још увек није добио од платиочевог пружаоца платних услуга.

Приступ централних банака надгледању/надзору платних система за инстант плаћања може се разликовати по земљама имајући у виду примену Принципа за инфраструктуре финансијског тржишта који су првенствено намењени системски важним платним системима. С обзиром на то да већина платних система за инстант плаћања неће бити од системског значаја – могу се појавити разлике у политикама надгледања што је аспект који ће у наредним годинама добити на значају у смислу постизања одређеног степена стандардизације на глобалном нивоу.