



НАРОДНА БАНКА НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

Врз основа на член 47 став 1 точка 6 од Законот за Народната банка на Република Северна Македонија („Службен весник на Република Северна Македонија“ бр. 158/10, 123/12, 43/14, 153/15, 6/16, 83/18 и „Службен весник на Република Северна Македонија“ бр. 110/21) и член 123 став 9 од Законот за платежни услуги и платни системи („Службен весник на Република Северна Македонија“ бр. 90/22), Советот на Народната банка на Република Северна Македонија донесе

ОДЛУКА

за насоките за класификација на оперативните и сигурносните инциденти и начинот и постапката за известување за настанати инциденти и измами

I. ОПШТИ ОДРЕДБИ

1. Со оваа одлука поблиску се пропишуваат:

- насоките за класификација на значајните оперативни или сигурносни инциденти од страна на давателите на платежни услуги во согласност со дефинирани критериуми, и
- начинот и постапката за известување за настанати значајни оперативни и сигурносни инциденти и измами до Народната банка на Република Северна Македонија (во натамошниот текст: Народната банка).

II. НАСОКИ ЗА КЛАСИФИКАЦИЈА НА ЗНАЧАЕН ОПЕРАТИВЕН ИЛИ СИГУРНОСЕН ИНЦИДЕНТ

2. Давателите на платежните услуги се должни да извршат класификација на значајноста на оперативниот и сигурносен инцидент со процена на неговото влијание преку следниве критериуми:

2.1 **„Засегнати трансакции“** – Давателите на платежните услуги се должни да ја утврдат вкупната вредност на платежните трансакции коишто се засегнати од инцидентот, како и нивниот процент од вообичаениот износ на платежни трансакции коишто се обезбедуваат преку засегнатата платежна услуга.

Како засегнати трансакции се сметаат сите домашни и прекугранични трансакции врз кои влијаел инцидентот директно или индиректно, или имало можност да влијае.

Притоа, се земаат предвид сите трансакции коишто не можеле да се иницираат или да се обработат, оние коишто се со измената содржина во пораката за плаќање и оние коишто се иницирани со намера за измама или оние чие редовно извршување на каков било начин било спречено

или загрозено од инцидент повеќе од 1 (еден) час. Траењето на инцидентот се мери од моментот на настанување на инцидентот до моментот кога редовните активности се вратени на истото ниво на квалитет на услугата којашто била загрозена од инцидентот.

Давателите на платежните услуги се должни како вообичаен износ на платежни трансакции да го сметаат годишниот дневен просек на домашни и прекугранични платежни трансакции извршени преку платежните услуги коишто се зафатени со инцидентот, земајќи ја претходната година како референтен период за пресметка.

По утврдувањето на засегнатите трансакции, се утврдува нивната вкупна вредност и нивниот процент од вообичаениот износ на платежни трансакции коишто се обезбедуваат преку засегнатата платежна услуга.

Ако давателот на платежни услуги проценува дека добиената бројка не е репрезентативна, должен е да употреби друга репрезентативна пресметка и да ја информира Народната банка за причините за употребата на избраниот пристап за пресметка.

- 2.2. **„Засегнати корисници на платежни услуги“** – Давателите на платежните услуги се должни да го определат бројот на корисниците на платежни услуги засегнати од инцидентот и нивниот процент од вкупниот број корисници на платежните услуги.

Како засегнати корисници на платежни услуги се сметаат сите клиенти кои имаат договор со давателот на платежни услуги кој им ја овозможува засегнатата платежна услуга и кои претрпеле или веројатно ќе претрпат последици од инцидент со времетраење повеќе од 1 (еден) час. Траењето на инцидентот се мери од моментот на настанувањето на инцидентот до моментот кога редовните активности се вратени на истото ниво на квалитет на услугата која била загрозена од инцидентот.

Давателите на платежни услуги во согласност со претходните активности се должни да го проценат бројот на корисниците кои веројатно би ја користеле платежната услуга во текот на инцидентот.

Во случај кога давателот на платежна услуга е дел од група, дава или користи оперативни услуги на други субјекти, тој е должен да ги земе предвид само своите корисници на платежни услуги.

Во утврдувањето на вкупниот број корисници се зема вкупниот број домашни и прекугранични корисници на платежни услуги коишто имаат склучени договори во моментот на настанување на инцидентот и коишто имаат пристап до засегнатата платежна услуга независно од нивната големина и од нивниот активен или пасивен статус.

- 2.3 **„Нарушена сигурност на мрежните или информациските системи“** – Давателите на платежните услуги се должни да утврдат дали некоја злонамерна активност ја загрозила расположливоста, автентичноста, интегритетот или доверливоста на мрежните или информациските

системи (вклучително и на податоците) поврзани со давањето платежни услуги.

- 2.4 **„Прекин на услугата“** – Давателите на платежните услуги се должни да го определат временскиот период во кој иницирањето и/или извршувањето на платежната услуга или пристапот до платежната сметка не е на располагање на корисникот на платежната услуга или времето во кое платниот налог нема да може да биде извршен.

Времетраењето на прекинет се утврдува од моментот кога прекинет е започнат, земајќи го предвид работното време на давателите на платежни услуги во кое се даваат платежните услуги. Доколку давателот на платежни услуги не е во состојба да го утврди моментот кога е започнат прекинет на услугите, должен е времето на прекин да го смета од моментот на откривањето на прекинет.

- 2.5 **„Економско влијание“** – Давателите на платежните услуги се должни да ги утврдат вкупните финансиски загуби коишто директно или индиректно се поврзани со инцидентот, како и нивната релативна вредност во однос на капиталот на давателот на платежни услуги.

Како финансиски загуби се земаат предвид загубените парични средства или имот, трошоци за замена на хардвер или софтвер, други трошоци поврзани со форензика или дополнителни мерки, надоместоци поради неисполнување на обврските од договорот, казни, штети настанати кон трети лица и изгубени приходи. Давателите на платежни услуги се должни да ги земат предвид само оние индиректни загуби коишто се веќе познати или постои голема веројатност дека ќе настанат.

- 2.6 **„Засилено ниво на интерна комуникација“** – Давателите на платежните услуги се должни да утврдат дали инцидентот е пријавен или ќе биде пријавен до членовите на органите на управување.

Исто така, давателите на платежни услуги се должни да утврдат дали поради влијанието на инцидентот кон платежните услуги постои веројатност да се прогласи кризна состојба во согласност со планот за непрекинатост во работењето.

- 2.7 **„Можност да бидат засегнати други даватели на платежните услуги и инфраструктури“** – Давателите на платежните услуги се должни да ги утврдат можните последици коишто би ги предизвикал инцидентот за системот, т.е. неговиот потенцијал да се пренесе надвор од засегнатиот давател на платежна услуга.

За таа цел, се врши проценка на влијанието на инцидентот кон финансискиот систем, дали е проширен кон други даватели на платежни услуги, односно дали е можно влијание врз правилното функционирање на инфраструктурата на финансискиот систем.

- 2.8 **„Влијание на репутација“** – Давателите на платежните услуги се должни да ги утврдат негативните влијанија на инцидентот врз довербата на корисниците кон давателот на платежната услуга и на загубата на довербата кон платежната услуга и платниот систем.

За таа цел, давателите на платежни услуги се должни да земат предвид: дали од корисниците на платежните услуги и/или други даватели на платежни услуги има оплаки за негативното влијание на настанатиот инцидент; дали инцидентот имал видливо влијание врз платежните услуги и поради тоа може да биде или веројатно ќе биде медиумски покриен (со традиционални и современи медиумски канали – социјални мрежи); дали има пропусти во исполнувањето на обврските од договорот според кои постои веројатност за правни последици кон давателот на платежната услуга; дали има пропусти во исполнувањето на законските обврски и дали би довел до преземање регулаторни мерки кон давателот на платежната услуга и дали сличен инцидент се случил и претходно.

3. Давателите на платежни услуги се должни да го проценат влијанието на инцидентот по секој критериум за класификација и да утврдат дали се веќе достигнати или постои веројатност да се достигнат поставените прагови (наведени во табелата од став 1 на оваа точка), сè до конечното разрешување на инцидентот.

Критериум	Ниско влијание	Високо влијание
Засегнати трансакции	(> 10% од редовното ниво на трансакции на давателот на платежна услуга (во однос на бројот трансакции) и времетраење на инцидентот > 1 час *) или (> 31 000 000 денари и времетраење на инцидентот > 1 час *)	(> 25% од редовното ниво на трансакции на давателот на платежна услуга (во однос на бројот трансакции)) или (> 310 000 000 денари)
Засегнати корисници на платежни услуги	(> 5.000 и времетраење на инцидентот > 1 час *) или (> 10% од корисниците на платежните услуги кај давателот на платежната услуга и времетраење на инцидентот > 1 час *)	(> 50 000) или (> 25% од корисниците а платежните услуги кај давателот на платежната услуга)
Прекин на услугата	> 2 часа	Не се применува
Нарушена сигурност на мрежните или информациските системи	Да	Не се применува

Економско влијание	Не се применува	Директна штета: > Максимум од: (0,1% од основен капитал; 12.400.000 денари) или Индиректна штета: > 310.000.000 денари
Засилено ниво на интерна комуникација	Да	Да, и активирање кризна состојба во согласност со планот за непрекинатост во работењето
Можност да бидат засегнати други даватели на платежните услуги и инфраструктури	Да	Не се применува
Влијание на репутација	Да	Не се применува

* Прагот од времетраењето на инцидентот поголем од 1 (еден) час се однесува на оперативните инциденти коишто имаат влијание врз иницирањето и/или обработката на платежните трансакции.

4. Давателите на платежните услуги се должни да го класифицираат оперативниот или сигурносниот инцидент за значаен, доколку се исполнети следниве услови:
- најмалку еден критериум за класификација е со високо ниво на влијание, во согласност со табелата од точка 3 став 1 од оваа одлука или
 - најмалку три критериуми за класификација се со ниско ниво на влијание, во согласност со табелата од точка 3 став 1 од оваа одлука.

5. Доколку давателите на платежни услуги не располагаат со точни податоци со кои може да ги поткрепат своите оценки за тоа дали одреден критериум е постигнат или веројатно ќе биде постигнат пред разрешувањето на инцидентот, потребно е да направат проценка.

Процената од став 1 од оваа точка од Одлуката може да се користи во почетната фаза на инцидентот.

6. Давателите на платежни услуги се должни во текот на траењето на инцидентот постојано да прават процени за измени во однос на класификацијата на инцидентот особено кон повисоко ниво (инцидент којшто не е значаен да стане значаен) или кон пониско ниво (значаен инцидент да се прекласифицира како незначаен).

За секоја прекласификација на инцидент од значајно ниво, во инцидент којшто не е значаен треба веднаш да се информира Народната банка.

III. ПОСТАПКА НА ИЗВЕСТУВАЊЕ ЗА ЗНАЧАЕН ОПЕРАТИВЕН И СИГУРНОСЕН ИНЦИДЕНТ ДО НАРОДНАТА БАНКА

7. Давателите на платежни услуги се должни да изготват и да поднесат до Народната банка извештај за значајниот оперативен и сигурносен инцидент, којшто е пропишан во прилогот 1 на оваа одлука.

За секој инцидент, давателите на платежните услуги се должни да поднесат почетен, преоден и конечен извештај со употреба на пропишан образец А, Б или Ц во прилогот 1 на оваа одлука.

Се смета дека давателите на платежни услуги уредно ги доставиле податоците доколку тие:

- се примени во Народната банка во рокови предвидени со одлуката;
- се точни и целосни.

8. Во случај кога инцидентот има или може да има влијание врз економската состојба на корисниците на платежни услуги, давателите на платежни услуги се должни да достават до Народната банка примерок од информацијата којашто е доставена до корисниците на платежни услуги за настанатиот инцидент и за мерките кои тие треба да ги преземат за намалување на негативните ефекти.
9. Давателите на платежните услуги се должни на барање на Народната банка да достават дополнителни документи како поткрепа на информациите доставени со пропишаниот образец.
10. Давателите на платежните услуги се должни да обезбедат доверливост и интегритет на информациите коишто се разменуваат.

Почетен извештај

11. Давателите на платежни услуги се должни да поднесат почетен извештај со пополнување на образецот А до Народната банка веднаш и без непотребно одлагање, а најдоцна во рок од три дена откако одреден инцидент ќе се класифицира како значаен.
12. Давателите на платежни услуги се должни да извршат класификација на значајноста на инцидент, во согласност со точка 4 од оваа одлука, не подоцна од 24 часа по откривањето на инцидентот.

Доколку за класификација на инцидентот е потребен подолг временски период, давателот на платежни услуги во почетниот извештај ги наведува причините поради кои не може да се изврши класификацијата.

Давателот на платежни услуги е должен да поднесе почетен извештај и во случај кога инцидент којшто претходно не бил значаен се рекласифицира како значаен инцидент, веднаш по промената на статусот.

Преоден извештај

13. По нормализацијата на редовните активности, давателите на платежни услуги се должни да поднесат преоден извештај до Народната банка.

За нормализација на редовните активности кај давателите на платежни услуги ќе се смета кога редовните активности ќе се одвиваат со исто ниво на услуга како што е одредена или утврдена од давателот на платежните услуги и кога не се во примена вонредни мерки.

Доколку редовните активности не се нормализирани, давателот на платежни услуги е должен да достави преоден извештај во рок од три работни дена од поднесувањето на почетниот извештај.

14. Преодниот извештај треба да содржи детален опис на инцидентот и неговите последици со пополнување на образецот Б. Во случај на недостаток на точни податоци, давателите на платежни услуги се должни да применат постапка на процена при пополнувањето на бараните полиња во обрасците.
15. Давателите на платежни услуги се должни да ги ажурираат информациите наведени во деловите на образецот А и образецот Б, при значителни измени коишто настанале од поднесувањето на претходниот преоден извештај.
16. Доколку во текот на три дена од моментот кога инцидентот е класифициран за значаен се воспостави редовното работење, давателот на платежни услуги должен е да поднесе истовремено почетен и преоден извештај (обрасците А и Б) до Народната банка во наведениот рок од три дена од точка 11 од оваа одлука.

Конечен извештај

17. Давателите на платежни услуги се должни да поднесат конечен извештај по извршените детални анализи за откривање на причините за настанување на инцидентот со пополнувањето на образецот Ц.
18. Давателите на платежни услуги се должни да го достават конечниот извештај до Народната банка не подоцна од 20 работни дена од датумот на нормализирање на редовното работење.

Доколку давателите на платежни услуги не се во можност да ги откријат вистинските причини за настанување на инцидентот или сè уште немаат точни податоци за ажурирање на претходните извештаи, се должни да побараат од Народната банка продолжување на рокот за достава на конечниот извештај од став 1 на оваа точка.

Во барањето од став 2 на оваа точка од Одлуката, давателите на платежни услуги се должни да ги наведат причините за пролонгирање на временскиот рок, како и да направат процена на датумот на доставување на конечниот извештај.

19. Давателите на платежни услуги се должни во својот конечен извештај да ја информираат Народната банка за:
 - точните податоци во обрасците А и Б, наместо проценетите вредности и
 - утврдената причина за инцидентот, доколку е познато и мерките коишто се усвоени или се предвидени за спречување на неговата повторна појава.
20. Во случај на утврдување случај кога пријавениот инцидент не ги исполнува критериумите за негова класификација како значаен, давателот на платежни услуги е должен веднаш да достави конечен извештај, пред предвидениот временски рок од точка 18 став 1 од оваа одлука.

Во случаите од став 1 на оваа точка, давателите на платежни услуги се должни наместо пополнување на образецот Ц да го означат полето **„инцидент рекласифициран како незначаен“** и да ги објаснат причините со кои се оправдува рекласификацијата.

IV. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

21. Давателите на платежните услуги се должни да го усогласат своето работење со барањата на оваа одлука најдоцна до 19 февруари 2024 година.

Давателите на платежните услуги коишто се основани до денот на примената на оваа одлука и коишто имаат дозвола за основање и работење на банка ќе ја применуваат одредбата од точка 47 од Одлуката за Методологија за сигурност на информативниот систем на банката („Службен весник на Република Македонија“ бр. 78/18) до денот на усогласувањето на своето работење со барањата на оваа одлука, а најдоцна до 19 февруари 2024 година.

22. Точката 47 од Одлуката за Методологија за сигурност на информативниот систем на банката („Службен весник на Република Македонија“ бр. 78/18) престанува да важи на 20 февруари 2024 година.

23. Оваа одлука влегува во сила на денот на објавувањето во „Службен весник на Република Северна Македонија“.

**О бр.02-15/XXII-9/2022
28 декември 2022 година
Скопје**

**Гувернер и
претседавач на Советот на
Народна банка на
Република Северна Македонија
д-р Анита Ангеловска-Бежоска**

Прилог 1:

Образец А (Почетен извештај)

Извештај за значаен инцидент				
Почетен извештај		се пополнуват три дена по класификација на инцидентот за значаен		
Датум на известување (ДД/ММ/ГГГГ)		Време (чч:мм)		
Уникатен код на инцидентот				
ОБРАЗЕЦ А - Почетен Извештај				
А 1 - ОПШТИ ПОДАТОЦИ				
Примарен контакт		Email		Тел
Резервен контакт		Email		Тел
А 2 - ОТКРИВАЊЕ И КЛАСИФИКАЦИЈА				
Датум и време на откривање на инцидентот (ДД/ММ/ГГГГ чч:мм)				
Датум и време на класификација на инцидентот (ДД/ММ/ГГГГ чч:мм)				
Инцидентот беше откриен од:				
Тип на инцидент:				
Критериум за значајност:				
☐ Засегнати трансакции ☐ Засегнати корисници на платевни услуги ☐ Прекин на услугата ☐ Нарушена сигурност на мрежите или информационо-ситеми ☐ Економско влијание ☐ Засегнато ниво на интерна комуникација ☐ Може да бидат засегнати други даватели на платевни услуги и ☐ Влијание на репутација				
Кратко и општо објаснување за инцидентот:				
Дали известивте други надлежни органи				
Причини за касно праќање на почетен извештај				

Образец Б (Преоден извештај)

[illegible]

Образец Ц (Конечен извештај)

Извештај за значаен инцидент	
Изберете го типот на извештај: 	во тек на 20 работни дена од испраќањето на претходниот преоден извештај
Ве молам објаснете причина за рекласификација: (се однесува само за инциденти рекласифицирани како нежачајни)	
Датум на известување (ДД/ММ/ГГГГ)	Време (чч:мм)
Уникатен код на инцидентот	

ОБРАЗЕЦ Ц - Конечен извештај	
Ако не е испратен преоден извештај, ве молам пополнете го и образецот Б	
Ц 1 - ОПШТИ ДЕТАЛИ	
Ажурирана информација од почетниот и преодниот извештај	
Имени направени од претходните извештаи	
Други релевантни информации?	
Дали сите почетни контроли се воспоставени?	☒ Да
Ако е „Не“ објасни која контрола недостига и за кој период ќе биде воспоставена	
Ц 2 - УТВРДУВАЊЕ НА ПРИЧИНА И ПРЕЗЕМЕНИ АКТИВНОСТИ	
Која е вистинската причина (ако е откриена)?	☐ Законерна активност ☐ грешка во процес ☐ грешка во систем ☐ новечка грешка ☐ надворешен настан ☐ друго
Изберете и/или наведете:	☒ Малициозен код ☒ Прибирање на информации ☒ Упад ☒ дистрибуирање/прекин на услуги (D/Dos) ☒ Намерени внатрешни активности ☒ Намерени надворешни физички изготвувања ☒ Безбедност на информација ☒ Идентификација ☒ Друго ☒ Слаба контрола или надзор ☒ проблем во комуникација ☒ Несоодветна активност ☒ Несоодветно управување со промени ☒ Неадекватни процедури и документираност ☒ Пропуст во обновата ☒ Друго Ако е „друго“, наведете: ☒ Грешка во хардвер ☒ Грешка во иража ☒ Проблем со база на податоци ☒ Софтверска грешка ☒ Физичка штета ☒ Друго ☒ Ненамерено ☒ Трејд ☒ Недоволно ресурси ☒ Друго ☒ Грешка на давател/инфраструктура ☒ Виша сила ☒ Друго
Други релевантни информации за причината за инцидентот	
Главни активности и мерки кои се преземени или се планираат да се преземат за да се спречи повторна појава на инцидентот во иднина (ако се знае)?	
Ц 3 - ДОПОЛНИТЕЛНИ ИНФОРМАЦИИ	
Дали за инцидентот се запознаени другите даватели?	☐ Да ☐ Не
Ако е „Да“, образложете:	
Дали има некоја правна постапка против Давателот на ПУ?	☐ Да ☐ Не
Ако е „Да“, образложете:	
Оценка на активност која е преземена?	☐ Да ☐ Не
Ве молам образложете:	