ЕС

ЗАРЕГИСТРИРОВАНО:
Министерство юстиции
№ 1905 от 19.01.2024 г.
Министр Вероника МИХАЙЛОВ-МОРАРУ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ НАЦИОНАЛЬНОГО БАНКА МОЛДОВЫ ПОСТАНОВЛЕНИЕ № 12 от 11.01.2024

(в силу 05.08.2024, за исключением пкт.72 - 26.01.2024)

об утверждении Регламента о строгой аутентификации клиентов и открытом, общем и безопасном стандарте связи между поставщиками платежных услуг

Мониторул Официал ал Р. Молдова № 36-39 ст. 90 от 26.01.2024
изменен Пост.НБМ N 267 от 31.10.2024 , *в силу 07.11.2024*

На основании части (7) ст.52[4] Закона о платежных услугах и электронных деньгах № 114/2012 (Официальный монитор Республики Молдова, 2012, № 193-197, ст.661), с последующими изменениями, Исполнительный комитет Национального банка Молдовы

ПОСТАНОВЛЯЕТ:

1. Утвердить Регламент о строгой аутентификации клиентов и открытом, общем и безопасном стандарте связи между поставщиками платежных услуг (прилагается).

2. Настоящее постановление вступает в силу 1 февраля 2025г., за исключением пкт.72, который вступает в силу на день опубликования.

[Пкт.2 изменен Пост.НБМ N 267 от 31.10.2024]

ПРЕДСЕДАТЕЛЬ
ИСПОЛНИТЕЛЬНОГО КОМИТЕТА **Анка-Дана ДРАГУ**

№ 12. Кишинэу, 11 января 2024 г.

Утвержден
Постановлением Исполнительного комитета
Национального банка Молдовы
№ 12 от 11.01.2024

РЕГЛАМЕНТ
о строгой аутентификации клиентов и открытом, общем и безопасном стандарте связи между поставщиками платежных услуг

Настоящий Регламент перелагает делегированный Регламент (ЕС) № 2018/389 Комиссии от 27 ноября 2017 года, о нормативных технических стандартах для строгой аутентификации клиентов и открыты, общих и безопасных стандартах связи, опубликованный в Официальном Журнале серия L № 69 от 13.03.2018, с последними поправками, внесенными Делегированным регламентом Комиссии (ЕС) 2022/2360 от 3 августа 2022 г. и Руководство EBA/GL/2018/07 относительно условий, необходимых для получения права на освобождение от резервного механизма, предусмотренного частью (6) статьи 33 Регламента (ЕС) 2018/389.

Глава I
ОБЩИЕ ПОЛОЖЕНИЯ

Часть 1
ПРЕДМЕТ

1. Регламент устанавливает требования, которые должны соблюдать поставщики платежных услуг в целях реализации мер безопасности, позволяющих им:

1) применять процедуру строгой аутентификации клиентов в соответствии со ст. 52^4 Закона о платежных услугах и электронных деньгах №114/2012 (далее – Закон № 114/2012);

2) быть освобожденными от применения требований безопасности, касающихся строгой аутентификации клиентов, при соблюдении определенных и ограниченных условий, в зависимости от уровня риска, суммы и частоты платежной операции, а также платежного канала, используемого для ее выполнения;

3) защищать конфиденциальность, целостность и подлинность персонализированных элементов безопасности пользователя платежных услуг;

4) внедрять открытый, общий и безопасный стандарт связи между поставщиками платежных услуг, которые предоставляют услуги по управлению счетом, поставщиками услуг по инициированию платежа, поставщиками услуг по информированию о счетах, плательщиками, получателями платежей и другими поставщиками платежных услуг в отношении предоставления и использования платежных услуг в соответствии со ст. 52^1 – 52^4 Закона № 114/2012.

2. Понятия и выражения, используемые в настоящем регламенте, имеют значения, предусмотренные Законом № 114/2012 и другими нормативными актами, изданными Национальным банком Молдовы.

3. Дополнительно для целей настоящего регламента используются следующие понятия:

Компетенции в области информационной безопасности – совокупность конкретных знаний, подтвержденных сертификатом специалиста, выданным признанным субъектом и позволяющих аудитору издать заключение о соответствии мер безопасности поставщика платежных услуг требованиям, изложенным в настоящем регламенте на основе знаний в области информационной безопасности.

Открытый, общий и безопасный стандарт связи – набор функциональных и технических спецификаций для конкретных интерфейсов поставщиков платежных услуг, предлагающих услуги по управлению счетами, позволяющий поставщикам услуг по инициированию платежей, поставщикам услуг по информированию о счетах и поставщикам платежных услуг, выпускающим платежные инструменты на основе карт, доступ к платежным счетам пользователей платежных услуг.

Ежедневная доля ошибочных ответов – доля, рассчитанная поставщиком платежных услуг, предоставляющим доступные онлайн услуги по управлению

платежных счетов, относительно количества сообщений об ошибках в день, которые касаются ошибок, которые могут быть отнесены к поставщику платежных услуг, предоставляющему доступные услуги по управлению платежных счетов онлайн, отправленное им в течение суток поставщикам услуг по инициированию платежей, поставщикам услуг по информированию о счетах и поставщикам платежных услуг, выпускающим платежные инструменты на основе карт, в соответствии с п. 102 и 103, разделенное на количество заявок, полученных в тот же день поставщиком платежных услуг, который предлагает услуги по управлению платежных счетов, доступных онлайн, от поставщиков услуг по инициированию платежей, поставщиков услуг по информированию о счетах и поставщиков платежных услуг, которые выпускают платежные инструменты на основе карт.

Часть 2
ОБЩИЕ ТРЕБОВАНИЯ К АУТЕНТИФИКАЦИИ

4. Поставщики платежных услуг создают механизмы мониторинга операций, позволяющие выявлять несанкционированные или мошеннические платежные операции, в целях реализации мер безопасности, предотвращения и ограничения несанкционированных или мошеннических платежных операций, предусмотренных подп. 1) и 2) п.1.

Эти механизмы основаны на анализе платежных операций с учетом особенных элементов пользователя платежных услуг при обычном использовании персонализированных элементов безопасности.

5. Поставщики платежных услуг должны обеспечить, чтобы механизмы мониторинга операций были основаны на риске и учитывали, как минимум, следующие факторы:

1) списки скомпрометированных или украденных учетных данных;
2) стоимость каждой платежной операции;
3) известные сценарии мошенничества при оказании платежных услуг;
4) показатели нарушения конфиденциальности, целостности или аутентичности сеанса в результате процедуры аутентификации;
5) реестр нормального и ненормального использования устройства доступа или программного обеспечения, предоставленного пользователю платежных услуг поставщиком платежных услуг;
6) аномальное/необычное географическое положение плательщика;
7) географическое положение с повышенным риском получателя платежа.

Часть 3
ПЕРЕСМОТР МЕР БЕЗОПАСНОСТИ

6. Реализация мер безопасности, предусмотренных п. 1, документируется, тестируется, оценивается и проверяется не реже одного раза в 3 года или по требованию Национального банка Молдовы аудиторами, обладающими компетенцией и опытом работы в области безопасности информации и платежей, которые являются в оперативном отношении независимыми от поставщика платежных услуг.

Период между проверками, предусмотренными настоящим пунктом, устанавливается с учетом соответствующей основы бухгалтерского учета и обязательного аудита, применимого к поставщику платежных услуг.

7. Поставщики платежных услуг, применяющие отступления, предусмотренные п. 42-44, подлежат проверке не реже одного раза в год в отношении методологии расчета уровня мошенничества, модели, используемой при расчете уровня мошенничества, и сообщаемых показателей мошенничества, а порядок расчета показателей мошенничества установлен п. 45-47. Внутренний аудитор, проводящий данный аудит, обладает компетенцией в области

информационной безопасности и безопасности платежей и в оперативном отношении независим от поставщика платежных услуг. В течение первого года, в котором применяется отступление, предусмотренное п. 42-44, а затем не реже одного раза в 3 года или чаще, по требованию Национального банка Молдовы, данный аудит проводится внешним независимым и квалифицированным аудитором.

8. Аудит, предусмотренный п. 6 и 7, представляет собой оценку и заключение аудитора о соответствии мер безопасности поставщика платежных услуг требованиям, установленным настоящим регламентом. Отчет и оценка представляются в Национальный банк Молдовы в соответствии с требованиями, установленными частью (3) ст. 30 Закона № 114/2012.

Глава II
МЕРЫ БЕЗОПАСНОСТИ ДЛЯ ОБЕСПЕЧЕНИЯ СТРОГОЙ АУТЕНТИФИКАЦИИ КЛИЕНТОВ
Часть 1
КОД АУТЕНТИФИКАЦИИ

9. Если поставщики платежных услуг применяют строгую аутентификацию клиентов в соответствии с частью (1) ст.52^4 Закона № 114/2012, аутентификация основана на двух или более элементах, которые включены в категорию знаний, владения и принадлежности, и приводит к генерированию кода аутентификации.

Код аутентификации принимается поставщиком платежных услуг только один раз, когда плательщик использует код аутентификации для доступа к своему платежному счету онлайн, для инициации электронной платежной операции или для удаленного выполнения любого действия, что может быть связано с риском мошенничества с платежами или других злоупотреблений.

10. Для целей п. 9 поставщики платежных услуг принимают меры безопасности, гарантируя выполнение каждого из следующих требований:

1) из раскрытия кода аутентификации не может быть получена никакая информация относительно любого из элементов, предусмотренных в п. 9;

2) невозможно сгенерировать новый код аутентификации на основе знания любого другого ранее сгенерированного кода аутентификации;

3) код аутентификации невозможно подделать;

4) код можно использовать только один раз;

5) код действителен ограниченное время.

11. Поставщики платежных услуг должны обеспечить, чтобы аутентификация с использованием кода аутентификации включала каждую из следующих мер:

1) если при аутентификации для удаленного доступа, для удаленных электронных платежей и для любых других удаленных действий, которые могут повлечь за собой риск мошенничества с платежами или других злоупотреблений, не удалось сгенерировать код аутентификации для целей п. 9, невозможно определить, какой из элементов, предусмотренных пунктом 9, был неверным;

2) количество неудачных попыток аутентификации, которые могут иметь место последовательно, после которых выполняются действия, предусмотренные частью (1) ст. 52^4 Закона № 114/2012 временно или постоянно блокируются, их количество не должно превышать пяти в течение 15 минут. Если блокировка носит временный характер, продолжительность блокировки и количество повторных попыток устанавливаются исходя из особенностей услуги, предоставляемой плательщику, и всех связанных с этих рисков с учетом как минимум факторов, предусмотренных пунктом 5. Если блокировка стала постоянной, поставщик платежных услуг устанавливает безопасную процедуру, позволяющую плательщику восстановить доступ к электронным платежным инструментам. Плательщик будет проинформирован до того, как блокировка станет постоянной.

3) сеансы связи защищены от перехвата аутентификационных данных и от манипуляций со стороны посторонних лиц в соответствии с требованиями, установленными главой V;

4) сеанс связи признается недействительным, если плательщик не совершает никаких действий в течение пяти минут после аутентификации.

Часть 2
ДИНАМИЧЕСКАЯ СВЯЗЬ

12. Если поставщики платежных услуг применяют строгую аутентификацию клиентов в соответствии с частью (2) ст. 52^4 Закона № 114/2012, в дополнение к требованиям, изложенным в п. 9–11 настоящего регламента, они также принимают меры безопасности, отвечающие каждому из следующих требований:

1) плательщик информируется о сумме платежной операции и о получателе платежа;

2) сгенерированный код аутентификации соответствует сумме платежной операции и получателю платежа, согласованными плательщиком во время инициирования операции;

3) код аутентификации, принятый поставщиком платежных услуг, соответствует первоначальной сумме платежной операции и личности получателя платежа, согласованными плательщиком;

4) любое изменение стоимости или получателя платежа приводит к аннулированию сгенерированного кода аутентификации.

13. В целях п. 12 поставщики платежных услуг принимают меры безопасности для обеспечения на всех этапах процесса аутентификации конфиденциальности, подлинности и целостности каждого из следующих элементов:

1) сумма платежной операции и получатель платежа;

2) информация, отображаемая плательщику, включая генерирование, передачу и использование кода аутентификации.

14. В целях подп.2) п. 12 и если поставщики платежных услуг применяют строгую аутентификацию клиентов в соответствии с частью (2) ст. 52^4 Закона № 114/2012, к коду аутентификации применяются следующие требования:

1) для платежной операции, связанной с картой, для которой плательщик дал свое согласие в отношении точной суммы денежных средств, подлежащих блокированию согласно части (1) ст. 60^1 Закона № 114/2012, код аутентификации должен соответствовать сумме, на блокировку которой плательщик дал согласие, и которая была согласована плательщиком в момент инициирования операции;

2) в отношении платежных операций, на совершение которых плательщик выразил согласие на выполнение серии (пакета инструкций) дистанционных электронных платежных операций одному или нескольким бенефициарам, код аутентификации относится к общей сумме серии платежных операций и указанным получателям платежа.

Часть 3
ТРЕБОВАНИЯ К ЭЛЕМЕНТАМ СТРОГОЙ АУТЕНТИФИКАЦИИ

15. Поставщики платежных услуг принимают меры безопасности для снижения рисков элементов:

a) строгой аутентификации клиентов, классифицируемых как знания, подлежащие прочтению или раскрытию неавторизованным лицам. Использование этих элементов плательщиком регулируется смягчающими мерами, направленными на предотвращение их раскрытия неавторизованным лицам;

b) строгой аутентификации клиентов, классифицированных как владение, предназначенное для использования неавторизованными лицами. Использование

этих элементов плательщиком регулируется мерами, направленными на предотвращение повторения элементов;

c) аутентификации, квалифицируемой как неотъемлемой и считываемой устройствами доступа и программным обеспечением, предоставленными плательщику для считывания неавторизованными сторонами. В качестве минимального условия поставщики платежных услуг должны обеспечить, чтобы их устройства доступа и программное обеспечение имели очень низкую вероятность аутентификации неавторизованной стороны в качестве плательщика. Использование этих элементов плательщиком регулируется мерами, гарантирующими, что эти устройства и программное обеспечение противостоят несанкционированному использованию элементов посредством доступа к этим устройствам и программному обеспечению.

16. Поставщики платежных услуг обеспечивают, чтобы использование элементов строгой аутентификации клиентов, предусмотренных в п. 15, с точки зрения их технологии, алгоритмов и параметров, подвергалось мерам, гарантирующим, что нарушение одного из элементов не ставит под угрозу надежность остальных элементов.

17. Поставщики платежных услуг должны применять меры безопасности в случае использования каких-либо элементов строгой аутентификации клиента или самого кода аутентификации через универсальное устройство, чтобы снизить риск, который может возникнуть в результате компрометации этого универсального устройства. Меры по смягчению последствий включают в себя каждое из следующих действий:

1) использование защищенных сред исполнения, выделенных с помощью программного обеспечения, установленных на универсальном устройстве;

2) механизмы, гарантирующие, что программное обеспечение или устройство не были модифицированы плательщиком или третьим лицом;

3) если произошли изменения в системах, управляющих элементами строгой аутентификации и кодами аутентификации на универсальном устройстве, механизмы смягчения их последствий.

Глава III
ОТСТУПЛЕНИЯ ОТ СТРОГОЙ АУТЕНТИФИКАЦИИ КЛИЕНТОВ

Часть 1
ДОСТУП К ИНФОРМАЦИИ О ПЛАТЕЖНОМ СЧЕТЕ НЕПОСРЕДСТВЕННО У ПОСТАВЩИКА ПЛАТЕЖНЫХ УСЛУГ, ПРЕДОСТАВЛЯЮЩЕГО УСЛУГИ ПО УПРАВЛЕНИЮ СЧЕТОМ

18. Поставщики платежных услуг имеют право не применять строгую аутентификацию клиентов при условии соблюдения требований, указанных в п. 4 и 5, если пользователь платежных услуг получает прямой онлайн-доступ к своему платежному счету, при условии, что доступ ограничен одним из следующие онлайн-элементов без раскрытия конфиденциальных платежных данных:

1) остаток одного или нескольких платежных счетов, указанных пользователем;

2) платежные операции, выполненные за последние 90 дней через один или несколько платежных счетов, указанных пользователем.

19. Для целей п. 18 поставщики платежных услуг не освобождаются от применения строгой аутентификации клиентов, если соблюдается любое из следующих условий:

1) пользователь платежных услуг впервые получает доступ в режиме онлайн к информации, указанной в п. 18;

2) прошло более 180 дней с момента последнего доступа пользователя платежных услуг в режиме онлайн к информации, предусмотренной п. 18, и с момента применения строгой аутентификации клиента.

Часть 2
ДОСТУП К ИНФОРМАЦИИ О ПЛАТЕЖНОМ СЧЕТЕ ЧЕРЕЗ ПОСТАВЩИКА УСЛУГ ПО ИНФОРМИРОВАНИЮ О СЧЕТАХ

20. Поставщики платежных услуг не применяют строгую аутентификацию клиентов, когда пользователь платежных услуг получает доступ к своему счету онлайн-платежей через поставщика услуг по информированию о счетах, при условии, что доступ ограничен одним из следующих онлайн-элементов без раскрытия конфиденциальных платежных данных:

1) остаток одного или нескольких указанных платежных счетов;

2) платежные операции, выполненные за последние 90 дней через один или несколько указанных платежных счетов.

21. В отступление от п. 20 поставщики платежных услуг применяют строгую аутентификацию клиентов, если соблюдается одно из следующих условий:

1) пользователь платежных услуг впервые получает онлайн-доступ к информации, указанной в п. 20, через поставщика услуг по информированию о счетах;

2) прошло более 180 дней с момента последнего доступа пользователя платежных услуг в режиме онлайн к информации, предусмотренной п. 20, через поставщика услуг по информированию о счетах и с момента применения строгой аутентификации клиента.

22. В отступление от п. 20 поставщики платежных услуг должны применять строгую аутентификацию клиентов, если пользователь платежных услуг получает доступ к своему платежному счету онлайн через поставщика услуг по информированию о счетах, и у поставщика платежных услуг есть обоснованные причины, подкрепленные соответствующими доказательствами, связанными с несанкционированным доступом или мошенническим доступом к платежному счету. В таком случае поставщик платежных услуг должным образом документирует и по запросу Национального банка Молдовы обосновывает причины применения строгой аутентификации клиентов.

23. Поставщики платежных услуг, предлагающие услуги по управлению счетом, обеспечивающие определенный интерфейс, как это предусмотрено в п. 75, не обязаны осуществлять отступление, предусмотренное в п. 20, в контексте реализации резервного механизма, предусмотренного в п. 86, если они не применяют отступления, предусмотренные в п. 18 и 19, в прямом интерфейсе, используемом для аутентификации и связи с пользователями их платежных услуг.

Часть 3
БЕСКОНТАКТНЫЕ ПЛАТЕЖИ, ПРОИЗВОДИМЫЕ НА POS-ТЕРМИНАЛАХ

24. Поставщики платежных услуг имеют право не применять строгую аутентификацию клиента при условии соблюдения требований, изложенных в п. 4 и 5, если плательщик инициирует бесконтактную электронную платежную операцию посредством платежного инструмента с бесконтактной функциональностью, в которой индивидуальная стоимость операции электронного бесконтактного платежа не превышает 1000 леев или эквивалента в иностранной валюте, при выполнении одного из следующих условий:

1) совокупная стоимость операций электронных бесконтактных платежей, инициированных плательщиком с даты последнего применения строгой аутентификации клиента, не превышает 3000 леев или эквивалента в иностранной валюте;

2) количество последовательных электронных бесконтактных платежных операций, инициированных с даты последнего применения строгой аутентификации клиента, не превышает пяти.

Часть 4

НЕОБСЛУЖИВАЕМЫЕ ТЕРМИНАЛЫ ДЛЯ БИЛЕТОВ НА ТРАНСПОРТ И ОПЛАТЫ ПАРКОВКИ

25. Поставщики платежных услуг имеют право не применять строгую аутентификацию клиента при условии соблюдения требований, изложенных в п. 4 и 5, если плательщик инициирует операцию электронного платежа на необслуживаемом платежном терминале (автоматический платеж без сопровождения), в целях оплаты проезда на транспорте или парковки.

Часть 5

УПОЛНОМОЧЕННЫЕ БЕНЕФИЦИАРЫ

26. Поставщики платежных услуг применяют строгую аутентификацию клиентов, когда плательщик создает или изменяет список уполномоченных получателей платежей через поставщика платежных услуг, управляющего счетом плательщика.

27. Поставщики платежных услуг имеют право не применять строгую аутентификацию клиентов при условии соблюдения требований, изложенных в п. 4 и 5, если плательщик инициирует платежную операцию и получатель платежа находится в списке уполномоченных получателей, ранее созданном плательщиком.

Часть 6

ПОВТОРЯЮЩИЕСЯ ОПЕРАЦИИ

28. Поставщики платежных услуг применяют строгую аутентификацию клиентов, когда плательщик впервые создает, изменяет или инициирует серию повторяющихся операций на одну и ту же сумму и с одним и тем же получателем платежа.

29. Поставщики платежных услуг имеют право не применять строгую аутентификацию клиентов при условии соблюдения требований, установленных п. 4 и 5, для инициирования всех последующих платежных операций, входящих в серию платежных операций, указанных в п. 28.

Часть 7

КРЕДИТОВЫЙ ПЕРЕВОД МЕЖДУ СЧЕТАМИ ОДНОГО И ТОГО ЖЕ ФИЗИЧЕСКОГО ИЛИ ЮРИДИЧЕСКОГО ЛИЦА

30. Поставщики платежных услуг имеют право не применять строгую аутентификацию клиентов при условии соблюдения требований, изложенных в п. 4 и 5, если инициируется операция кредитового перевода, в которой плательщиком и получателем платежа являются одно и то же физическое или юридическое лицо, и оба платежных счета принадлежат одному и тому же поставщику платежных услуг, который управляет счетом.

Часть 8

ОПЕРАЦИИ С НИЗКОЙ СТОИМОСТЬЮ

31. Поставщики платежных услуг имеют право не применять строгую аутентификацию клиентов при условии соблюдения требований, изложенных в п. 4 и 5, если плательщик инициирует операцию электронного дистанционного платежа на сумму, не превышающую 600 леев, или эквивалента в иностранной валюте, которая соответствует одному из следующих условий:

1) совокупная стоимость предыдущих электронных дистанционных платежных операций, инициированных плательщиком с момента последнего

применения строгой аутентификации, не превышает 2000 леев или эквивалента в иностранной валюте;

2) количество предыдущих электронных дистанционных платежных операций, инициированных плательщиком с момента последнего применения строгой аутентификации клиентов, не превышает 5 таких отдельных последовательных операций.

Часть 9
БЕЗОПАСНЫЕ ПРОЦЕССЫ И ПРОТОКОЛЫ ПЛАТЕЖЕЙ

УТВЕРЖДЕНИЕ ОСВОБОЖДЕНИЯ ОТ ОБЯЗАТЕЛЬСТВА СТРОГОЙ АУТЕНТИФИКАЦИИ КЛИЕНТОВ

32. Поставщики платежных услуг имеют право не применять строгую аутентификацию клиентов при условии соблюдения требований, изложенных в п. 4 и 5, к юридическим лицам, инициирующим электронные платежные операции с использованием определенных платежных процессов или протоколов, которые предоставляются только плательщикам-не потребителям, если Национальный банк Молдовы сочтет, что эти процессы или протоколы гарантируют уровни безопасности, как минимум эквивалентные тем, которые предусмотрены Законом № 114/2012. Чтобы воспользоваться исключением из обязательства применять строгую аутентификацию клиентов, поставщикам платежных услуг, которые предоставляют клиентам определенные платежные процессы или протоколы, используемые исключительно не потребителями, необходимо запросить у Национального банка Молдовы предоставление этого освобождения.

33. Для предоставления освобождения от обязанности применять строгую аутентификацию клиентов, предусмотренную п. 32, Национальный банк Молдовы рассмотрит соблюдение следующих требований:

1) Поставщик платежных услуг имеет систему мониторинга платежных операций, инициируемых посредством определенных платежных процессов или протоколов, которые доступны только плательщикам, не являющимся потребителями;

2) Поставщик платежных услуг имеет безопасную систему связи, соответствующую требованиям настоящего регламента (включая аспекты шифрования данных, конфиденциальности и целостности персонализированных элементов безопасности);

3) Поставщик платежных услуг использует безопасный метод аутентификации клиентов, чтобы снизить риск аутентификации неавторизованного лица.

34. В целях оценки и мониторинга соблюдения поставщиками платежных услуг требований п. 32 и 33 Национальный банк Молдовы будет учитывать уровень мошенничества, зафиксированный соответствующими поставщиками платежных услуг. Уровень мошенничества будет рассчитываться путем сообщения совокупной стоимости удаленных платежных операций, считающихся мошенническими, для которых применялась строгая аутентификация клиентов и платежных операций, выполненных с использованием определенных платежных процессов или протоколов, которые доступны не потребителям, к общей стоимости транзакции удаленных платежей, независимо от того, применялась ли строгая аутентификация клиентов или были ли они выполнены с использованием определенных платежных процессов или протоколов, которые доступны плательщикам, не являющимся потребителями.

Все мошеннические платежные операции будут включены, независимо от того, были ли возвращены средства или нет. Расчет будет осуществляться ежеквартально, а базовым курсом, используемым для конвертации валюты, будет

средний курс обмена Национального банка Молдовы в квартале, для которого рассчитываются уровни мошенничества.

35. Поставщик платежных услуг, желающий получить освобождение от обязанности применять строгую аутентификацию клиентов, должен подать в Национальный банк Молдовы заявление о предоставлении освобождения с приложением следующих документов и информации:

1) Подробный аудиторский отчет, выявляющий соответствие конкретных платежных процессов и протоколов требованиям, установленным в ст. 32^1 и 32^2 Закона №. 114/2012 и п. 4-8, 53-61, 95-100 настоящего регламента и других нормативных актов Национального банка Молдовы в области мер безопасности, связанных с операционными рисками и рисками безопасности, связанными с платежными услугами. Кроме того, поставщик платежных услуг-заявитель должен представить в Национальный банк Молдовы декларацию под собственную ответственность лица, которое проверяло соответствующик платежные процессы или протоколы (в рамках ИТ-системы поставщика платежных услуг или независимо) относительно его операционной независимости в отношении поставщика платежных услуг и сертификаций в области ИТ-безопасности, а также опыта в области платежей;

2) Уровень мошенничества для платежных операций, инициированных посредством определенных платежных процессов и протоколов. Об этом будет сообщаться Национальному банку Молдовы ежеквартально.

36. Заявление о предоставлении освобождения от обязанности строгой аутентификации клиентов, прилагаемые к нему документы и информация подаются в Национальный банк Молдовы на румынском языке в оригинале или заверенных копиях. Если документы и информация составлены на иностранном языке, они должны быть представлены в оригинале или заверенных копиях с приложением авторизированного перевода на румынский язык.

37. Заявление и документы, предусмотренные п. 35, подаются в Национальный банк Молдовы его органом управления/членом или лицом, уполномоченным в соответствии с законодательством (из которых следует, что лицо уполномочено представлять заявителя в отношениях с Национальным банком Молдовы).

38. В течение 30 дней со дня получения полного пакета документов в соответствии с п. 35 Национальный банк Молдовы принимает решение о предоставлении освобождения от обязанности применять строгую аутентификацию клиентов или решает отклонить запрос, информируя поставщика платежных услуг о своем решении. Национальный банк Молдовы может установить, по информации поставщика платежных услуг, более длительный срок выдачи решения, который не превысит 90 дней, в соответствии с положениями Административного кодекса Республики Молдова.

39. Если пакет документов, представленный в Национальный банк Молдовы, не является полным и поставщик платежных услуг не представляет необходимые документы для его заполнения в срок, установленный Национальным банком Молдовы, он информирует поставщика платежных услуг о прекращении административной процедуры по истечении 3 рабочих дней со срока, установленного Национальным банком Молдовы.

40. Если документов или информации, представленных в соответствии с п. 35, недостаточно для принятия решения, Национальный банк Молдовы может запросить дополнительные документы и информацию. Поставщик платежных услуг обязан предоставить дополнительную информацию и документы в срок, указанный Национальным банком Молдовы, период, в течение которого срок, установленный Национальным банком Молдовы в соответствии с п. 38, приостанавливается.

41. Национальный банк отклоняет ходатайство об освобождении от обязанности применять строгую аутентификацию клиентов в случае, если:

a) в результате оценки всех имеющихся документов и информации Национальный банк Молдовы приходит к выводу, что требования, изложенные в п. 32 и 33, не соблюдены; и/или

b) информация и документы, представленные Национальному банку Молдовы, являются ошибочными, недостоверными и/или противоречивыми.

Часть 10
АНАЛИЗ РИСКА ОПЕРАЦИЙ

42. Поставщики платежных услуг имеют право не применять строгую аутентификацию клиентов, если плательщик инициирует операцию удаленного электронного платежа, которая определяется поставщиком платежных услуг как представляющая низкий уровень риска в соответствии с механизмами мониторинга операций, предусмотренными в п. 4-5 и подп. 3) п. 43.

43. Считается, что электронные платежные операции представляют собой низкий уровень риска, если в совокупности выполняются следующие условия:

1) Уровень мошенничества по данному виду операций, сообщенный поставщиком платежных услуг и рассчитанный в соответствии с пунктами 45-47, равен или ниже контрольного уровня мошенничества, указанного в таблице, приведенной в приложении № 1;

2) стоимость операции не превышает соответствующего значения порога освобождения, указанного в таблице приложения № 1;

3) поставщики платежных услуг после анализа рисков в режиме реального времени с помощью механизмов мониторинга операций не выявили ни одного из следующих элементов:

a) необычные расходы или модель поведения плательщика;
b) необычная информация о доступе плательщика к устройству/ программному обеспечению;
c) заражение вредоносными программами в любом сеансе процедуры аутентификации;
d) известные сценарии мошенничества при предоставлении платежных услуг.

44. Оценка, проводимая поставщиком платежных услуг, объединяет все основанные на риске факторы, предусмотренные подп. 3) п. 43, в единую систему оценки риска для каждой отдельной операции, чтобы определить, следует ли разрешить определенный платеж без строгой аутентификации клиентов.

Часть 11
РАСЧЕТ УРОВНЯ МОШЕННИЧЕСТВА

45. Для каждого вида операций, представленных в таблице приложения № 1, поставщик платежных услуг обеспечивает, чтобы общий уровень мошенничества для всех видов платежных операций были эквивалентны или не превышали значений эталонных показателей мошенничества для того же вида платежной операции, указанной в таблице приложения № 1.

46. Общий уровень мошенничества для каждого типа операции рассчитывается ежеквартально как общая сумма несанкционированных или мошеннических дистанционных сделок, независимо от того, возвращены ли средства, разделенная на общую сумму всех удаленных операций одного и того же типа.

47. Методика и модели, используемые поставщиком платежных услуг для расчета уровня мошенничества, а также фактические уровни мошенничества должным образом документируются и полностью предоставляются Национальному банку Молдовы по его запросу.

Часть 12

ПРЕКРАЩЕНИЕ ОТСТУПЛЕНИЙ НА ОСНОВЕ АНАЛИЗА РИСКОВ ОПЕРАЦИЙ

48. Поставщики платежных услуг, которые используют отступление, предусмотренное в п. 42-44, немедленно информируют Национальный банк Молдовы, когда один из наблюдаемых показателей мошенничества для любого типа платежной операции, указанной в таблице в приложении № 1, превышает применимый базовый уровень мошенничества, и предоставляет Национальному банку Молдовы описание мер, которые они намерены принять, чтобы привести наблюдаемый уровень мошенничества в соответствие с применимыми базовыми показателями.

49. Поставщики платежных услуг немедленно прекращают использовать отступление, предусмотренное п. 42-44, для любого типа платежной операции, указанной в таблице приложения № 1 и находящейся в определенном диапазоне порога освобождения, когда наблюдаемый ими уровень мошенничества превышает в течение двух кварталов подряд базовую ставку мошенничества, применимую к соответствующему платежному инструменту или типу платежной операции в соответствующем диапазоне порога отступления.

После прекращения использования отступления, предусмотренного в п. 42–44, поставщики платежных услуг больше не должны использовать это отступление до тех пор, пока уровень мошенничества, рассчитанный за квартал, не станет равным или меньшим, чем базовые уровни мошенничества, применимые для этого типа платежной операции в соответствующем диапазоне порога отступления.

50. Если намереваются снова использовать отступление, предусмотренное в п. 42-44, поставщики платежных услуг информируют Национальный банк Молдовы и перед повторным использованием отступления предоставляют доказательства того, что отслеживаемый ими уровень мошенничества вернулся в соответствие с эталонным уровнем мошенничества, применимым для этого порогового интервала отступления.

Часть 13
МОНИТОРИНГ

51. Чтобы использовать отступления от применения строгой аутентификации клиентов, поставщики платежных услуг должны регистрировать и контролировать данные инфраструктуры для каждого типа платежных операций с разделением как на удаленные, так и на те, которые не осуществляются удаленно, по крайней мере раз в квартал:

1) общая стоимость несанкционированных платежных операций, в том числе мошеннических в соответствии с частью (2) ст. 52 Закона № 114/2012, общая стоимость всех платежных операций и связанный с этим уровень мошенничества, включая разбивку платежных операций, инициированных строгой аутентификацией клиентов, и операций, выполняемых в рамках каждого отступления;

2) средняя стоимость операции, включая разделение платежных операций, инициируемых строгой аутентификацией клиентов, и операций, выполняемых в рамках каждого отступления;

3) количество платежных операций, к которым применялось каждое из отступлений, и их доля по отношению к общему количеству платежных операций.

52. Поставщики платежных услуг представляют результаты мониторинга, проведенного в соответствии с п. 51, Национальному банку Молдовы по его запросу.

ГЛАВА IV
КОНФИДЕНЦИАЛЬНОСТЬ И ЦЕЛОСТНОСТЬ ПЕРСОНАЛИЗИРОВАННЫХ ЭЛЕМЕНТОВ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЕЙ ПЛАТЕЖНЫХ УСЛУГ

53. Поставщики платежных услуг обеспечивают конфиденциальность и целостность персонализированных элементов безопасности пользователей платежных услуг, включая коды аутентификации, на всех этапах аутентификации путем реализации как минимум следующих требований:

1) персонализированные элементы безопасности маскируются при вводе пользователем платежных услуг во время аутентификации;

2) специальные элементы защиты в формате данных и криптографические материалы, связанных с шифрованием персонализированных элементов защиты, не хранятся в виде обычного текста;

3) секретные криптографические материалы защищены от несанкционированного раскрытия;

4) персонализированные элементы безопасности создаются в безопасной среде. Они реализуют меры по снижению рисков несанкционированного использования персонализированных элементов безопасности, устройств или ИТ-приложений, используемых для аутентификации;

5) обработка и передача персонализированных элементов безопасности и кодов аутентификации, сгенерированных в соответствии с главой II, происходят в безопасных средах, в соответствии с профессиональными стандартами в области и которые широко признаны;

6) передача персонализированных элементов защиты и устройств аутентификации и программного обеспечения пользователю платежных услуг осуществляется в безопасных условиях, направленных на борьбу с рисками, связанными с их несанкционированным использованием после их утраты, кражи или копирования. В этом отношении поставщики платежных услуг должны реализовать, как минимальное требование, каждую из следующих мер:

a) эффективные и безопасные механизмы передачи, которые гарантируют, что персонализированные элементы безопасности, устройства и программное обеспечение аутентификации передаются законному пользователю платежных услуг;

b) механизмы, позволяющие поставщику платежных услуг проверять подлинность программного обеспечения аутентификации, передаваемого пользователю платежных услуг через интернет;

c) меры, гарантирующие, что если передача персонализированных элементов безопасности осуществляется за пределами помещений поставщика платежных услуг или по удаленному каналу:

– ни одна несанкционированная сторона не может получить более одного компонента персонализированных элементов безопасности, устройств или программного обеспечения аутентификации, когда они передаются по одному и тому же каналу;

– персонализированные элементы защиты или передаваемые устройства, или программное обеспечение аутентификации должны быть активированы перед использованием;

d) меры, гарантирующие, что в случае, если персонализированные элементы безопасности, устройства или программное обеспечение аутентификации должны быть активированы перед первым использованием, активация происходит в безопасной среде в соответствии с процедурами ассоциации, предусмотренными в пункте 55.

54. Поставщики платежных услуг должны полностью документировать процесс, связанный с управлением криптографическими материалами, используемыми для шифрования или сокрытия персонализированных элементов безопасности.

55. Поставщики платежных услуг обеспечивают в безопасных условиях, чтобы только пользователь платежных услуг был связан с настроенными элементами безопасности, устройствами и программным обеспечением аутентификации. С

этой целью поставщики платежных услуг должны обеспечить выполнение каждого из следующих требований:

1) связь личности пользователя платежных услуг с персонализированными элементами безопасности, устройствами и программным обеспечением аутентификации осуществляется в защищенной среде под контролем поставщика платежных услуг; Это распространяется как минимум на помещение поставщика платежных услуг, интернет-среду, предоставляемую поставщиком платежных услуг, или другие аналогичные защищенные веб-сайты, используемые поставщиком платежных услуг, а также услуги банкоматов этого поставщика. Также будут приняты во внимание риски, связанные с устройствами и их компонентами, которые используются в процессе подключения и не находятся под контролем поставщика платежных услуг;

2) соединение по удаленному каналу личности пользователя платежных услуг с персонализированными средствами безопасности и устройствами или программным обеспечением аутентификации осуществляется с использованием строгой аутентификации клиентов.

56. Поставщики платежных услуг обеспечивают, чтобы обновление или повторная активация персонализированных элементов безопасности соответствовала процедурам создания, подключения и передачи элементов безопасности и устройств аутентификации в соответствии с п. 53-55.

57. Поставщики платежных услуг должны обеспечить наличие эффективных процедур для применения каждой из следующих мер безопасности:

1) безопасное уничтожение, деактивация или изъятие персонализированных средств безопасности, устройств и программного обеспечения аутентификации;

2) если поставщик платежных услуг распространяет устройства и программное обеспечение аутентификации для повторного использования, безопасное повторное использование устройства или программного обеспечения должно быть установлено, документировано и реализовано до их предоставления другому пользователю платежных услуг;

3) деактивация или удаление информации, связанной с персонализированными мерами безопасности, хранящейся в системах и базах данных поставщика платежных услуг и, если применимо, в публичных реестрах.

ГЛАВА V
ОТКРЫТЫЙ, ОБЩИЙ И БЕЗОПАСНЫЙ СТАНДАРТ СВЯЗИ
Часть 1
ОБЩИЕ ТРЕБОВАНИЯ К СВЯЗИ

58. Поставщики платежных услуг обеспечивают создание условий безопасной идентификации для связи между устройством плательщика и устройствами получателя платежа, принимающими электронные платежи, включая, помимо прочего, платежные терминалы.

59. Поставщики платежных услуг должны обеспечить эффективное снижение рисков, связанных с неверным направлением сообщения неавторизованным лицам в случае мобильных приложений и других интерфейсов пользователей платежных услуг, предоставляющих услуги электронных платежей.

60. Поставщики платежных услуг устанавливают процедуры, обеспечивающие, чтобы все платежные операции и другие взаимодействия, осуществляемые в контексте предоставления платежных услуг, с пользователем платежных услуг, с другими поставщиками платежных услуг и с другими субъектами, включая торговцев, могли отслеживаться, обеспечивая получение последующей информации обо всех событиях, имеющих отношение к электронной операции на любом этапе.

61. Для целей пункта 60 поставщики платежных услуг обеспечивают, чтобы любой сеанс связи, осуществляемый с пользователем платежных услуг, с другими

поставщиками платежных услуг и с другими субъектами, включая торговцев, основывался на каждом из следующих элементов:

1) единый идентификатор сессии;

2) механизмы безопасности для подробной записи операции, включая номер операции, временные метки и все соответствующие данные операции;

3) временные метки, основанные на единой системе времени и синхронизированные в соответствии с официальным сигналом времени.

Часть 2
ОСОБЫЕ ТРЕБОВАНИЯ К ОТКРЫТОМУ, ОБЩЕМУ И БЕЗОПАСНОМУ СТАНДАРТУ СВЯЗИ

Подчасть 1
ОБЩИЕ ОБЯЗАННОСТИ ПО ИНТЕРФЕЙСАМ ДОСТУПА

62. Поставщики платежных услуг, которые предоставляют услуги по управлению счетом и которые предоставляют плательщику доступный онлайн платежный счет, должны иметь, как минимум, один интерфейс, отвечающий каждому из следующих требований:

1) поставщики услуг по информированию о счетах, поставщики услуг по инициированию платежей и поставщики платежных услуг, выпускающие платежные инструменты на основе карт, должны иметь возможность идентифицировать себя поставщику платежных услуг, предлагающему услуги по управлению счетом;

2) поставщики услуг по информированию о счетах должны иметь возможность безопасного взаимодействия для запроса и получения информации об одном или нескольких платежных счетах, назначенных пользователем, и связанных с ними платежных операциях;

3) поставщики услуг инициирования платежа должны иметь возможность безопасного взаимодействия для инициирования платежного поручения с платежного счета плательщика и получения всей информации, касающейся инициирования платежной операции, а также всей информации, доступной поставщикам платежных услуг, предлагающих услуги по управлению счетом относительно выполнения платежной операции.

63. В целях аутентификации пользователя платежной услуги интерфейс, предусмотренный в п. 62, должен позволять поставщикам услуг по информировании о счетах и поставщикам услуг по инициированию платежей полагаться на все процедуры аутентификации, предоставляемые поставщиком платежных услуг, который предлагает услуги по управлению счетом пользователю платежных услуг.

64. Интерфейс отвечает, как минимум следующим требованиям:

1) поставщик услуг инициирования платежа или поставщик услуг по информированию о счетах должен иметь возможность потребовать от поставщика платежных услуг, предоставляющего услуги по управлению счетом, инициировать аутентификацию на основании согласия пользователя платежной услуги, предоставленного поставщику услуг инициирования платежа или услуг по информированию о счете;

2) сеансы связи между поставщиком платежных услуг, предоставляющим услуги по управлению счетом, поставщиком услуг по информированию о счетах, поставщиком услуг инициирования платежей и любым пользователем соответствующих платежных услуг должны быть установлены и поддерживаться на протяжении всего периода аутентификации;

3) целостность и конфиденциальность персонализированных элементов безопасности и кодов аутентификации, передаваемых поставщиком услуг

инициирования платежа или через него, или поставщиком услуг по информированию о счетах, должны гарантироваться всеми поставщиками платежных услуг.

65. Поставщики платежных услуг, предлагающие услуги по управлению счетом, гарантируют, что их интерфейсы соответствуют стандарту открытой, общей и безопасной связи, выпущенному международными или европейскими организациями по стандартизации, как это установлено в функциональных и технических требованиях, выпущенных Национальным банком Молдовы.

66. Поставщики платежных услуг, предоставляющие услуги по управлению счетом, также должны гарантировать, что технические спецификации любого интерфейса, разработанного в соответствии с открытым, общим и безопасным стандартом связи, документируются с информацией, определяющей рутинные процессы, протоколы и инструменты, необходимые поставщикам услуг по инициированию платежей, поставщикам услуг по информированию о счетах и поставщикам платежных услуг, которые выпускают платежные инструменты на основе карт, чтобы обеспечить совместимость их программного обеспечения и приложений с системами поставщиков платежных услуг, которые предлагают услуги по управлению счетом.

67. Поставщики платежных услуг, предлагающие услуги по управлению счетом, бесплатно предоставляют документацию по запросу лицензированных поставщиков услуг по инициированию платежей, лицензированных поставщиков услуг по информированию о счетах и поставщиков платежных услуг, которые выпускают лицензированные платежные инструменты на основе карт или поставщиков платежных услуг, подавших заявление в Национальный банк Молдовы на получение соответствующей лицензии и опубликовавшие краткое изложение документации, общедоступной на их веб-сайте.

68. Кроме требований, изложенных в пунктах 65-67, поставщики платежных услуг, предлагающие услуги по управлению счетом, обеспечивают, чтобы, за исключением чрезвычайных ситуаций, любые изменения, внесенные в технические характеристики их интерфейса, были доступны лицензированным поставщикам услуг по инициированию платежа, лицензированным поставщикам услуг по информированию о счетах и лицензированным поставщикам платежных услуг, выпускающим платежные инструменты на основе карт, или поставщикам платежных услуг, подавших заявление в Национальный банк Молдовы на получение соответствующей лицензии как можно раньше, но не менее чем за 3 месяца до внесения изменений.

69. Поставщики платежных услуг документируют чрезвычайные ситуации, в которых были внесены изменения, и по запросу представляют документацию Национальному банку Молдовы.

70. В отступление от п. 68 и 69 поставщики платежных услуг, предлагающие услуги по управлению счетом, представляют поставщикам платежных услуг изменения, внесенные в технические характеристики их интерфейсов для соответствия п. 20-23, не позднее, чем за 2 месяца до вступления в силу данных изменений.

71. Поставщики платежных услуг, предоставляющие услуги по управлению счетом, должны предоставить тестовую платформу, включая соответствующую поддержку, для подключения и функционального тестирования, чтобы предоставить лицензированным поставщикам услуг по инициированию платежей, лицензированных поставщикам услуг по информированию о счетах и лицензированным поставщикам платежных услуг, выпускающим платежные инструменты на основе карт, или поставщикам платежных услуг, подавших заявление в Национальный банк Молдовы на получение соответствующей лицензии на тестирование программного обеспечения и приложений, используемых для предоставления платежных услуг пользователям.

72. Тестовая платформа, предусмотренная п. 71, должна быть предоставлена не позднее, чем за три месяца до даты, запланированной для вывода на рынок интерфейса доступа. Однако через платформу тестирования не предоставляется конфиденциальная информация.

73. Национальный банк Молдовы обеспечивает, чтобы поставщики платежных услуг, предлагающие услуги по управлению счетом, всегда соблюдали обязательства, включенные в открытый, общий и безопасный стандарт связи, в отношении интерфейса(ов), который(ые) они установили.

74. Если поставщик платежных услуг, предлагающий услуги по управлению счетом, не соблюдает требования к интерфейсам, предусмотренным стандартом связи, Национальный банк Молдовы обеспечивает, чтобы предоставление услуг по инициированию платежей и услуг по информированию о счетах не было затруднено или нарушено в той степени, в которой соответствующие поставщики таких услуг соблюдают условия, установленные в п. 87 и 88.

Подчасть 2
ОПЦИИ ОТНОСИТЕЛЬНО ИНТЕРФЕЙСОВ ДОСТУПА

75. Поставщики платежных услуг, оказывающие услуги по управлению счетом, устанавливают интерфейс (интерфейсы), предусмотренный (предусмотренные) в п. 62-74 через специальный интерфейс или предоставляют поставщикам платежных услуг, предусмотренных п. 62, право использовать интерфейсы, используемые для аутентификации и связи с пользователями платежных услуг поставщика платежных услуг, предлагающего услуги по управлению счетом.

Подчасть 3
ОБЯЗАТЕЛЬСТВА ПО СПЕЦИАЛЬНОМУ ИНТЕРФЕЙСУ

76. При условии соблюдения п. 62–75 поставщики платежных услуг, предоставляющие услуги по управлению счетом и установившие специальный интерфейс, обеспечивают, чтобы этот интерфейс всегда обеспечивал тот же уровень доступности и производительности, включая поддержку, что и интерфейсы, предоставленные пользователю платежных услуг для прямого доступа к его счету онлайн-платежей.

77. Поставщики платежных услуг, которые предоставляют услуги по управлению счетом и установили специальный интерфейс, должны определить ключевые показатели эффективности и прозрачные цели уровня услуг, которые, по крайней мере, столь же строги, как и для интерфейса, используемого их пользователями платежных услуг, как с точки зрения доступности, так и с точки зрения предоставляемых данных в соответствии с п. 101-106. Указанные интерфейсы, показатели и цели контролируются Национальным банком Молдовы и подвергаются стресс-тестированию со стороны поставщиков платежных услуг, предлагающих услуги по управлению счетом.

78. Поставщики платежных услуг, предоставляющие услуги по управлению счетом и установившие специальный интерфейс, должны обеспечить, чтобы этот интерфейс не создавал препятствий для предоставления услуг по инициированию платежей и услуг по информированию о счетах.

79. К препятствиям, предусмотренным в п. 78, относятся, среди прочего, предотвращение использования поставщиками платежных услуг, предусмотренных в п. 62, элементов безопасности, выданных поставщиками платежных услуг, которые предлагают своим клиентам услуги по управлению счетом, введение перенаправления службе аутентификации поставщика платежных услуг, который предлагает услуги по управлению счетом, или другим его функциям, запрос дополнительных разрешений и регистраций, помимо предусмотренных в Части 1 главы III Закона № 114/2012, или запрос дополнительных

проверок согласия пользователей платежных услуг поставщикам услуг инициирования платежей и услуг по информированию о счетах.

80. Для целей п 76 и 77 поставщики платежных услуг, предлагающие услуги по управлению счетом, контролируют доступность и производительность специального интерфейса.

81. Поставщики платежных услуг, предоставляющие услуги по управлению счетом, обязаны ежеквартально публиковать на своем веб-сайте статистику о наличии и работоспособности специального интерфейса и интерфейса, используемого пользователями их платежных услуг.

Подчасть 4

РЕЗЕРВНЫЙ МЕХАНИЗМ ДЛЯ СПЕЦИАЛЬНОГО ИНТЕРФЕЙСА

82. Поставщики платежных услуг, предоставляющие услуги по управлению счетом, при разработке специального интерфейса должны предусмотреть стратегию и планы резервных механизмов на случай, если специальный интерфейс не работает в соответствии с п. 76-81 или сталкивается с непредвиденной недоступностью или в случае, если система перестает работать.

83. Незапланированной недоступностью или сбоем в работе систем считается произошедшее, если на пять последовательных запросов на доступ к информации для оказания услуг по инициированию платежей или для предоставления информации о счете не получен ответ в течение 30 секунд.

84. Меры на случай непредвиденных обстоятельств включают в себя планы связи, позволяющие поставщикам платежных услуг использовать специальный интерфейс с информацией о мерах по восстановлению системы и описанием немедленно доступных альтернативных вариантов, которыми в это время располагают поставщики платежных услуг.

85. Как поставщик платежных услуг, предлагающий услуги по управлению счетом, так и поставщики платежных услуг, предусмотренные в п. 62, должны незамедлительно направить в Национальный банк Молдовы отчеты о проблемах со специальными интерфейсами, описанными в п. 82, 83.

86. В рамках резервного механизма поставщики платежных услуг, предусмотренные п. 62, имеют право использовать до тех пор, пока конкретный интерфейс не вернется к уровню доступности и производительности, предусмотренному п. 76-81, интерфейсы, предоставленные пользователям платежных услуг для аутентификации и связи со своим поставщиком платежных услуг, который предоставляет услуги по управлению счетом.

87. С этой целью поставщики платежных услуг, предлагающие услуги по управлению счетом, обеспечивают возможность идентификации поставщиков платежных услуг, предусмотренных в п. 62, и могут полагаться на процедуры аутентификации, предоставляемые поставщиком платежных услуг, который предлагает услуги по управлению счетом для пользователей платежных услуг.

88. Поставщики платежных услуг, предусмотренные п. 86, в случае использования интерфейса, предусмотренного п. 62:

1) принимают необходимые меры для обеспечения того, чтобы они не получали доступ, не хранили и не обрабатывали данные для целей, отличных от предоставления услуги, запрошенной пользователем платежных услуг;

2) продолжают соблюдать обязательства, вытекающие из части (3) ст. 52^2 части (2) ст. 52^3 Закона № 114/2012;

3) регистрируют данные, доступ к которым осуществляется через интерфейс поставщика платежных услуг, который предлагает услуги по управлению счетом пользователям своих платежных услуг, и предоставляет записанные данные Национальному банку Молдовы по запросу и без неоправданного опоздания;

4) должным образом обосновывают Национальному банку Молдовы, по запросу и без неоправданного опоздания, использование интерфейса,

предоставленного пользователям платежных услуг, с целью прямого доступа к их счету онлайн-платежей;

5) информируют об этом поставщика платежных услуг, предлагающего услуги по управлению счетом.

89. Поставщики платежных услуг, предлагающие услуги по управлению счетом и выбравшие специальный интерфейс, освобождаются Национальным банком Молдовы в соответствии с главой VI от обязательства по установлению резервного механизма, описанного в п. 86, в случае, если специальный интерфейс отвечает всем следующим условиям:

1) соблюдает все обязательства по специальным интерфейсам, предусмотренным п. 76-81;

2) был спроектирован и тестирован в соответствии с п. **Error! Reference source not found.** и **Error! Reference source not found.** таким образом, который поставщик платежных услуг, предусмотренный настоящей статьей, считает удовлетворительным.

3) широко использовался в течение не менее трех месяцев поставщиками платежных услуг для предоставления услуг по информировании о счете и услуг по инициированию платежей, а также для подтверждения наличия средств для платежей, связанных с картой;

4) любая проблема, связанная с конкретным интерфейсом, решалась без неоправданного опоздания.

90. Национальный банк Молдовы отменяет исключение, предусмотренное пунктом 89, если условия подп. 1) и 4) п. 89 не соблюдаются поставщиками платежных услуг, предлагающими услуги по управлению счетом в течение более двух календарных недель подряд. Национальный банк Молдовы информирует поставщика платежных услуг, предлагающего услуги по управлению счетом, об отзыве. Таким образом, Национальный банк Молдовы обеспечивает, чтобы поставщик платежных услуг, предлагающий услуги по управлению счетом, в кратчайшие сроки, максимум в течение двух месяцев, установил резервный механизм, предусмотренный п. 86.

Подчасть 5
СЕРТИФИКАТЫ

91. Для целей идентификации, предусмотренной подп. 1) п. 62, поставщики платежных услуг полагаются на квалифицированные сертификаты для электронных печатей или для аутентификации веб-страниц, как это определено в Законе об электронной идентификации и доверительных услугах № 124/2022.

92. Для целей настоящего регламента регистрационный номер, указанный в официальных реестрах, предусмотренный Законом об электронной идентификации и доверительных услугах № 124/2022, является номером разрешения поставщиков платежных услуг, выпускающих платежные инструменты, связанные с картой, поставщиков услуг по информированию о счетах и поставщиков услуг по инициированию платежей, в том числе поставщиков платежных услуг, предоставляющих услуги по управлению счетом и таких услуг, номер которых доступен в публичном реестре в соответствии со ст. 23 Закона №. 114/2012 или в результате разрешений, выданных в соответствии с Законом о деятельности банков № 202/2017.

93. Для целей настоящего регламента квалифицированные сертификаты для электронных печатей или для аутентификации веб-сайтов, предусмотренные в п. 91, включают на языке, обычно используемом в сфере международных финансов, дополнительные конкретные атрибуты в отношении каждого из следующих элементов:

1) роль поставщика платежных услуг, которая может быть одной или несколькими из следующих:

a) оказание услуг по управлению счетом;
b) оказание услуг по инициированию платежа;
c) оказание услуг по информированию о счетах;
d) выпуск платежных инструментов, связанных с картой;

2) наименование компетентных органов, в которых зарегистрирован поставщик платежных услуг, соответственно Национальный банк Молдовы.

94. Атрибуты, предусмотренные в п. 93, не влияют на совместимость и признание квалифицированных сертификатов для электронных печатей или для аутентификации интернет-сайтов.

Подчасть 6
БЕЗОПАСНОСТЬ СЕАНСОВ СВЯЗИ

95. Поставщики платежных услуг, предоставляющие услуги по управлению счетом, поставщики платежных услуг, выпускающие платежные инструменты на основе карт, поставщики услуг по информированию о счетах и поставщики услуг по инициированию платежей должны гарантировать, что при обмене данными через интернет между взаимодействующими сторонами применяются процессы безопасного шифрования на протяжении всего сеанса связи для защиты конфиденциальности и целостности данных с использованием надежных и широко признанных методов шифрования.

96. Поставщики платежных услуг, выпускающие платежные инструменты на основе карт, поставщики услуг по информированию о счетах и поставщики услуг по инициированию платежей должны поддерживать как можно более короткую продолжительность сеансов, в которых предоставляется доступ и которые предоставляются поставщиками платежных услуг, предоставляющими услуги по управлению счетом, и активно прекращать такие сеансы, как только запрошенное действие будет завершено.

97. При поддержании параллельных сетевых сеансов с поставщиком платежных услуг, предоставляющим услуги по управлению счетом, поставщики услуг по информированию о счетах и поставщики услуг по инициированию платежей должны обеспечить, чтобы эти сеансы были надежно связаны с соответствующими сеансами, установленными с пользователем (пользователями) платежных услуг, во избежание риска передачи любого сообщения или информации, передаваемой между ними, не в тот пункт назначения.

98. Поставщики услуг по информированию о счетах, поставщики услуг по инициированию платежей и поставщики платежных услуг, которые выпускают платежные инструменты на основе карт, вместе с поставщиком платежных услуг, который предоставляет услуги по управлению счетом, указывают четкие ссылки на каждый из следующих элементов:

1) пользователя или пользователей платежных услуг и соответствующие сеансы связи с целью различения нескольких запросов от одного и того же пользователя (пользователей) платежных услуг;

2) для услуг по инициированию платежа - однозначно идентифицируемая инициированная платежная операция;

3) для подтверждения наличия денежных средств – однозначно идентифицируемый запрос суммы, необходимой для выполнения платежной операции по карте.

99. Поставщики платежных услуг, предоставляющие услуги по управлению счетом, поставщики услуг по информированию о счетах, поставщики услуг по инициированию платежей и поставщики платежных услуг, выпускающие платежные инструменты на основе карт, должны гарантировать, что, если они передают специальные элементы безопасности и коды аутентификации, они не могут быть прочитаны напрямую или косвенно, любым сотрудником в любое время.

100. В случае утраты конфиденциальности персонализированных элементов безопасности, когда они находятся в сфере их компетенции, заинтересованные поставщики должны незамедлительно проинформировать пользователя соответствующих платежных услуг и эмитента персонализированных элементов безопасности.

101. Поставщики платежных услуг, предлагающие услуги по управлению счетом, должны соблюдать каждое из следующих требований:

1) они предоставляют поставщикам услуг по информированию о счетах ту же информацию о платежных счетах, назначенных пользователем, и связанных с ними платежных операциях, которая доступна пользователю платежных услуг, когда он запрашивает прямой доступ к информации о счете, при условии, что такая информация не включает конфиденциальные платежные данные;

2) они предоставляют поставщикам услуг по инициированию платежа сразу же после получения платежного поручения ту же информацию об инициировании и выполнении платежной операции, которая была представлена или предоставлена пользователю платежных услуг, если операция инициируется непосредственно последним;

3) они немедленно информируют по запросу поставщиков платежных услуг посредством подтверждения в простом формате «да» или «нет», имеется ли на платежном счете плательщика сумма, необходимая для выполнения платежной операции.

102. В случае непредвиденного события или ошибки, возникшей в процессе идентификации или аутентификации, или при обмене информацией, поставщик платежных услуг, предлагающий услуги по управлению счетом, отправляет поставщику услуг уведомляющее сообщение, инициирующее платеж или поставщику услуг по информированию о счетах и поставщику платежных услуг, выпускающему платежные инструменты на основе карт, с объяснением причины возникновения непредвиденного события или ошибки.

103. Если поставщик платежных услуг, предоставляющий услуги по управлению счетом, предоставляет специальный интерфейс в соответствии с п. 76-81, интерфейс делает доступными уведомительные сообщения, связанные с непредвиденными событиями или ошибками, которые должны быть сообщены любым поставщиком платежных услуг, обнаружившим событие или ошибку остальным поставщикам платежных услуг, участвующим в сеансе связи.

104. Поставщики услуг по информированию о счетах должны иметь адекватные и эффективные механизмы для предотвращения доступа к информации, отличной от информации, полученной от платежных счетов, назначенных пользователем, и связанных с ними платежных операций, в соответствии с явным согласием пользователя.

105. Поставщики услуг по инициированию платежей обязаны предоставлять поставщикам платежных услуг, предоставляющим услуги по управлению счетом, ту же информацию, которую запрашивает пользователь платежных услуг при непосредственном инициировании платежной операции.

106. Поставщики услуг по информированию о счетах должны иметь возможность доступа к информации с назначенных пользователем платежных счетов и связанных с ними платежных операций, проводимых поставщиками платежных услуг, предлагающими услуги по управлению счетом, для выполнения услуги по информированию о счетах в любом из следующих обстоятельств:

1) всякий раз, когда пользователь платежных услуг активно запрашивает такую информацию;

2) если пользователь платежных услуг активно не запрашивает такую информацию, не более четырех раз в течение 24 часов, за исключением случаев, когда поставщик услуг по информированию о счетах и поставщик платежных

услуг, предоставляющий услуги по управлению счетом, не договорились о более высокой частоте с согласия пользователя платежных услуг.

ГЛАВА VI
УТВЕРЖДЕНИЕ ОСВОБОЖДЕНИЯ ОТ ОБЯЗАТЕЛЬСТВА УЧРЕЖДЕНИЯ РЕЗЕРВНОГО МЕХАНИЗМА, ПРЕДУСМОТРЕННОГО В ПУНКТЕ 82.

107. Эта глава применяется к поставщикам платежных услуг, которые предоставляют услуги по управлению платежными счетами, доступными онлайн, и предоставляют специальный интерфейс, который позволяет сторонним поставщикам платежных услуг получать доступ к платежным счетам.

108. В этой главе установлены требования, которым должны соответствовать поставщики платежных услуг, предлагающие услуги по управлению платежными счетами, доступные онлайн, чтобы воспользоваться освобождением от обязательства по установлению резервного механизма в соответствии с условиями п. 89.

109. Для предоставления освобождения от обязанности учреждения резервного механизма, предусмотренного п. 82, Национальный банк Молдовы оценит выполнение поставщиком платежных услуг условий, предусмотренных п. 89, требований, указанных в приложении № 3 настоящего регламента и положений Закона № 114/2012.

110. Поставщик платежных услуг, намеревающийся получить освобождение от обязанности учреждения резервного механизма, предусмотренного п. 82, должен подать в Национальный банк Молдовы заявление о предоставлении освобождения в соответствии с приложением № 2 к настоящему регламенту, с приложением следующих документов и сведений:

1) информацию и документы, подтверждающие выполнение требований, изложенных в Приложении № 3, и подтверждение одобрения заявления органом управления или высшим руководством поставщика платежных услуг, в зависимости от обстоятельств;

2) информацию и документы, подтверждающие выполнение условий п.**Error! Reference source not found.** настоящего регламента.

111. Поставщик платежных услуг подает запрос согласно п. 110 по каждому специальному предоставленному интерфейсу, для которого предусмотрено освобождение от обязательства по учреждению резервного механизма.

112. Если поставщик платежных услуг считает, что одно из требований, изложенных в Приложении № 3, к нему не применимо, он должен указать в документации, направляемой в Национальный банк Молдовы, обоснование того, почему указанное требование к нему не применимо.

113. Заявления о предоставлении освобождения от обязанности учреждения резервного механизма, предусмотренного п. 82, прилагаемые к ним документы и информация подаются в Национальный банк Молдовы на румынском языке в оригинале или заверенных копиях. Если документы и сведения составлены на иностранном языке, они представляются в оригинале или заверенных копиях с приложением авторизированного перевода на румынский язык.

114. Документы, предусмотренные п. 110, представляются в Национальный банк Молдовы органом управления/ его членом или лицом, уполномоченным в соответствии с законодательством (из чего видно, что лицо уполномочено представлять заявителя в отношениях с Национальным банком Молдовы).

115. В течение 30 дней со дня получения полного пакета документов в соответствии с п. 110 Национальный банк Молдовы принимает решение о предоставлении освобождения от обязанности учреждения резервного механизма, предусмотренного п. 82, или принимает решение об отказе заявления, информируя поставщика платежных услуг о своем решении. Национальный банк Молдовы может установить, с информацией поставщика платежных услуг, более

длительный срок выдачи решения, который не будет превышать 90 дней, в соответствии с положениями Административного кодекса Республики Молдова.

116. Если пакет документов, представленный в Национальный банк Молдовы, не является полным и поставщик платежных услуг не представляет необходимые документы для его заполнения в срок, установленный Национальным банком Молдовы, Национальный банк Молдовы информирует об этом поставщика платежных услуг о прекращении административной процедуры – по истечении 3 рабочих дней со дня, установленного Национальным банком Молдовы.

117. Если документов или информации, представленных в соответствии с п. 110, недостаточны для принятия решения, Национальный банк Молдовы может запросить дополнительные документы и информацию. Поставщик платежных услуг обязан предоставить дополнительную информацию и документы в срок, указанный Национальным банком Молдовы, период, в течение которого срок, установленный Национальным банком Молдовы в соответствии с пунктом 115, приостанавливается.

118. Национальный банк отклоняет ходатайство об освобождении от обязанности учреждения резервного механизма, предусмотренного п. 82, в следующих случаях:

a) в результате оценки всех имеющихся документов и информации Национальный банк Молдовы приходит к выводу, что условия, изложенные в п. 89, не соблюдены и/или требования, изложенные в приложении № 3 не выполняются; и/или

b) представление Национальному банку Молдовы ошибочной, недостоверной и/или противоречивой информации и документов;

119. После утверждения освобождения от обязательства по учреждению резервного механизма, предусмотренного п. 82, Национальный банк Молдовы может в любое время запросить у поставщика платежных услуг любую другую соответствующую информацию, данные и документы для оценки постоянного соблюдения требований настоящего нормативного акта.

Приложение № 1 к Регламенту о строгой аутентификации клиентов и открытом, общем и безопасном стандарте связи между поставщиками платежных услуг

	Процентные ставки мошенничества (%) для:	
ETV (пороговое значение отступления)	**Дистанционные электронные платежи на основе карты**	**Удаленные электронные кредитовые переводы**
10 000 леев или эквивалент в иностранной валюте	0,01	0,005
5 000 леев или эквивалент в иностранной валюте	0,06	0,01
2 000 леев или эквивалент в иностранной валюте	0,13	0,015

Приложение № 2 к Регламенту о строгой аутентификации клиентов и открытом, общем и безопасном стандарте связи между поставщиками платежных услуг

Заявление на предоставление освобождения от обязанности учреждения срочного механизма согласно п. Error! Reference source not found.

Нижеподписавшийся, ...(фамилия и имя), в качестве . . . . . ., прошу освободить от учреждения срочного механизма согласно п. **Error! Reference source not found.** регламента . . . . . (название поставщика платежных услуг, который предлагает услуги по управлению платежными счетами, доступными онлайн), с местонахождением. . . . . .., ул. . . . . ., №. . . . . , почтовый индекс. . . . . ., зарегистрированный в. . . . . ., единый идентификационный код . . . . . для специального интерфейса . . . . . (наименование специального интерфейса, используемого запрашивающим поставщиком платежных услуг).

Специальный интерфейс:

- ☐ разработан внутри
- ☐ разработан в рамках финансово-банковской группы, к которой принадлежит запрашивающий поставщик платежных услуг
- ☐ разработан в сотрудничестве со сторонним банком
- ☐ разработан в сотрудничестве с небанковской третьей стороной

☐ приобретен у . . . . . (название производителя интерфейса), с местонахождением. . . . ., ул. . . . . ., №. . . . ., почтовый индекс. . . . . .., зарегистрированный в. . . . . ., единый идентификационный код . . . . . .

Программное обеспечение, предназначенное для специального интерфейса, запускается по адресу. . . . . .

Запрашивающий поставщик платежных услуг является/не является аффилированным лицом или членом финансовой/банковской группы.

Специальный интерфейс используется/будет использоваться следующими поставщиками платежных услуг:

1. . . . . ., с идентификационным кодом . . . . . ., в стране. . . . ., под маркой . . . . . .
2. . . . . ., с идентификационным кодом. . . . . ., в стране. . . . ., под маркой. . . . .
n. . . . . ., с идентификационным кодом. . . . . ., в стране. .. . ., под маркой. . . . . . .

К запросу прилагаются следующие документы:

1. . . . . .
2.
...
n. . . . . .

Контактные лица, которые могут предоставить разъяснения по данному запросу:

1. Фамилия и имя . . . . . .
Телефон: . . . . . Эл. адрес: . . . .
2. Фамилия и имя. . . . . .
Телефон: . . . . . Эл. адрес: . . . .

Предоставленные данные и информация являются достоверными, правильными и отражают существующую ситуацию (вплоть до) даты . . . ./ . . . ./ . . . . .

Подпись

Приложение № 3 к Регламенту о строгой аутентификации клиентов и открытом, общем и безопасном стандарте связи между поставщиками платежных услуг

Требования к предоставлению освобождения от обязанности учреждения резервного механизма

1. Заявитель должен определить ключевые показатели эффективности и цели уровня обслуживания, в том числе для разрешения проблем, помощи в нерабочее время, мониторинга, планов действий в чрезвычайных ситуациях и обслуживания

специального интерфейса, которые должны быть, по крайней мере, такими же строгими, как и для интерфейса или интерфейсов, доступных для пользователей своих платежных услуг для прямого онлайн-доступа к своим платежным счетам.

2. Заявитель должен определить, как минимум следующие ключевые показатели эффективности в отношении доступности специального интерфейса:

1) ежедневная продолжительность доступности каждого интерфейса и

2) ежедневная продолжительность недоступности каждого интерфейса.

3. Помимо ключевых показателей, предусмотренных пунктом 2 настоящего приложения, заявитель должен определить, как минимум следующие ключевые показатели эффективности, касающиеся эффективности специального интерфейса:

1) средняя дневная продолжительность (выраженная в миллисекундах) одного запроса, необходимая для того, чтобы заявитель предоставил поставщику услуг инициирования платежа всю информацию, запрошенную в соответствии с п. b) части (4) ст.52^2 Закона № 114/2012 и подп. 2) п.101 настоящего регламента;

2) средняя дневная продолжительность (выраженная в миллисекундах) одного запроса, необходимая для того, чтобы заявитель предоставил поставщику услуг по информированию о счетах всю информацию, запрошенную в соответствии с подп. 2) п.101 настоящего регламента;

3) средняя дневная продолжительность (выраженная в миллисекундах) одного запроса, необходимая для того, чтобы заявитель предоставил эмитенту платежных инструментов на основе карты или поставщику услуг по инициированию платежа подтверждение «да» или «нет» в соответствии с частью (3) ст. 52^1 Закона № 114/2012 и подп. 3) п.101 настоящего регламента;

4) ежедневная доля неправильных ответов.

4. Для расчета показателей наличия специального интерфейса, предусмотренного п. 2) настоящего приложения, заявителю необходимо:

1) рассчитать время доступности, выраженное в процентах, как 100% минус процент времени недоступности;

2) рассчитать время недоступности, выраженное в процентах, используя общее количество секунд, в течение которых специальный интерфейс был недоступен в течение 24-часового периода, начинающегося и заканчивающегося в полночь;

3) считать интерфейс недоступным, если пять последовательных запросов на доступ к информации для оказания услуг по инициированию платежей, услуг по информированию о счетах или подтверждению наличия средств не получили ответа в течение суммарного интервала 30 секунд, независимо от того, исходят ли такие запросы от одного или нескольких поставщиков услуг по инициированию платежей, поставщиков услуг по информированию о счетах или поставщиков платежных услуг, которые выпускают платежные инструменты на основе карт. В этом случае запрашивающая сторона исчисляет время недоступности с момента поступления первого запроса в серии из пяти последовательных запросов, на который не был дан ответ в течение 30 секунд, при условии, что что среди пяти запросов, на которые был отправлен ответ, нет ни одного успешно решенного запроса.

5. В соответствии с п. 80 и 81 регламента заявитель должен предоставить Национальному банку Молдовы план ежеквартальной публикации ежедневной статистики о наличии и работе специального интерфейса, согласно положениям п.2 и 3. настоящего приложения, а также каждого из интерфейсов, предоставляемых пользователям их платежных услуг для прямого доступа к их платежным счетам в режиме онлайн, а также информацию о месте публикации этой статистики и дате первой публикации.

6. Публикация статистических данных, предусмотренных п. 5 настоящего приложения, должна позволять поставщикам услуг по инициированию платежей, поставщикам услуг по информированию о счетах, поставщикам платежных услуг,

выпускающим платежные инструменты на основе карт, пользователям платежных услуг и компетентным органам сравнивать доступность и ежедневную производительность каждого специального интерфейса, предоставленного поставщиком платежных услуг, запрашивающего исключение, с доступностью и производительностью каждого из интерфейсов, предоставленных его собственным пользователям платежных услуг тем же поставщиком платежных услуг для прямого онлайн-доступа к платежным счетам.

7. Для проведения тестов на устойчивость, предусмотренных п. 77 настоящего регламента, заявитель должен иметь процессы для установления и оценки того, как ведет себя специальный интерфейс, когда он подвергается чрезвычайно большому количеству запросов от поставщиков услуг инициирования платежей, поставщиков услуг по информированию о счетах и поставщиков платежных услуг, которые выпускают платежные инструменты на основе карт, с точки зрения влияния этих перегрузок на доступность и производительность специального интерфейса, а также на определенные цели в отношении уровня услуг.

8. Заявитель должен провести соответствующие стресс-тесты специального интерфейса, включая, помимо прочего:

1) возможность предоставления доступа нескольким поставщикам услуг по инициированию платежей, поставщикам услуг по информированию о счетах и поставщикам платежных услуг, выпускающим платежные инструменты на основе карт;

2) способность обрабатывать чрезвычайно большое количество запросов от поставщиков услуг по инициированию платежей, поставщиков услуг по информированию о счетах и поставщиков платежных услуг, выпускающих платежные инструменты на основе карт, в короткий период времени без сбоев и/или неисправностей;

3) использование чрезвычайно большого количества одновременно открытых сессий для запросов на инициирование платежей, информирование о счете и подтверждение наличия средств; и

4) запросы больших объемов данных.

9. Заявитель должен предоставить Национальному банку Молдовы сводку всех результатов проведенных стресс-тестов, включая сценарии, использованные в качестве основы для тестирования каждого из элементов, указанных в п. 8 настоящего приложения, и то, как были решены все выявленные проблемы.

10. Заявитель должен предоставить Национальному банку Молдовы:

1) краткое описание метода или методов применения процедуры или процедур строгой аутентификации пользователей платежных услуг, поддерживаемых специальным интерфейсом, а именно «перенаправление», «разъединение», «встраивание» или их комбинация; и

2) ясное, подробное и полное объяснение мотивации, по которой способ или способы применения процедуры или процедур аутентификации, предусмотренных подп. 1), не представляют собой препятствия, предусмотренные п. 78 и 79 настоящего регламента, и о том, как эти методы позволяют поставщикам услуг по инициированию платежей и поставщикам услуг по информированию о счетах полагаться на все процедуры аутентификации, предоставляемые их собственным пользователям платежных услуг поставщиком платежных услуг, запрашивающим исключение, вместе с доказательствами того, что специальный интерфейс не вызывает ненужных опозданий или неудобств для пользователей платежных услуг, когда они получают доступ к своему счету через поставщика услуг инициирования платежей, поставщика услуг по информированию о счетах или поставщика платежных услуг, который выпускает платежные инструменты на основе карт, а также любые другие неудобства, включая прохождение ненужных шагов или использование неясных или сдерживающих формулировок, которые могут прямо или косвенно отпугивать пользователей платежных услуг от

использования услуг поставщиков услуг по инициированию платежей, поставщиков услуг по информированию о счетах и поставщиков платежных услуг, которые выпускают платежные инструменты на основе карт.

11. В рамках разъяснения, предусмотренного подп. 2) п. 10 настоящего приложения, заявитель должен предоставить Национальному банку Молдовы подтверждение того, что:

1) специальный интерфейс не препятствует поставщикам услуг по инициированию платежей и поставщикам услуг по информированию о счетах полагаться на процедуру или процедуры аутентификации, предоставленную или предоставленные заявителем своим собственным пользователям платежных услуг;

2) от поставщиков услуг по инициированию платежей, поставщиков услуг по информированию о счетах и поставщиков платежных услуг, выпускающих платежные инструменты на основе карт, не требуется никакого дополнительного лицензирования или регистрации, кроме тех, которые предусмотрены Частью 1 Главы III Закона № 114/2012;

3) дополнительные проверки, предусмотренные п. 78 и 79 регламента, заявителем не проводятся по согласию пользователя платежных услуг, данному поставщику услуг инициирования платежа или поставщику услуг по информированию о счетах для доступа к информации о платежных счетах, открытых у заявителя, или инициировать платежи с платежных счетов, открытых у заявителя, и

4) не осуществляется ни одна проверка согласия пользователя платежных услуг, данного поставщику платежных услуг, выпускающему платежные инструменты на основе карт, в соответствии с п. a) части (2) ст. 52^1 Закона № 114/2012.

12. Для подтверждения соответствия требованию, установленному подп. 2) п. 89 настоящего регламента, относительно дизайна специального интерфейса, заявитель должен предоставить Национальному банку Молдовы:

1) доказательство того, что специальный интерфейс соответствует правовым требованиям относительно доступа и данных, предусмотренным Законом № 114/2012 и настоящим регламентом, в том числе:

a) описание функциональных и технических характеристик, реализованных поставщиком платежных услуг; и

b) краткое изложение того, насколько реализация этих спецификаций соответствует требованиям Закона № 114/2012 и настоящего регламента;

2) информацию о том, взаимодействовал ли и в какой форме поставщик платежных услуг, запрашивающий исключение, с поставщиками услуг инициирования платежей, поставщиками услуг по информированию о счетах и поставщиками платежных услуг, выпускающими платежные инструменты на основе карт.

13. Если заявитель реализует стандарт, разработанный в рамках рыночной инициативы:

1) сведения, предусмотренные п. a) подп. 1) п. 12 настоящего приложения могут состоять из информации о стандарте рыночной инициативы, примененном заявителем, независимо от того, отклонился ли он в каком-либо конкретном аспекте от такого стандарта, и если да, то каким образом он отклонился и как он соответствует требования Закона № 114/2012 и настоящего регламента;

2) сведения, предусмотренные п. b) подп. 1) п. 12 настоящего приложения могут включать, если таковые имеются, результаты испытаний на соответствие, разработанных рыночной инициативой, результаты, удостоверяющие соответствие специального интерфейса соответствующему стандарту рыночной инициативы.

14. Для выполнения требования, установленного подп. 2) п. 89 настоящего регламента, о тестировании специального интерфейса, заявитель должен

предоставить технические характеристики специального интерфейса авторизированным поставщикам услуг по инициированию платежей, поставщикам услуг по информированию о счетах и поставщикам платежных услуг, которые выпускают авторизованные платежные инструменты на основе карт, или субъектам, подавшим в Национальный банк Молдовы заявление на получение соответствующего разрешения в соответствии с п. 65-67 настоящего регламента, которые должны включать, как минимум, публикацию краткого изложения технических характеристик специального интерфейса на собственном сайте в соответствии с п. 65-66 настоящего регламента.

15. Тестовая платформа должна позволять авторизованным поставщикам платежных услуг, предоставляющим услуги по управлению счетом, поставщикам услуг по инициированию платежей, поставщикам услуг по информированию о счетах и поставщикам платежных услуг, выпускающим платежные инструменты на основе карты, а также лицам, подавшим заявление в Национальный банк Молдовы о соответствующем разрешении на тестирование специального интерфейса в выделенной, безопасной тестовой среде и с использованием вымышленных данных пользователей платежных услуг для следующих целей:

1) стабильное и безопасное соединение;

2) способность заявителя и поставщиков услуг по инициированию платежей, поставщиков услуг по информированию о счетах и поставщиков платежных услуг, выпускающих платежные инструменты на основе карт, уполномоченных обменивать соответствующие сертификаты, в соответствии с п. 91-94 настоящего регламента;

3) возможность отправки и получения сообщений об ошибках, согласно п. 102 и 103 настоящего регламента;

4) способность поставщиков услуг по инициированию платежа отправлять, а заявителя получать поручения на инициирование платежа, а также способность заявителя предоставлять запрошенную информацию в соответствии с п. b) части (4) статьи 52^2 Закона № 114/2012 и с подп. 2) п. 101 настоящего регламента;

5) способность поставщиков услуг по информированию о счетах отправлять, а заявителя получать запросы на доступ к данным платежного счета, а также способность заявителя предоставлять информацию, запрошенную в соответствии с подп. 1) п. 101 настоящего регламента;

6) способность поставщиков платежных услуг, выпускающих платежные инструменты на основе карточек, и поставщиков услуг инициирования платежей передавать, а заявителя получать запросы от поставщиков платежных услуг, выпускающих платежные инструменты на основе карточек, и поставщиков услуг инициирования платежей, а также возможность заявителя направлять подтверждение «да» или «нет» поставщикам платежных услуг, выпускающим платежные инструменты на основе карточек, и поставщикам услуг по инициированию платежей в соответствии с подп. 3) п. 101 настоящего регламента, и

7) способность поставщиков услуг по инициированию платежей и поставщиков услуг по информированию о счетах полагаться на процедуры аутентификации, предоставляемые заявителем своим собственным пользователям платежных услуг.

16. Заявитель должен предоставить Национальному банку Молдовы сводку результатов испытаний, предусмотренных п. 71 и 72 настоящего регламента, для каждого из элементов, подлежащих испытанию в соответствии с п. 15 настоящего приложения, включая количество поставщиков услуг, поставщиков услуг по инициированию платежей, поставщиков услуг по информированию о счетах и поставщиков платежных услуг, выпускающих платежные инструменты на основе карт, которые использовали тестовую платформу, ответ, полученный заявителем от этих поставщиков услуг по инициированию платежей, поставщиков услуг по

информированию о счетах и поставщиков платежных услуг, выпускающих платежные инструменты на основе карт, выявленные проблемы и описание способов их решения.

17. Для подтверждения соответствия требованию подп. 3) п. 89 настоящего регламента заявитель должен предоставить Национальному банку Молдовы:

1) описание использования конкретного интерфейса на период, предусмотренный подп. 3) п. 89 настоящего регламента, включая, но не ограничиваясь:

a) количество поставщиков услуг по инициированию платежей, поставщиков услуг по информированию о счетах и поставщиков платежных услуг, выпускающих платежные инструменты на основе карт, которые использовали интерфейс для предоставления услуг клиентам; и

b) количество запросов, отправленных этими поставщиками услуг по инициированию платежей, поставщиками услуг по информированию о счетах и поставщиками платежных услуг, выпускающими платежные инструменты на основе карточек, заявителю, через специальный интерфейс, на которые получен ответ от заявителя;

2) доказательства того, что заявитель предпринял все разумные усилия для обеспечения широкого использования специального интерфейса, в том числе путем сообщения о доступности специального интерфейса по соответствующим каналам, и, если применимо, на веб-сайте заявителя, платформах социальных сетей, через профессиональные отраслевые организации, на конференциях и посредством прямого участия известных игроков рынка.

18. Трехмесячный срок, предусмотренный в подп. 3) п. 76 может течь параллельно с тестированием, указанным в п.58.

19. В целях п. **Error! Reference source not found.** и подп. 4) п. **Error! Reference source not found.** настоящего регламента заявитель должен представить Национальному банку Молдовы:

1) информацию о существующих системах или процедурах отслеживания, решения и закрытия проблем, в частности о тех, о которых сообщают поставщики услуг инициирования платежей, поставщики услуг по информированию о счетах и поставщики платежных услуг, которые выпускают платежные инструменты на основе карты; и

2) анализ проблем и недостатков, в частности, о которых сообщили поставщики услуг по инициированию платежей, поставщики услуг по информированию о счетах и поставщики платежных услуг, которые выпускают платежные инструменты на основе карты, которые не были решены в соответствии с целями относительно уровня услуг, установленных в п. 1 настоящего приложения.