ГЛАВА 1.

ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Предмет рассмотрения

Закон устанавливает технические требования к организаторам платежей для обеспечения безопасности, что обеспечивает:

a. выполнение процедур строгой аутентификации пользователей в соответствии со статьей 97 директивы Европейского Союза 2015/2366 (PSD2).

b. исключение применения процедур строгой аутентификации пользователей, в случаях, которые определяются уровнем риска проводимых операций, суммой перевода, используемым каналом управления счетом, повторяемостью платежей.

c. защиту целостности и конфиденциальности учетных данных плательщика

d. общие правила информационного обмена между участниками платежей (в терминах PSD2)

Статья 2. Основные требования к аутентификации

Организаторы платежей должны использовать механизмы анализа транзакционного риска для обнаружения неавторизованных или мошеннических транзакций для реализации положений (a) и (b) статьи 1.

Механизмы оценки транзакционного риска должны базироваться на анализе платежных транзакций, типичных для пользователя при условии нормального использования персональных учетных данных клиента.
Организаторы платежей должны гарантировать, что механизм оценки транзакционных рисков, как минимум, учитывает каждый из нижеперечисленных факторов:

a. Список скомпрометированных или утерянных аутентификационных элементов
b. Сумму каждой платежной транзакции

c. Известные сценарии мошенничества для данного типа платежных услуг

d. Признаки наличия вредоносного программного обеспечения на любом из этапов аутентификационного процесса

e. В том случае, если устройство доступа к платежам или соответствующее программное обеспечение предоставлено организатором платежей, с учетом журнала доступа к устройству доступа к платежам или программному обеспечению – например, для карточных платежей в POS терминалах

Статья 3. Контроль за мерами безопасности.

Выполнение мер безопасности, описанных в статье 1, должно быть документировано, должно проходить через процедуры периодических проверок и аудитов в соответствии с внутренними требованиями организатора платежей. Аудит должен выполняться организацией, имеющей компетенции в информационных технологиях, организации платежей и операционно-независимой от организатора платежей

Период между процедурами аудита, описанными в параграфе 1 данной статьи, должен определяться внутренними документами организатора платежей по бухгалтерскому учету и аудиту.

В том случае, если организатор платежей использует механизм исключения процедур строгой аутентификации в соответствии со статьей 17, то он обязан проводить аудит методологии и заявленных уровней потерь как минимум, на ежегодной основе. Аудит должен выполняться организацией, имеющей компетенции в информационных технологиях, организации платежей и в операционном смысле независимой от организатора платежей. В первый год применения механизмов исключения в соответствии со статьей 17, и не менее 3 лет после первого года, или более часто, по соответствующему запросу регулятора, аудит должен проводиться внешней компанией.

Проводимый аудит должен оценить соответствие требованиям организатора платежей данному стандарту и выдать соответствующее заключение.

Полный текст аудиторского отчета должен быть предоставлен по требованию регулятора.

Глава II
МЕРЫ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СТРОГОЙ АУТЕНТИФИКАЦИИ

Глава 4. Аутентификационный код

1.В тех случаях, когда организатор платежей применяет строгую аутентификацию пользователей (в соответствии с статьей 97 (1) Директивы Евросоюза 2015/2366), аутентификация должна базироваться на двух или более аутентификационных факторах, определяемых как:

- знание
- владение
- биометрия

и должно приводить к созданию аутентификационного кода.

Аутентификационный код является одноразовым и используется в процессе онлайн доступа к счету пользователя, для инициирования платежной транзакции или выполнения любого другого действия, которое может создать риск мошенничества при использовании канала дистанционного управления счетом.

2. В целях реализации параграфа 1 организатор платежей должен использовать меры безопасности с обязательным выполнением нижеперечисленных требований:

a) из факта раскрытия аутентификационного кода нельзя извлечь информацию об упомянутых в параграфе 1 факторах

b) нельзя вычислить новый аутентификационный код, основываясь на известном значении использованного ранее аутентификационного кода

c) аутентификационный код не может быть подделан.

3. Организаторы платежей должны гарантировать, что при использовании аутентификационного кода выполняются все нижеперечисленные условия:

(a) если при аутентификации в процессе удаленного доступа к счету, платежа с использованием удаленного доступа к счету или другой операции, которая может привести к риску мошеннических действий не удалось сгенерировать правильный аутентификационный код, то должна отсутствовать практическая возможность выявить, какой из аутентификационных факторов, описанных в данном параграфе, был неверно использован;

(b) количество неудачных попыток аутентификации, имевших место один за другим, не должно превышать 5 за заданный период времени. После превышения вышеуказанного лимита аутентификационные процедуры, описанные в статье 97(1) PSD2, блокируются временно или на постоянной основе.

(c) коммуникационные сессии защищены от захвата аутентификационных данных в процессе аутентификации и исключают манипуляции с аутентификационными данными неавторизованной третьей стороной в соответствии с требованиями главы V.

(d) Максимальный период от момента аутентификации плательщика при онлайн доступе к счету до проведения им операций не должен превышать 5 минут.

4. В том случае, если блокировка системы аутентификации, упомянутая в параграфе 3(b) является временной, время блокировки и количество попыток должно базироваться на типе услуг, предоставляемых плательщику и связанных с типом услуг рисками с учетом, как минимум факторов, упомянутых в статье 2(3).

При постоянной блокировке пользователь должен быть заблаговременно уведомлен.

В случае постоянной блокировки, должен быть предусмотрен безопасный механизм, позволяющий пользователю повторно получить доступ к управлению счетом.

Статья 5. Динамическая связь.

1. В тех случаях, когда организатор платежей применяет строгую аутентификацию пользователей (в соответствии с статьей 97 (1) Директивы Евросоюза 2015/2366), в дополнение к требованиям статьи 4 данного документа, также необходимо использование мер безопасности, соответствующие следующим требованиям:

(a) плательщик должен быть проинформирован о сумме и получателе платежа*;*

(b) сгенерированный аутентификационный код является специфичным для суммы платежа и указанного плательщиком получателя платежа;

(c) полученный организатором платежей аутентификационный код соответствует сумме платежа и указанного плательщиком получателя платежа;

(d) любое изменение суммы или получателя платежа приводит к нарушению валидности аутентификационного кода.

2. В целях соответствия параграфу 1, организатор платежа должен использовать меры безопасности, обеспечивающее конфиденциальность, аутентичность и целостность всего нижеперечисленного:

(a) суммы транзакции и получателя платежа в течение всех фаз аутентификации;

(b) информации, которая демонстрируется плательщику в течение всех фаз аутентификации, включая генерацию, передачу и использование аутентификационного кода.

3. В целях соответствия параграфу 1(b), когда организатор платежей применяет строгую аутентификацию пользователей (в соответствии с статьей 97 (1) Директивы Евросоюза 2015/2366), должны применяться следующие меры безопасности для аутентификационного кода:
(a) по отношению к транзакциям с использованием платежных карт, по отношению к которым плательщик подтвердил согласие на точное значение средств, блокируемых в соответствии со статьей 75(1) директивы PSD2, аутентификационный код должен соответствовать сумме блокировки в момент инициации;

(b) в случае платежных транзакций, если плательщик решил провести несколько платежей в удаленном режиме одному или нескольким получателям денежных средств, код подтверждения должен соответствовать общей сумме платежей и специфицированным получателям.

Статья 6. Требования к аутентификационному фактору «Знание»

1. Организатор платежей должен использовать меры, способные защитить от компрометации аутентификационный фактор «Знание» со стороны третьих лиц.

2. Использование данного аутентификационного фактора плательщиком должно быть также защищено от компрометации третьей стороной.

Статья 7. Требования к аутентификационному фактору «Владение»

1. Организатор платежей должен принять меры, исключающие возможность использования аутентификационного фактора «Владение» за счет исключения доступа к ним неавторизованных участников

2. Использование аутентификационного фактора «Владение» на стороне плательщика должно предусматривать меры, исключающие создание копий данного фактора.

Статья 8 Требования к устройствам и программному обеспечению, связанному с биометрическим аутентификационным фактором.

1. Организатор платежей должен принять меры, исключающие риски, связанные с тем, что биометрический аутентификационный фактор, который считывается устройством доступа и соответствующим программным обеспечением для доступа к системе платежей, защищены от вмешательства третьих лиц. Как минимум, организатор платежей должен обеспечить очень низкую вероятность того, что постороннее лицо будет признано за законного владельца счета.

2. Использование данного фактора для аутентификации пользователя должно сопровождаться мерами, гарантирующими, что биометрический фактор не будет скомпрометирован третьими лицами за счет подключения к устройству доступа или его программному обеспечению.

Статья 9. Независимость аутентификационных факторов

1.Организатор платежей должен обеспечить применение аутентификационных факторов, используемых для строгой аутентификации клиентов, описанных в статьях 6,7 и 8 таким образом, чтобы в пределах использованных технологий, алгоритмов и параметров, раскрытие одного из аутентификационных факторов не приводит к компрометации других факторов.

2. Организатор платежей должен предпринять меры безопасности, которые исключают компрометацию аутентификационных факторов, используемых для строгой аутентификации пользователя или самого аутентификационного кода, который может возникнуть при компрометации устройств, совмещающих функции инициирования и подтверждения транзакций.

3. Для выполнения требований параграфа 2, меры по защите аутентификационных факторов должны включать все нижеперечисленные:

(a) использование раздельных сред безопасного исполнения программ для устройств, которые используются как для инициации, так и для подтверждения транзакции в рамках программного обеспечения, установленного на устройство

(b) наличие механизмов, обеспечивающих невозможность изменения программного обеспечения, установленного на устройство или самого устройства как пользователем, так и третьими лицами;

(c) наличие механизмов, исключающих последствия вмешательства, в том случае, если оно имело место.

ГЛАВА III
ИСКЛЮЧЕНИЯ ИЗ МЕТОДОВ СТРОГОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ

Статья 10. Информация о платежном счете

1. Организаторам платежей разрешается отказаться от использования строгой аутентификации пользователя, в соответствии с требованиями нижеизложенного в статье 2 и параграфе 2 данной статьи, в том случае, если речь идет исключительно о предоставлении пользователю онлайн информации о счете или других, нижеперечисленных услугах без раскрытия чувствительных данных:

   (a) баланс одного или более платежных счетов;

   (b) информация о проведенных в течение последних 90 дней транзакциях по одному или более счетам.

2. Применение параграфа 1 на стороне организатора платежей с исключением процедур строгой аутентификации пользователя невозможно, если имеет место хотя бы одно из нижеперечисленных условий:

   (a) пользователь пользуется услугой, описанной в параграфе 1 впервые;

   (b)с момента последнего использования онлайн доступа к услугам со стороны пользователя в соответствии с параграфом 1(b) прошло более 90 дней и строгая аутентификация имела место.

Статья 11. Безконтактные платежи в POS терминалах

Организатор платежей может исключить процедуры строгой аутентификации пользователя, в соответствие с требованиями, изложенными в статье 2, если плательщик инициирует бесконтактный электронный платеж с учетом выполнения следующих условий:

(a) сумма транзакции не превышает 50 Евро; и

(b) сумма предшествующих бесконтактных платежных транзакций, инициированных платежным средством с бесконтакным функционалом, от момента последнего применения методов строгой аутентификации, не превышает 150 Евро; или

(c) количество последовательных бесконтактных транзакций, инициированных платежным средством с бесконтакным функционалом, с момента последнего применения методов строгой аутентификации, не превышает пяти.

Статья 12. Оплата транспорта и парковок

Организаторы платежей могут исключить использование методов строгой аутентификации, в соответствие с требованиями, изложенными в статье 2, если плательщик инициирует электронный платеж в необслуживаемом терминале в целях оплаты проезда в транспорте или оплаты парковки.

Статья 13 Доверенные получатели

1. Организатор платежей должен обеспечить выполнение строгой аутентификации пользователя в случае создания или редактирования списка доверенных бенефициаров.
2. Организатор платежей имеет право отказаться от использования строгой аутентификации пользователя, в том случае, если плательщик инициирует транзакцию в пользу получателя платежа из списка доверенных бенефициаров, который был ранее создан плательщиком.

Статья 14. Повторяющиеся транзакции

1. Организатор платежей должен обеспечить выполнение строгой аутентификации пользователя в случае создания, редактирования или инициирования списка повторных транзакций с одинаковой суммой и получателем.

2. Организатор платежей имеет право отказаться от использования строгой аутентификации пользователя, в том случае, если плательщик инициирует любую последующую транзакцию, включенную в ранее подтвержденный список в соответствие с параграфом 1.

Статья 15. Переводы средств между счетами физического или юридического лица

Организатор платежей имеет право отказаться от использования строгой аутентификации пользователя, в том случае если счета получателя и плательщика принадлежат одному и тому же юридическому или физическому лицу и находятся в одной и той же финансовой организации.

Статья 16. Транзакции на малые суммы

Организатор платежей имеет право отказаться от использования строгой аутентификации пользователя, в том случае если плательщик инициирует транзакцию по каналу дистанционного управления счетом и выполняются следующие условия:

(a) сумма платежа не превышает 30 Евро; и

(b) суммарное значение предшествующих транзакций по каналам дистанционного обслуживания без применения строгой аутентификации не превышает 100 Евро; или

(c) число предшествующих транзакций по каналу дистанционного обслуживания, которые провел плательщик с момента последнего применения механизмов строгой аутентификации, не превосходит 5 следующих друг за другом платежей с использованием канала дистанционного управления счетом.

Статья 17. Анализ риска транзакций

1. Организатор платежей имеет право отказаться от использования строгой аутентификации пользователя, в том случае если плательщик инициирует транзакцию по каналу дистанционного обслуживания, которую организатор платежей определяет как несущую малый риск в соответствии с системой анализа транзакционных рисков, описанной в статье 2 и параграфе 2(d) данной статьи.

2. Электронная транзакция, описанная в параграфе 1, будет считаться малорисковой, если выполняются все нижеперечисленные условия:

(a) уровень мошенничества для данного типа транзакций, заявленный организатором платежей и вычисленный в соответствии со статьей 18, равен или ниже референсных значений для уровня мошенничества, приведенного в Приложении для «удаленных операций с использованием платежных карт» или «электронных транзакций с использование дистанционных каналов» соответственно; или

(b) Уровень мошенничества для канала дистанционного управления счетом, в котором выделенные платежные механизмы и протоколы недоступны для розничных потребителей, равен или ниже 0,005% в соответствии с таблицей, приведенной в Приложении для данного типа транзакций; и

(c) сумма транзакции не превосходит соответствующий лимит, который приведен в таблице Приложения, за исключением платежей, соответствующих параграфу 2(b), для которых значение лимита отсутствует;

(d) организатор платежей в результате проверки в режиме реального времени не обнаружил ни одного из нижеперечисленных признаков:

(i) ненормального поведения или платежных привычек на стороне пользователя;
(ii) необычной информации в используемом плательщиком устройстве доступа/программном обеспечении;
(iii) признаков вредоносного программного обеспечения на любом этапе аутентификации;
(iv) признаков известных схем мошенничества;
(v) ненормального местоположения плательщика;
(vi) нахождения плательщика в зоне высокого риска

3.Организатор платежей, намеревающийся использовать механизмы отключения системы строгой аутентификации на основании оценки рисков транзакций, должны, как минимум, учитывать следующие факторы:

(a) предшествующий профиль расходов индивидуального плательщика;

(b) историю платежей пользователя с каждым организатором платежей;

(c) местоположение плательщика и получателя в момент совершения транзакции в тех случаях, когда устройство доступа и соответствующее программное обеспечение предоставляется организатором платежей;

(d) идентификацию факта отклонения характера проводимых платежей от нормального в рамках истории платежей;

Оценка риска организатором платежей должна сочетать все оцениваемые факторы риска и осуществлять скоринг риска для всех проводимых транзакций.

Статья 20. Мониторинг

1.Для того, чтобы использовать исключения из системы строгой аутентификации, которые описаны в статьях 10-17, организатор платежей должен вести записи и производить мониторинг следующих данных для каждого типа транзакций с разбиением на транзакции в дистанционном режиме и недистанционном режиме, как минимум ежеквартально:

(a) общего объема неавторизованных и мошеннических транзакций в соответствии со статьей 64 (2) директивы PSD2, общего объема платежных транзакций и результирующий уровень мошенничества, включая разбиение платежных транзакций, прошедших механизм строгой аутентификации и исключенные из строгой аутентификации по каждому из критериев отдельно;

(b) среднюю сумму транзакции, включая разбиение платежных транзакций, прошедших механизм строгой аутентификации и исключенные из строгой аутентификации по каждому из критериев отдельно;

(c) количество платежных транзакций, которые не проходили через систему строгой аутентификации с разбиениями по типу исключения и их процент в общем количестве платежных

2. Организаторы платежей должны, в соответствие с параграфом 1, предоставлять результаты мониторинга регулятору и EBA по их запросу, с предварительным уведомлением.

ГЛАВА IV
КОНФИДЕНЦИАЛЬНОСТЬ И ЦЕЛОСТНОСТЬ УЧЕТНЫХ ДАННЫХ ПЛАТЕЛЬЩИКОВ

Статья 21. Общие требования

1. Организатор платежей должен обеспечить конфиденциальность и целостность персональных учетных данных плательщика, включая аутентификационный код, в течение всех этапов аутентификации.

2. Для реализации требования в параграфе 1, организатор платежей должен обеспечить выполнение всех нижеперечисленных требований:

(a) закрытые персонализированные учетные данные плательщика маскируются и не отображаются полностью при вводе пользователем в процессе аутентификации;

(b) закрытые персонализированные учетные данные плательщика, как и криптографические средства, используемые для защиты учетных данных, не хранятся в открытом виде;

(c) Используемые криптографические материалы защищены от неавторизованного раскрытия.

3. Организатор платежей должен полностью задокументировать процессы, связанные с использованием криптографических материалов, которые используются в целях обеспечения невозможности получения закрытых персонализированных учетных данных плательщика в открытом виде.

4. Организатор платежей должен гарантировать, что обработка и маршрутизация закрытых персонализированных учетных данных плательщика и аутентификационных кодов, сгенерированных в соответствие требованием главы 2 происходит в защищенном окружении в соответствии с устоявшимися и признанными промышленными стандартами.

Статья 22. Создание и передача учетных данных

Организатор платежей должен обеспечить создание персонализированных учетных данных в безопасном окружении.
Организатор платежей должен исключить риски неавторизованного использования закрытых персонализированных учетных данных плательщика, аутентификационных устройств и программного обеспечения вследствие утери, воровства или копирования до момента получениях их плательщиком

.

Статья 23 Привязка к плательщику

1. Организатор платежей должен обеспечить надежную и безопасную привязку закрытых персонализированных учетных данных плательщика, аутентификационных устройств и программного обеспечения к плательщику.

2. Для выполнения параграфа 1б организатор платежей должен обеспечить выполнение всех нижеперечисленных условий:

(a) привязка закрытых персонализированных учетных данных плательщика, аутентификационных устройств и программного обеспечения происходит в безопасном окружении под ответственностью организатора платежей и включает как офисы организатора платежей, так и его защищенные web-сайты, и банкоматы. При этом организатор платежей должен принимать в учет риски, связанные с устройствами и их компонентами, которые не находятся под контролем организатора платежей.

(b) подобная привязка, в том случае, если она осуществляется по удаленному каналу доступа, должна выполняться с использованием механизма строгой аутентификации пользователя.

Статья 24 Доставка учетных данных, Аутентификационных устройств и программного обеспечения

1. Организаторы платежей должны обеспечить предоставление персонализированных учетных данных плательщика, аутентификационных устройств и программного обеспечения безопасным способом, исключающим риски их неавторизованного использования в результате утери, похищения и копирования.

2. Для выполнения требования параграфа 1, организатор платежей обязан, как минимум, обеспечить выполнение следующих мер:

(a) созданы эффективные и безопасные механизмы доставки, гарантирующие, что учетные данные плательщика, аутентификационные устройств и программное обеспечение будут получены законным плательщиком

(b) используются механизмы, позволяющие убедиться в аутентичности доставленного клиенту по каналу Интернет программного обеспечения;

(c) приняты меры, обеспечивающие, в том случае, когда доставка учетных данных плательщика проводится вне офисов организатора платежей или по каналу удаленного взаимодействия:

(i) неавторизованные лица не могут получить доступ более чем к одному компоненту учетных данных плательщика, аутентификационным устройствам и программному обеспечению в случае их доставки по одному и тому же каналу;
(ii) доставленные персонализированные учетные данные, аутентификационные устройства и программное обеспечение требуют активации до начала использования;
(d) принимаются меры, что в том случае, если персонализированные учетные данные, аутентификационные устройства и программное обеспечение требуют активации до начала использования, то их активация происходит в безопасном окружении в соответствии с требованиями статьи 23.

Статья 25. Восстановление персонализированных учетных данных

Организаторы платежей должны обеспечить соответствие процедур возобновления и реактивации персонализированных учетных данных процедурам для создания привязки и доставки персонализированных учетных данных, устройств аутентификации и программного обеспечения в соответствие со статьями 22-24.

Статья 26 Уничтожение, деактивация и отзыв

Организаторы платежей должны обеспечить наличие эффективных процессов для обеспечения безопасности:

(a) при безопасном уничтожении, деактивации и отзыве персонализированных учетных данных, устройств аутентификации и программного обеспечения;

(b) в том случае, если организатор платежей распределяет повторно используемые средства аутентификации и программное обеспечение, механизмы безопасности для повторного использования должны быть разработаны, приведены в действие и

документированы до предоставления устройств аутентификации и программного обеспечения новому плательщику.

(c) при деактивации или отзыве информации, относящейся к персонализированным учетным данным, из баз данных организатора платежей или из публичных репозиториев, в том случае, если это имеет место.

Приложение

Таблица 1

Допустимые уровни потерь при проведении операций в соответствии с RTS SCA*

Пороговые значения для сумм	Платежи с использованием карт по удаленным каналам (card-not-present)	Денежные переводы
500 €	0,01%	0,005%
250 €	0,06%	0,01%
100 €	0,13%	0,015%