



**Проект Руководства по Рекомендации 16 для
проведения консультаций***



АВГУСТ 2026



Ассоциация участников рынка электронных денег и денежных переводов «АЭД» - отраслевая ассоциация, созданная в 2010 году.

Ассоциация является широко признанным центром компетенции по платежам, специализированному финансовому регулированию, повышению доступности финансовых услуг и финансовым инновациям как в России, так и за рубежом. Основные задачи АЭД – устойчивое развитие отрасли, распространение лучших деловых практик и оказание экспертной поддержки для государственных органов и частного сектора.

Сайт Ассоциации: www.npaed.ru,

Электронная почта: npaed@npaed.ru

Телеграмм-канал «Записки на рукавах» - здесь мы обсуждаем новации в платежном секторе и регулировании, рассуждаем о будущем платежей, финтехе и криптовалюте.

Будем рады видеть новых подписчиков!



* неофициальный перевод

©2026 Ассоциация «АЭД». Все права защищены.

Перевод: Анна Леонова

Воспроизведение без указания на источник запрещено. Распространяется по лицензии CC BY-NC-ND 4.0

Фото на титульной странице: сгенерировано ИИ

[*Draft Recommendation 16 Guidance for consultation*](#)

24 June 2026

The Financial Action Task Force (FATF)

Содержание

Сокращения и аббревиатуры	5
1.1 Резюме.....	7
1.2 Правовой статус Руководства.....	10
Глава 2. Введение	10
2.1 Цель Рекомендации 16	10
2.2 Предпосылки последних изменений Рекомендации 16 - эволюция платежной экосистемы	12
2.3 Деятельность ФАТФ по повышению прозрачности платежей в рамках Дорожной карты «Группы двадцати»	13
2.4 Сроки реализации	13
Глава 3. Сфера применения Рекомендации 16	15
3.1 Платежи и переводы ценностей	15
3.2 Внутренние и трансграничные платежи и переводы	15
3.3 Субъекты, на которых распространяются требования Рекомендации 16	16
3.4 Взаимодействие с другими Рекомендациями ФАТФ.....	17
Глава 4. Обязанности участников платежной цепочки	24
4.1 Определение платежной цепочки по маршруту передачи распоряжения.....	24
4.2 Принципы определения платежной цепочки	24
4.3 Системы нетто-расчетов и пакетные транзакции: обязанности участвующих финансовых учреждений	25
4.4 Обязанности финансовых учреждений.....	28
4.5 Особенности применения требований к услугам по переводу денежных средств или ценностей (УПДЦ).....	33
4.6 Платежные инфраструктуры.....	37
Глава 5. Требования к информации.....	41
5.1 Общие положения о требованиях Рекомендации 16 к информации.....	41
5.2 Структурированные данные в соответствии со стандартами обмена сообщениями (например, ISO 20022)	41
5.3 Обязательства в отношении трансграничных платежей и переводов.....	44
5.4 Внутренние переводы.....	53
5.5 Виртуальные номера счетов.....	55
5.6 Сноски об источнике средств	60
5.7 Вопросы финансовой доступности, связанные с применением порога <i>de minimis</i> 64	
Глава 6. Требования, применяемые к карточным операциям	66
6.1 Сфера применения	66
6.2 Обязанности участников платежной цепочки.....	70
Глава 7. Выдача наличных денежных средств за рубежом.....	76
7.1 Обоснование применения специальных требований к операциям по выдаче наличных денежных средств за рубежом.....	76
7.2 Проблемы в сфере ПОД/ФТ, связанные с выдачей наличных денежных средств за рубежом	76
7.3 Требования к информации при снятии наличных	77
Глава 8. Применение Рекомендации 16 к различным способам оплаты и переводов.....	80
8.1 Основные принципы.....	80

8.2	Применение Рекомендации 16 к мгновенным платежам	80
8.3	Платежи с использованием цифровых кошельков	83
8.4	Платежи с использованием сервисов мобильных денег	86
Глава 9. Вопросы защиты неприкосновенности частной жизни и персональных данных		89
9.1	Правовые основания для сбора, обработки и передачи информации в соответствии с Рекомендацией 16.....	89
9.2	Основные принципы	90
9.3	Имплементация требований Рекомендации 16 в национальное законодательство	92
9.4	Требования к информационной безопасности и данным повышенного риска	96
9.5	Особенности применения Рекомендации 16 к карточным платежам и выдаче наличных денежных средств за рубежом.....	98
9.6	Вопросы защиты персональных данных при использовании комплексных систем постоянного мониторинга	99
10.1	Обоснование проведения проверок соответствия данных	100
10.2	Обзор вариантов внедрения	100
10.3	Понятие проверки соответствия данных	101
10.4	Область применения проверок соответствия данных	103
10.5	Реализация механизмов проверки соответствия данных	103
10.6	Действия при выявлении несоответствий	114
Приложение: Схемы платежных цепочек		116

Сокращения и аббревиатуры

БМР	Банк международных расчетов
ЕЭЗ	Европейская экономическая зона
ЕС	Европейский союз
ИНН	идентификационный номер налогоплательщика
ОД	отмывание денег
ООН	Организация Объединенных Наций
ПОД	противодействие отмыванию денег
ПУВА	поставщик услуг в сфере виртуальных активов
ПФР	подразделение финансовой разведки
СБ ООН	Совет Безопасности Организации Объединенных Наций
УПДЦ	услуги по переводу денежных средств или ценностей
ФАТФ	Группа разработки финансовых мер борьбы с отмыванием денег
ФРОМУ	финансирование распространения оружия массового уничтожения
ФТ	финансирование терроризма
AMLR	Регламент Европейского союза о противодействии использованию финансовой системы для отмывания денег или финансирования терроризма
API	интерфейс прикладного программирования
BCR	обязательные корпоративные правила
BIC	идентификационный код юридического лица
BIN	банковский идентификационный номер
BISIH	Инновационный центр Банка международных расчетов
CASP	поставщик услуг в сфере криптоактивов
CDD	надлежащая проверка клиента
CoP	подтверждение получателя платежа (Confirmation of Payee)
CPMI	Комитет по платежам и рыночным инфраструктурам
CSCF	Система контроля безопасности клиентов
DPP	защита неприкосновенности частной жизни и персональных данных
EDS	Сервис каталогов Европейского платежного совета
EMV	международный стандарт проведения карточных операций
EPC	Европейский платежный совет
FPS	Система быстрых платежей Гонконга
GDPR	Общий регламент Европейского союза по защите данных
GSMA	Ассоциация операторов мобильной связи
IBAN	международный номер банковского счета
IMF	Международный валютный фонд
IMPS	Система мгновенных платежей Индии
ISO	Международная организация по стандартизации
IEC	Международная электротехническая комиссия
KYC	процедура идентификации и проверки клиента («Знай своего клиента»)
LEI	идентификатор юридического лица
MT	формат финансовых сообщений SWIFT
NEFT	Система национальных электронных переводов Индии
NIST	Национальный институт стандартов и технологий США

P2P	перевод между физическими лицами
PAN	основной номер счета платежной карты
PCI DSS	Стандарт безопасности данных индустрии платежных карт
PETs	технологии повышения конфиденциальности
RFI	сообщение о запросе информации
RTGS	Система валовых расчетов в режиме реального времени
SCT Inst	схема мгновенных кредитовых переводов в евро
SIM	модуль идентификации абонента
SMS	служба коротких сообщений
SWIFT	Сообщество всемирных межбанковских финансовых телекоммуникаций
SWIFT gpi	сервис глобальных платежных инноваций SWIFT
TFR	Регламент о сведениях, сопровождающих переводы денежных средств и отдельных криптоактивов
TFS	целевые финансовые санкции
UPI	Единый платежный интерфейс Индии
USSD	неструктурированные дополнительные сервисные данные
vIBAN	виртуальный международный номер банковского счета
VoP	проверка получателя платежа (Verification of Payee)
VPA	виртуальный платежный адрес

Глава 1. Резюме

1.1 Резюме

1. Платежи и переводы ценностей играют ключевую роль в мировой экономике. Они расширяют доступ населения к финансовым услугам, способствуют развитию торговли и поддерживают систему денежных переводов, имеющую важное социально-экономическое значение для миллионов семей. Вместе с тем платежная инфраструктура может использоваться не только для проведения законных финансовых операций, но и в противоправных целях, включая перемещение средств, связанных с преступной деятельностью. Развитие финансовых технологий и появление новых участников платежного рынка привели к усложнению платежных цепочек, что затрудняет выявление финансовыми учреждениями подозрительной деятельности, а также получение компетентными органами необходимой информации. В настоящее время мошенничество является основным источником преступных доходов во всем мире и одним из основных предикатных преступлений, связанных с отмыванием денег. Именно эти обстоятельства обусловили пересмотр Рекомендации 16 ФАТФ, обновленная редакция которой была принята в июне 2025 года.

2. Рекомендация 16 устанавливает требования к прозрачности платежей в целях противодействия отмыванию денег (ОД), финансированию терроризма (ФТ), финансированию распространения оружия массового уничтожения (ФРОМУ) и мошенничеству. Указанные требования обязательны для государств и финансовых учреждений. Пересмотренная редакция Рекомендации 16 уточняет распределение функций и обязанностей финансовых учреждений на всех этапах платежной цепочки и усиливает требования к составу информации, сопровождающей платежи и переводы. Кроме того, она вводит проверки соответствия данных для выявления ошибочно направленных платежей и устанавливает специальные требования к операциям по трансграничной выдаче наличных денежных средств. Полное внедрение пересмотренной редакции Рекомендации 16 ожидается к концу 2030 года.

3. Пересмотренная редакция Рекомендации 16 основана на принципе «одинаковая деятельность - одинаковые риски - одинаковые правила», согласно которому обязанности определяются характером осуществляемой деятельности, а не видом организации. В главе 3 рассматриваются сфера применения Рекомендации 16 и ее взаимосвязь с другими Рекомендациями ФАТФ и международными стандартами, включая Рекомендацию 15, посвященную виртуальным активам. Установление требований, сверх предусмотренных Рекомендацией 16, может привести к увеличению стоимости платежей и переводов, а также создать риски ограничения доступа к финансовым услугам без повышения эффективности применения соответствующих мер. В Руководстве вопросы доступности финансовых услуг учитываются применительно к ряду аспектов, включая пороговые значения *de minimis*¹, альтернативные механизмы и

¹ Минимальные пороговые значения, при превышении которых применяются соответствующие требования. Прим. пер.

упрощенные меры проверки. Государствам настоятельно рекомендуется в полной мере использовать предусмотренные Рекомендацией 16 возможности для гибкой реализации ее требований, а также разрабатывать рекомендации для финансовых учреждений с учетом особенностей их деятельности, включая учреждения, осуществляющие деятельность в условиях ограниченных возможностей.

4. Финансовые учреждения, участвующие в платежной цепочке, должны выполнять обязанности, соответствующие их роли в платежной цепочке. Платежная цепочка начинается с финансового учреждения, получившего распоряжение плательщика, и заканчивается финансовым учреждением, обслуживающим счет получателя либо осуществляющим выдачу наличных денежных средств получателю. В главе 4 определены обязанности финансового учреждения плательщика, финансового учреждения-посредника и финансового учреждения получателя, сформулированы общие принципы, применимые к различным сценариям осуществления платежей и переводов, а также изложены практические меры, способствующие реализации требований Рекомендации 16 операторами платежной инфраструктуры.

5. В главе 5 установлен состав информации, который должен сопровождать платежи и переводы, и определены случаи, когда ее передача обязательна. Состав такой информации зависит от того, является ли перевод внутренним или трансграничным, а также превышает ли сумма перевода пороговое значение *de minimis*. При осуществлении трансграничных переводов, превышающих указанное пороговое значение, финансовое учреждение плательщика обязано проверить достоверность информации о плательщике, включая его имя (наименование), номер счета, адрес, дату рождения, а также, при наличии, идентификатор юридического лица (LEI). Требования к информации о получателе являются менее строгими: в качестве адреса достаточно указать страну и населенный пункт, а сведения о дате рождения не требуются. При осуществлении внутренних переводов платежное сообщение может содержать только номер счета либо уникальный идентификатор операции при условии, что полная информация может быть предоставлена в течение трех рабочих дней. Если финансовое учреждение плательщика не поддерживает с плательщиком постоянные отношения, предусматривающие возможность хранения ценностей (например, на счете или в электронном кошельке), требуется дополнительная информация, позволяющая идентифицировать счет и финансовое учреждение, с которого списываются средства. Идентификаторы счетов, включая номера виртуальных счетов, не должны скрывать сведения о финансовом учреждении, обслуживающем счет, а также о государстве, в котором оно находится.

6. В главе 6 рассматриваются две категории карточных операций. Карточные P2P-переводы между физическими лицами, включая пополнение счетов и электронных кошельков, на которых могут храниться средства, подпадают под действие всех требований Рекомендации 16. В отношении операций по оплате товаров и услуг с использованием платежных карт применяется упрощенный порядок. В Руководстве изложены практические принципы, позволяющие определить, к какой из указанных категорий относится соответствующая операция. При осуществлении любых карточных операций по оплате товаров и услуг платежное сообщение должно содержать номер

платежной карты, а сведения о наименовании и месте нахождения финансового учреждения-эмитента и финансового учреждения-эквайера должны предоставляться по запросу. Ключевая роль в выполнении указанных требований отводится карточным платежным системам.

7. В главе 7 установлен специальный порядок применения требований Рекомендации 16 к операциям по снятию наличных денежных средств за рубежом. По запросу финансового учреждения-эквайера информация об имени держателя платежной карты должна быть предоставлена финансовому учреждению-эквайеру в течение трех рабочих дней с момента получения такого запроса. В Руководстве также разъясняется порядок применения указанного требования к группам финансовых учреждений, использующим эквивалентные политики доступа к информации.

8. В главе 8 приведены подробные разъяснения по применению требований Рекомендации 16 к мгновенным платежам, операциям через электронные кошельки и сервисы мобильных денег, без установления для них отдельных правил. В главе рассматриваются вопросы сопоставления прокси-идентификаторов, определения финансового учреждения плательщика при осуществлении операций с использованием электронных кошельков, а также применения требований Рекомендации 16 к платформам сервисов мобильных денег, обслуживающим уязвимые категории населения.

9. Все главы Руководства следует рассматривать во взаимосвязи с главой 9. Вопросы защиты неприкосновенности частной жизни и персональных данных рассматриваются не изолированно, а применительно ко всем этапам сбора, хранения и передачи информации, предусмотренных Рекомендацией 16. В главе приведены разъяснения по вопросам определения правовых оснований обработки персональных данных. В частности, каким образом режимы ПОД/ФТ/ФРОМУ и защиты неприкосновенности частной жизни и персональных данных взаимно дополняют друг друга, а также - особенности обработки данных повышенного риска, данных платежных карт и применения комплексных механизмов мониторинга.

10. Пересмотренная редакция Рекомендации 16 вводит обязанность финансовых учреждений получателя проводить проверку соответствия данных в целях противодействия серьезной и возрастающей угрозе мошенничества. При осуществлении трансграничных переводов, превышающих пороговое значение *de minimis*, финансовые учреждения получателя должны выявлять платежи, направленные ненадлежащему получателю. В главе 10 разъясняется, что проверка соответствия данных представляет собой поэтапный риск-ориентированный процесс. В ней описаны три варианта проведения такой проверки, а также порядок учета выявленных несоответствий при принятии решений и определении последующих мер в рамках риск-ориентированного подхода.

11. Эффективность применения Рекомендации 16 в конечном счете зависит от последовательного внедрения ее требований. ФАТФ намерена и далее содействовать

развитию диалога, подчеркивая важность согласованных усилий всех заинтересованных сторон.

1.2 Правовой статус Руководства

12. Настоящее Руководство следует рассматривать во взаимосвязи с Рекомендацией 16 и Пояснительной запиской к ней в редакции, принятой в июне 2025 года². Руководство не является обязательным и не устанавливает новых обязанностей, не изменяет действующие требования, предусмотренные Стандартами ФАТФ. Его цель заключается в разъяснении практического применения Стандартов ФАТФ и описании возможных подходов, которые государства и финансовые учреждения могут использовать для эффективного внедрения Рекомендации 16. Руководство не носит обязательного характера, а содержащиеся в нем рекомендации могут применимы не во всех случаях. Любые ссылки в настоящем Руководстве на подходы, применяемые в отдельных юрисдикциях, приводятся исключительно в качестве примеров и не должны рассматриваться как одобренные ФАТФ либо как свидетельствующие об эффективности системы соответствующей юрисдикции.

Глава 2. Введение

2.1 Цель Рекомендации 16

13. Рекомендация 16 применяется к внутренним и трансграничным платежам и переводам и предусматривает, что финансовые учреждения и поставщики услуг в сфере виртуальных активов (ПУВА) должны, помимо прочего, сопровождать такие операции требуемой информацией о плательщике и получателе. Такая информация позволяет финансовым учреждениям эффективно выявлять подозрительные или необычные операции, а также содействует отслеживанию движения средств подразделениями финансовой разведки и правоохранительными органами в целях проведения анализа, расследования и уголовного преследования. Кроме того, Рекомендация 16 требует, чтобы финансовые учреждения, участвующие в осуществлении платежей и переводов, принимали разумные меры по выявлению операций, не сопровождающихся требуемой информацией. При выявлении таких операций финансовое учреждение должно определить, следует ли исполнить, отклонить или приостановить операцию, а также какие последующие меры необходимо принять в соответствии с риск-ориентированным подходом.

14. ФАТФ ожидает, что компетентные органы не допустят ограничения законного доступа к финансовым услугам, в том числе для уязвимых категорий населения. Вопросы взаимосвязи требований Рекомендации 16 с задачами повышения доступности финансовых услуг рассматриваются в главе 3, в которой приводятся ссылки на соответствующие материалы ФАТФ, а также интегрированы положения, сформулированные в ранее опубликованных документах ФАТФ по данной тематике.

² [ФАТФ обновляет стандарты по Рекомендации № 16 о прозрачности платежей](#)

Кроме того, принимая во внимание чувствительный характер платежных данных, в главе 9 приведены специальные рекомендации по вопросам защиты персональных данных и конфиденциальности. ФАТФ ожидает, что государства не допустят, чтобы меры по соблюдению требований Рекомендации 16 ограничивали законный доступ к финансовым услугам, а также обеспечат безопасную обработку всей информации, собираемой в соответствии с Рекомендацией 16, с соблюдением применяемых требований законодательства и стандартов в области защиты персональных данных и конфиденциальности.

15. Рекомендация 16 направлена на достижение следующих целей: (1) предотвращение использования платежей и переводов для перемещения средств террористами, лицами, совершающими легализацию (отмывание) преступных доходов, включая связанные с ней предикатные преступления, в том числе мошенничество, а также другими преступниками; и (2) выявление таких случаев неправомерного использования.

16. В частности, Рекомендация 16 направлена на предоставление незамедлительного доступа к базовой информации о плательщике и получателе платежей и переводов:

- (a) компетентным правоохранительным органам и (или) органам прокуратуры - в целях содействия выявлению, расследованию и уголовному преследованию террористов и иных преступников, а также отслеживанию их активов;
- (b) подразделениям финансовой разведки - в целях анализа подозрительной или необычной деятельности и, при необходимости, передачи соответствующей информации; и
- (c) финансовым учреждениям плательщика, финансовым учреждениям-посредникам и финансовым учреждениям получателя - в целях содействия выявлению и сообщению о подозрительных операциях, а также выполнения требований по замораживанию активов и соблюдению запретов на проведение операций с обозначенными лицами и организациями в соответствии с обязательствами, установленными соответствующими резолюциями Совета Безопасности Организации Объединенных Наций (СБ ООН), касающимися предупреждения и пресечения терроризма и финансирования терроризма, а также резолюциями, касающимися предупреждения, пресечения и противодействия распространению оружия массового уничтожения и его финансированию.

2.2 Предпосылки последних изменений Рекомендации 16³ - эволюция платежной экосистемы

17. Платежная экосистема, включая способы осуществления платежей, платежные инструменты, платежные системы, технологии и поставщиков платежных услуг, претерпела значительные изменения с момента принятия Рекомендации 16 в 2012 году⁴.

18. Развитие финансовых технологий привело к появлению новых способов осуществления платежей и переводов ценностей. Одновременно с этим появились различные финансовые учреждения, оказывающие платежные услуги вне банковского сектора и взаимодействующие с клиентами напрямую. Такие изменения создали неопределенность в отношении применения Рекомендации 16.

19. Например, появление сторонних операторов платежных услуг, непосредственно взаимодействующих с клиентами, означает, что финансовые учреждения, на которые традиционно распространяются требования Рекомендации 16 (например, учреждения, обслуживающие счета), могут больше не иметь полного представления обо всей платежной цепочке, а также своевременного или полного доступа к информации о плательщике и получателе. Дальнейшая фрагментация платежных цепочек также затрудняет получение информации, необходимой для выявления подозрительной деятельности или подозрительных операций и выполнения обязанностей в области ПОД/ФТ/ФРОМУ. Кроме того, это осложняет подразделениям финансовой разведки и правоохранительным органам доступ к необходимой информации. В связи с этим важно, чтобы Рекомендация 16 четко определяла роли финансовых учреждений в рамках установленной платежной цепочки.

20. Характер угроз, связанных с незаконной финансовой деятельностью, также изменился. За последние годы количество и объем мошеннических операций существенно возросли в мировом масштабе, и в настоящее время мошенничество является основным видом преступной деятельности, приносящей доход.⁵ В связи с этим в Рекомендации 16 мошенничество прямо включено в число ее целей, а также введено требование о проведении проверок соответствия данных в целях снижения риска ошибочного направления платежей наряду с более широким набором мер, направленных на повышение прозрачности информации, сопровождающей трансграничные платежи и переводы.

³ По состоянию на дату публикации настоящего Руководства под Рекомендацией 16 понимается редакция, принятая в июне 2025 года.

⁴ Рекомендация ФАТФ «Электронные переводы денежных средств» ранее входила в состав [Специальной рекомендации VII ФАТФ](#) (последний пересмотр - 2008 г.).

⁵ 156 юрисдикций (90% от общего числа прошедших оценку юрисдикций) прямо определяют мошенничество в качестве одного из основных рисков легализации (отмывания) преступных доходов. Более подробную информацию см. в документе [«Незаконные финансовые потоки, связанные с мошенничеством с использованием кибертехнологий» \(2023 г.\)](#).

2.3 Деятельность ФАТФ по повышению прозрачности платежей в рамках Дорожной карты «Группы двадцати»

21. Платежи и переводы ценностей имеют важное значение для устойчивого развития. На Саммите «Группы двадцати», состоявшемся в ноябре 2020 года, лидеры «Группы двадцати» одобрили Дорожную карту по совершенствованию трансграничных платежей, направленную на решение выявленных проблем, связанных с их высокой стоимостью, длительными сроками проведения, недостаточной доступностью и прозрачностью. Указанные проблемы тесно связаны с затруднениями при передаче платежных данных и недостаточным качеством таких данных в рамках все более сложных и фрагментированных платежных цепочек.

22. Изменения, внесенные в Рекомендацию 16, являются одним из ключевых результатов реализации Дорожной карты «Группы двадцати» (Блок 5). Они развивают систему прозрачности платежей, сформированную ФАТФ, и направлены на сокращение существующих затруднений при сохранении безопасности и целостности трансграничных платежей, в том числе за счет повышения прозрачности платежных цепочек и расширения возможностей финансовых учреждений по выявлению мошенничества и иной незаконной деятельности. «Группа двадцати» признала такие виды преступной деятельности одним из ключевых источников затруднений и снижения доверия к платежным услугам. Указанные требования основаны на принципе «одинаковая деятельность - одинаковые риски - одинаковые правила», согласно которому обязательства определяются характером осуществляемой деятельности, а не типом организации, которая ее осуществляет. Таким образом, повышение прозрачности будет способствовать снижению негативных последствий от незаконной деятельности, одновременно усиливая меры в области ПОД/ФТ/ФРОМУ.

23. Более четкое разграничение ролей и обязанностей участников, единые требования к информации и более широкое использование структурированных данных ⁶, как ожидается, будут способствовать повышению качества данных и развитию сквозной обработки платежей, что сократит количество ошибок и задержек, а также объем ручной обработки. Кроме того, применение более согласованных подходов в различных юрисдикциях позволит снизить регуляторную фрагментацию, которая способствует увеличению стоимости и сложности осуществления трансграничных платежей.

2.4 Сроки реализации

24. Для полноценной реализации обновленной Рекомендации 16 необходим переходный период, который позволит частному сектору планомерно внедрить новые требования, а операторам платежной инфраструктуры - адаптировать используемые ими системы к новым требованиям. ФАТФ ожидает, что все обновленные требования будут в полном объеме реализованы к концу 2030 года. Настоящее Руководство, а также дальнейшее взаимодействие ФАТФ с заинтересованными сторонами направлены на

⁶ См. главу 5, посвященную понятию «структурированных данных» в контексте Рекомендации 16.

содействие внедрению обновленных требований регуляторами, органами по установлению стандартов и представителями отрасли.

Глава 3. Сфера применения Рекомендации 16

25. В настоящей главе разъясняются сфера применения Рекомендации 16, основные термины и ее взаимосвязь с другими Стандартами ФАТФ и иными международными стандартами, включая ISO 20022.

3.1 Платежи и переводы ценностей

26. В первоначальной редакции Рекомендации 16 использовался термин «электронные переводы денежных средств», при этом основное внимание уделялось случаям, когда платеж инициируется финансовым учреждением, обслуживающим счет клиента. По мере изменения рыночной практики ФАТФ приняла решение заменить термин «электронные переводы денежных средств», чтобы обеспечить нейтральность Рекомендации 16 по отношению к способам осуществления платежей и привести ее в большее соответствие с целями данного Стандарта.

27. Понятие «платеж(и) и перевод ценностей» толкуется широко и охватывает любую операцию, осуществляемую от имени плательщика через финансовое учреждение плательщика с использованием электронных средств в целях предоставления определенной суммы средств в распоряжение получателя в финансовом учреждении получателя независимо от того, являются ли плательщик и получатель одним и тем же лицом. В понятие «платеж(и) и перевод ценностей» также входит выдача наличных денежных средств.

28. Для целей применения Рекомендации 16 электронные кошельки и иные аналогичные платежные счета рассматриваются в качестве счетов. Идентификатор счета, например адрес электронного кошелька или номер телефона, используемый в качестве идентификатора электронного кошелька, может выполнять для целей Рекомендации 16 функцию, эквивалентную традиционному номеру счета.

29. Рекомендация 16 применяется ко всем операциям, подпадающим под указанное определение, при этом состав соответствующих требований различается в зависимости от вида операции и применимого порогового значения *de minimis*.

3.2 Внутренние и трансграничные платежи и переводы

30. Рекомендация 16 применяется как к внутренним, так и к трансграничным платежам и переводам. Ключевое различие заключается в месте нахождения финансовых учреждений, участвующих в платежной цепочке, как это определено в Глоссарии ФАТФ и изложено ниже:

31. Внутренние платежи и переводы: данное определение включает два элемента. Во-первых, оно относится к платежной цепочке или цепочке перевода ценностей, полностью проходящей в пределах одного государства, то есть когда финансовое учреждение

плательщика и финансовое учреждение получателя находятся в одной стране⁷. Во-вторых, как отмечено в Пояснительной записке к Рекомендации 16, данный термин также охватывает любую цепочку платежей и переводов, которая полностью осуществляется в пределах Европейской экономической зоны (ЕЭЗ)⁸.

32. Трансграничные платежи и переводы: трансграничным платежом или переводом признается любой перевод, при котором финансовое учреждение плательщика и финансовое учреждение получателя находятся в разных странах. Данное определение также охватывает любую цепочку платежей и переводов, в которой хотя бы одно из участвующих финансовых учреждений находится в иной стране.

3.3 Субъекты, на которых распространяются требования Рекомендации 16

33. Требования Рекомендации 16 распространяются на любые субъекты, подпадающие под определение «финансовое учреждение» в Глоссарии ФАТФ. Данное определение охватывает широкий круг субъектов и должно применяться исходя из фактически осуществляемой деятельности, а не организационно-правовой формы или наименования субъекта. Такой подход отражает принцип «одинаковая деятельность - одинаковые риски - одинаковые правила» и обеспечивает распространение требований Рекомендации 16 на всех участников платежной цепочки, имеющих значение для целей настоящей Рекомендации. В контексте Рекомендации 16 к таким видам деятельности, указанным в определении «финансовое учреждение» в Глоссарии ФАТФ, относятся оказание услуг по переводу денежных средств или ценностей, выпуск или управление средствами платежа, а также привлечение депозитов или иных возвратных средств от населения. По мере развития платежной экосистемы в сферу применения Рекомендации 16 могут подпадать новые виды субъектов, если осуществляемая ими деятельность соответствует указанному определению. Государствам следует оценивать новых участников платежного рынка с учетом данного функционального подхода.

34. Субъекты, оказывающие услуги по переводу денежных средств или ценностей (УПДЦ), прямо включены в определение «финансовое учреждение» в Глоссарии ФАТФ. Согласно Глоссарию ФАТФ, такие услуги представляют собой финансовые услуги, предусматривающие прием наличных денежных средств, чеков, иных денежных инструментов или иных средств, предназначенных для хранения ценностей, а также выплату соответствующей суммы наличными денежными средствами или в иной форме получателю посредством передачи сообщений, перевода либо через клиринговую сеть. Данное определение намеренно сформулировано широко, чтобы охватывать широкий

⁷ Местонахождение системы, используемой для передачи платежных сообщений, не влияет на определение того, является ли платеж или перевод ценностей внутренним или трансграничным.

⁸ На момент публикации настоящего Руководства ЕЭЗ является единственной юрисдикцией, обозначенной ФАТФ в качестве наднациональной юрисдикции для целей Рекомендации 16. Любая организация может подать в ФАТФ ходатайство о признании её в качестве наднациональной юрисдикции для целей оценки соблюдения любых Стандартов ФАТФ в соответствии с процедурой, изложенной в [Универсальных процедурах ФАТФ](#).

круг операций, включая операции с использованием новых способов осуществления платежей или с участием посредников (в соответствующих случаях - операторов сервисов мобильных денег). Если иное прямо не указано, требования настоящего Руководства распространяются на все виды платежных цепочек (например, с использованием виртуальных активов или гибридных моделей). Помимо общих требований, применимых ко всем видам финансовых учреждений, в случаях, когда поставщик услуг по переводу денежных средств или ценностей (УПДЦ) осуществляет контроль как на стороне плательщика, так и на стороне получателя перевода, применяется пункт 32 Пояснительной записки к Рекомендации 16.

35. Определение «финансовое учреждение» в Глоссарии ФАТФ прямо исключает любых физических и юридических лиц, которые предоставляют финансовым учреждениям исключительно услуги по обмену сообщениями или иные вспомогательные системы для передачи средств. Такие субъекты не осуществляют платежи и переводы в значении Рекомендации 16 и не относятся к субъектам, на которых распространяются требования настоящей Рекомендации.

36. Несмотря на то что поставщики технических услуг и операторы инфраструктуры платежного рынка не подпадают под действие Рекомендации 16, они играют важную роль в соблюдении ее требований финансовыми учреждениями. ФАТФ рекомендует поставщикам технических услуг, включая поставщиков услуг по обмену сообщениями, содействовать соблюдению требований Рекомендации 16, обеспечить возможность передачи по всей платежной цепочке требуемой информации о плательщике и получателе.

37. Государствам и надзорным органам следует отслеживать непредвиденные последствия реализации Рекомендации 16 и принимать меры для предотвращения необоснованных нарушений в функционировании платежной системы, особенно в случаях, когда существуют технические ограничения.

3.4 Взаимодействие с другими Рекомендациями ФАТФ

Взаимодействие обязательств, предусмотренных Рекомендацией 16, с обязательствами, предусмотренными Рекомендацией 10

38. В соответствии с Рекомендацией 10 меры надлежащей проверки клиента применяются в следующих случаях:

- (i) при установлении деловых отношений;
- (ii) при проведении разовых операций (а) на сумму, превышающую установленное пороговое значение (15 000 долларов США/евро); или (б) представляющих собой платежи или переводы в случаях, предусмотренных Пояснительной запиской к Рекомендации 16;
- (iii) при наличии подозрений в ОД/ФТ; или
- (iv) если у финансового учреждения возникают сомнения в достоверности или достаточности ранее полученных идентификационных данных клиента.

39. Рекомендация 16 сама по себе не устанавливает полный перечень требований к надлежащей проверке клиента, предусмотренных Рекомендацией 10. Вместе с тем Рекомендация 16 содержит специальные требования к проверке данных, направленные на повышение прозрачности платежей. При осуществлении трансграничных и внутренних платежей и переводов, превышающих пороговое значение *de minimis*, финансовые учреждения плательщика обязаны проверять достоверность информации о плательщике. Для платежей и переводов ниже порогового значения *de minimis* такая проверка требуется только при наличии подозрений в ОД/ФТ. Кроме того, при трансграничных платежах и переводах, превышающих пороговое значение *de minimis*, финансовые учреждения получателя обязаны проверить личность получателя, если такая проверка ранее не проводилась. Указанные требования к проверке следует отличать от проверки соответствия данных о получателе, которая направлена на выявление ошибочно направленных платежей и снижение рисков мошенничества и не является идентификацией клиента или надлежащей проверкой клиента.

40. Информация, полученная при проведении надлежащей проверки клиента в соответствии с Рекомендацией 10, позволяет финансовым учреждениям выполнять требования Рекомендации 16, включая в платежные сообщения необходимую информацию о плательщике и получателе.

Взаимодействие обязательств, предусмотренных Рекомендацией 16, с обязательствами, предусмотренными Рекомендацией 14

41. Согласно Рекомендации 14, государства должны осуществлять эффективный мониторинг и контроль за соблюдением соответствующих Стандартов ФАТФ физическими и юридическими лицами, оказывающими услуги по переводу денежных средств или ценностей (УПДЦ). В соответствии со Стандартами ФАТФ любое физическое или юридическое лицо, оказывающее такие услуги, относится к финансовым учреждениям. Соответственно, требования Рекомендации 16 распространяются на финансовые учреждения, включая поставщиков УПДЦ, при осуществлении ими платежей и переводов. Пунктом 32 Пояснительной записки к Рекомендации 16 установлены специальные требования к таким поставщикам, которые самостоятельно либо через сеть по переводу денежных средств или ценностей осуществляют контроль как на стороне плательщика, так и на стороне получателя (подробная информация приведена в главе 4).

Взаимосвязь обязательств, предусмотренных Рекомендацией 16, с обязательствами, предусмотренными Рекомендацией 15

42. Если в настоящем Руководстве упоминаются финансовые учреждения, то под ними также понимаются поставщики услуг виртуальных активов (ПУВА), поскольку требования Рекомендации 16 распространяются на них в соответствии с Пояснительной запиской к Рекомендации 15. ПУВА следует выполнять обязанности, установленные настоящим Руководством для финансовых учреждений, к своей деятельности аналогичным образом с учетом особенностей, изложенных ниже в разделе, посвященном

взаимосвязи требований Рекомендации 16 и Рекомендации 15. На практике ПУВА обязаны выполнять те же требования, что и финансовые учреждения, включая сбор и передачу необходимой информации, а также, при необходимости, проверку ее достоверности.

43. При осуществлении ПУВА перевода виртуальных активов применяются требования Рекомендации 15 (включая Travel Rule⁹). Если на любом этапе гибридной платежной цепочки осуществляется операция с фиатными денежными средствами, к такой операции применяются требования Рекомендации 16. При этом гибридная платежная цепочка считается единой, если перевод осуществляется на основании единого распоряжения плательщика независимо от способа его исполнения (см. главу 4). При осуществлении переводов виртуальных активов, подпадающих под действие Рекомендации 15, требования Рекомендации 16 применяются с учетом следующих особенностей: необходимая информация передается такому поставщику на стороне получателя по соответствующим безопасным каналам передачи информации и не включается непосредственно в перевод виртуальных активов. Кроме того, на таких поставщиков распространяются новые требования Рекомендации 16, касающиеся проверок соответствия данных.¹⁰

44. В обновленном Руководстве ФАТФ по риск-ориентированному подходу к виртуальным активам и поставщикам услуг виртуальных активов (2021 г.) разъясняется ряд особенностей применения требований Рекомендации 16:

- кастодиальные кошельки для целей применения Рекомендации 16 рассматриваются как функциональный аналог традиционных банковских счетов. В частности, адреса кошельков выполняют ту же функцию, что и номера счетов, при идентификации плательщиков и получателей, а ПУВА при участии в платежных цепочках обязаны соблюдать те же требования к составу передаваемой информации и ее хранению, что и финансовые учреждения.
- для целей применения Рекомендации 16 государствам следует рассматривать все переводы виртуальных активов как трансграничные независимо от того, находятся ли плательщик и получатель в одной юрисдикции.

⁹ «Travel rule» (иногда переводится как «правило путешествия») – означает требование передавать в составе расчетных документов информацию об отправителе и получателе. Прим. пер.

¹⁰ В рамках обеих публичных консультаций ПУВА отмечали необходимость повышения гибкости при выполнении указанных требований, поскольку они не связаны ограничениями, характерными для традиционной платежной инфраструктуры, и зачастую используют современные решения для реализации Travel Rule. Они также указывали, что инструменты предварительной проверки уже широко применяются в сфере виртуальных активов, что обусловлено практически мгновенным и необратимым характером переводов виртуальных активов.

- пороговое значение разовой операции, при превышении которого ПУВА обязаны проводить надлежащую проверку клиента, составляет 1 000 долларов США/евро (а не 15 000 долларов США/евро).

45. ФАТФ продолжит содействовать внедрению Travel Rule в сфере виртуальных активов.

Сноска 49 к пункту 1(с) Пояснительной записки к Рекомендации 16 и требования о целевых финансовых санкциях

46. В ходе консультаций по обновлению Рекомендации 16 заинтересованные стороны отмечали, что проверка соблюдения требований о целевых финансовых санкциях («санкционная проверка») существенно осложняет обработку платежей и переводов. В частности, Рекомендация 16 нередко толковалась как устанавливающая требование о проведении санкционной проверки в режиме реального времени. Такое толкование основывалось на содержащемся в Рекомендации 16 указании на роль финансовых учреждений при «обработке» платежей и переводов в целях соблюдения требований о целевых финансовых санкциях. Соответствующее положение сформулировано следующим образом:

«Государствам следует требовать от финансовых учреждений при обработке платежей и переводов ценностей осуществлять замораживание активов и не проводить операции с лицами и организациями, в отношении которых применяются целевые финансовые санкции, ...»
(Рекомендация 16).

47. Этот вопрос разъяснен в новой сноске 49 к пункту 1(с) Пояснительной записки к Рекомендации 16, в которой указано, что Рекомендация 16:

- не изменяет сферу применения действующих требований о целевых финансовых санкциях, которые регулируются другими Рекомендациями ФАТФ (в частности, Рекомендациями 6 и 7¹¹); и
- не устанавливает требований относительно того, *должна ли передаваемая информация проверяться по санкционным перечням и каким образом такая проверка должна осуществляться, поскольку соблюдение соответствующих требований может обеспечиваться различными механизмами (...).*

48. Способ проведения санкционной проверки в целях соблюдения международных стандартов определяется национальным регулированием и сложившейся отраслевой практикой. ФАТФ признает существование различных подходов к реализации требований о целевых финансовых санкциях (например, проведение санкционной

¹¹ В соответствии со Стандартами ФАТФ и резолюциями Совета Безопасности ООН основными обязанностями при реализации целевых финансовых санкций являются незамедлительное замораживание средств или иных активов лиц и организаций, в отношении которых применяются целевые финансовые санкции, а также недопущение предоставления таким лицам и организациям каких-либо средств или иных активов.

проверки ежедневно, а не в режиме реального времени) и не устанавливает в Рекомендации 16 конкретный способ выполнения требований о целевых финансовых санкциях.

Вставка 1. Практический пример - подходы к проведению санкционной проверки при осуществлении мгновенных платежей

В Европейском союзе для эффективного соблюдения требований о целевых финансовых санкциях и снижения нагрузки, связанной с проведением санкционной проверки каждой операции в режиме реального времени, Регламент о мгновенных платежах предусматривает иной подход. Вместо проверки каждой операции финансовые учреждения обязаны не реже одного раза в календарный день, а также незамедлительно после вступления в силу каждого нового или измененного санкционного перечня Европейского союза (и, соответственно, ООН) проверять, включены ли их клиенты в соответствующие перечни. При выявлении совпадений финансовые учреждения обязаны осуществлять замораживание активов и не допускать предоставления таким лицам каких-либо средств или иных активов.

Источник: Европейская комиссия

Взаимосвязь с другими международными стандартами (в частности, стандартами CPMI по инфраструктурам финансового рынка и стандартом SWIFT ISO 20022)

49. Стандарты ФАТФ не предусматривают непосредственного распространения требований в сфере ПОД/ФТ/ФРОМУ на операторов инфраструктуры платежного рынка. Такой подход соответствует определению финансового учреждения, закрепленному ФАТФ, согласно которому к финансовым учреждениям не относятся физические и юридические лица, предоставляющие финансовым учреждениям исключительно услуги по обмену сообщениями или иные вспомогательные системы для передачи средств.

50. Вместе с тем операторы инфраструктуры платежного рынка по-прежнему играют ключевую роль в соблюдении обновленных требований Рекомендации 16, в частности передавая необходимую информацию по всей платежной цепочке. ФАТФ намерена и далее поддерживать эту работу во взаимодействии с частным сектором, в том числе со SWIFT, и другими международными организациями, разрабатывающими стандарты, в том числе CPMI. Одним из направлений дальнейшей работы станет обновление стандарта ISO 20022, позволяющее указывать либо дату рождения без места рождения, либо только год рождения вместо полной даты рождения. Это обусловлено тем, что в действующем формате дата и место рождения объединены в одном поле.¹²

¹² ФАТФ приняла решение не требовать предоставления информации о месте рождения ввиду более ограниченных возможностей её проверки, особенно в условиях ограниченных ресурсов.

Взаимодействие с пересмотренной Рекомендацией 1 и Руководством по финансовой доступности

51. Компетентные органы должны сохранить предусмотренные Рекомендацией 16 гибкие и альтернативные механизмы и отразить их в национальном регулировании и надзорной практике. Такой подход отражает изменения, внесенные в 2025 году в Руководство ФАТФ по вопросам финансовой доступности¹³ и Рекомендацию 1, согласно которым меры в сфере ПОД/ФТ/ФРОМУ должны быть соразмерны оцененным рискам и предусматривать возможность применения упрощенных мер в случаях выявления более низких рисков.

52. На практике несоразмерное применение Рекомендации 16 может иметь место, например, если регуляторы, надзорные органы или финансовые учреждения не учитывают должным образом риски ОД/ФТ. Это может выражаться в следующем:

- a. систематическом истребовании информации или проведении проверок сверх требований, установленных Рекомендацией 16, независимо от вида операции или применимого порогового значения;
- b. необоснованном отнесении операций с низким уровнем риска к операциям с более высоким уровнем риска;
- c. неприменении упрощенных режимов, прямо предусмотренных Рекомендацией 16 (например, пороговых значений *de minimis*); или
- d. признании отдельных операционных или технологических решений обязательными, несмотря на то что Стандарты ФАТФ предусматривают несколько вариантов их реализации.

53. Как отмечается в обновленном Руководстве ФАТФ по вопросам финансовой доступности, такой подход повышает риск ограничения доступа к финансовым услугам, может увеличивать издержки, создавать дополнительные барьеры и сокращать доступ к регулируемым платежным услугам, не повышая при этом эффективность мер в сфере ПОД/ФТ/ФРОМУ.

54. При внедрении обновленной Рекомендации 16 государствам рекомендуется:

- Четко определить в своих документах порядок применения требований Рекомендации 16, в том числе разъяснить, в каких случаях допускается гибкость, а в каких - нет, чтобы снизить риск неправильного толкования требований и их избыточного применения.
- Любые дополнительные требования, выходящие за рамки Рекомендации 16, следует применять только при наличии риск-ориентированного обоснования, при этом основания для их применения должны быть понятны как финансовым

¹³ [FATF press release of the Guidance paper on Financial inclusion and AML/CFT measures](#)

учреждениям, так и надзорным органам, в том числе с учетом результатов оценки рисков, проведенной в соответствии с Рекомендацией 1.

- Исходить из того, что риск несоразмерного применения требований существует не только в странах с ограниченными ресурсами, особенно в части сбора и проверки информации. Аналогичные проблемы могут возникать и у уязвимых групп населения в странах с более развитой экономикой, что следует учитывать при осуществлении надзора.
- Учитывать особенности небольших финансовых учреждений (например, кредитных союзов), которые могут сталкиваться с трудностями при внедрении Рекомендации 16 вследствие ограниченных технических возможностей и отсутствия необходимых инструментов для соблюдения ее требований. Надзорным органам следует устанавливать четкие требования, соразмерные уровню риска и особенностям деятельности таких организаций.
- использовать приведенные в главе 5 настоящего Руководства примеры альтернативных способов проверки и идентификации, направленных на снижение негативного влияния на финансовую доступность, в том числе в странах с менее развитой системой идентификации или в отношении клиентов, не имеющих стандартизированных почтовых адресов, при внедрении обновленных требований.

55. Соблюдение принципа соразмерности рискам при применении Рекомендации 16 имеет ключевое значение для повышения прозрачности платежей и формирования эффективной, менее затратной, доступной и устойчиво функционирующей платежной экосистемы.

Глава 4. Обязанности участников платежной цепочки

4.1 Определение платежной цепочки по маршруту передачи распоряжения

56. Развитие платежных технологий и изменение структуры рынка все больше затрудняют определение начала и окончания платежной цепочки. В частности, небанковские финансовые учреждения все чаще осуществляют прием и выплату средств в электронной форме, а также используют национальные платежные системы для проведения трансграничных переводов. На практике это может затруднять определение государства отправления или назначения платежа либо перевода, что, в свою очередь, осложняет проведение проверок, мониторинга, а также осуществление надзорных и правоохранительных мероприятий.

57. Одним из ключевых требований Рекомендации 16 является включение предусмотренной информации в платежное распоряжение и ее передача по всей платежной цепочке - от ее начала до завершения платежа или перевода. В связи с этим четкое определение платежной цепочки имеет принципиальное значение для установления обязанностей финансовых учреждений, участвующих в осуществлении платежа или перевода, независимо от их вида, а также для единообразного применения требований ко всем категориям финансовых учреждений. Это также позволяет предотвратить дробление одного трансграничного перевода на несколько операций, которые формально выглядят как внутренние, в условиях развития платежной экосистемы, предполагающей участие различных посредников и платежных систем. При этом финансовые учреждения, участвующие в платежной цепочке, несут ответственность за соблюдение требований Рекомендации 16 независимо от того, кем выполняются отдельные операционные функции (например, если техническую поддержку оказывают посредники, не являющиеся финансовыми учреждениями).

58. Для целей Рекомендации 16 платежная цепочка определяется следующим образом:

- Начинается с финансового учреждения, получающего распоряжение от клиента (по маршруту передачи распоряжения); и
- Заканчивается финансовым учреждением, обслуживающим счет получателя либо осуществляющим выдачу наличных денежных средств получателю.

4.2 Принципы определения платежной цепочки

59. Способы осуществления платежей и переводов постоянно развивается и, как ожидается, будет меняться и в дальнейшем. В настоящем разделе изложены принципы, обеспечивающие единообразное определение платежной цепочки применительно к различным видам платежей и переводов по мере появления новых механизмов их осуществления. Для пояснения порядка применения определения платежной цепочки и соответствующих принципов к различным практическим ситуациям в приложении приведены иллюстративные примеры.

60. К основным принципам относятся:

- Платежная цепочка начинается с распоряжения плательщика о предоставлении средств получателю. Для целей Рекомендации 16 такое распоряжение дается плательщиком финансовому учреждению плательщика для исполнения соответствующего платежа или перевода.
- Если распоряжение плательщика с его согласия передается финансовому учреждению плательщика третьим лицом, в частности финансовым учреждением получателя (такой механизм иногда именуется «платежом по требованию получателя» (pull payment) или прямым дебетованием (direct debit)), такая операция также подпадает под действие Рекомендации 16. Передача распоряжения финансовому учреждению плательщика через третье лицо не изменяет его правовой природы.
- В качестве конечного участника платежной цепочки финансовое учреждение получателя считается *предоставляющим средства получателю*¹⁴, независимо от того, выдаются ли они наличными денежными средствами (или в иной эквивалентной форме) либо зачисляются на счет получателя.
- Для целей Рекомендации 16 под *счетом*¹⁵ понимается счет или платежный инструмент, оформленный на имя пользователя либо используемый в его интересах для хранения средств (включая кошельки с электронными деньгами).
- Если в рамках платежной цепочки изменяется форма средств или передаваемой ценности (например, осуществляется конвертация одной формы денег в виртуальные активы либо обмен иностранной валюты), это само по себе не означает возникновения новой платежной цепочки или завершения существующей, если только плательщик не дал нового распоряжения.

4.3 Системы нетто-расчетов и пакетные транзакции: обязанности участвующих финансовых учреждений

Переводы между финансовыми учреждениями¹⁶

61. На переводы или расчеты между финансовыми учреждениями, в которых и плательщиком, и получателем являются финансовые учреждения, действующие от собственного имени и за свой счет, требования Рекомендации 16 в части передачи информации не распространяются. К таким операциям относятся, в частности, межбанковские переводы, а также нетто-расчеты и расчеты с отсроченным завершением,

¹⁴ Согласно Глоссарию ФАТФ к Рекомендации 16, под «платежом или переводом ценностей» понимается любая операция, осуществляемая по поручению плательщика через финансовое учреждение плательщика с использованием электронных средств в целях предоставления средств получателю в финансовом учреждении получателя, независимо от того, совпадают ли плательщик и получатель. К таким операциям также относится выдача наличных денежных средств.

¹⁵ Согласно Глоссарию ФАТФ, термин «счет» охватывает также иные аналогичные формы деловых отношений между финансовыми учреждениями и их клиентами.

¹⁶ Пункт 13 Пояснительной записки к Рекомендации 16

осуществляемые для взаимозачета требований и обязательств и управления риском ликвидности между несколькими финансовыми учреждениями, действующими от собственного имени и за свой счет.

Нетто-расчеты, возникающие в результате платежей и переводов, осуществляемых от имени клиентов¹⁷

62. При нетто-расчетах финансовые учреждения осуществляют взаимозачет клиентских операций, после чего между соответствующими финансовыми учреждениями проводится один перевод на сумму итоговой задолженности¹⁸. В отличие от пакетных транзакций (рассматриваются ниже), при переводе в рамках нетто-расчетов ни плательщиком, ни получателем не является отдельный клиент. Информация об операциях, лежащих в основе нетто-расчета, не должна сопровождать такой перевод

63. Вместе с тем клиентские операции, по которым производится нетто-расчет, по-прежнему подпадают под действие соответствующих требований Рекомендации 16. Это означает, что каждая такая операция должна соответствовать требованиям Рекомендации 16 в части передачи информации независимо от того, что расчеты по ней осуществляются в рамках нетто-расчета, как если бы она исполнялась как самостоятельная операция.

Риски неправомерного использования механизмов нетто-расчетов

64. При оценке соблюдения требований Рекомендации 16 надзорным органам, финансовым учреждениям плательщика и финансовым учреждениям получателя следует исходить из фактического характера платежей и переводов, а не только из используемого формата сообщений. Такой подход позволяет предотвратить неправомерное использование механизмов нетто-расчетов при осуществлении платежей и переводов по поручению клиентов. Финансовые учреждения-посредники при этом не обязаны выделять отдельные операции из платежей, осуществляемых в рамках нетто-расчетов.

Маршруты обмена сообщениями в рамках корреспондентских отношений (покрытые платежи)

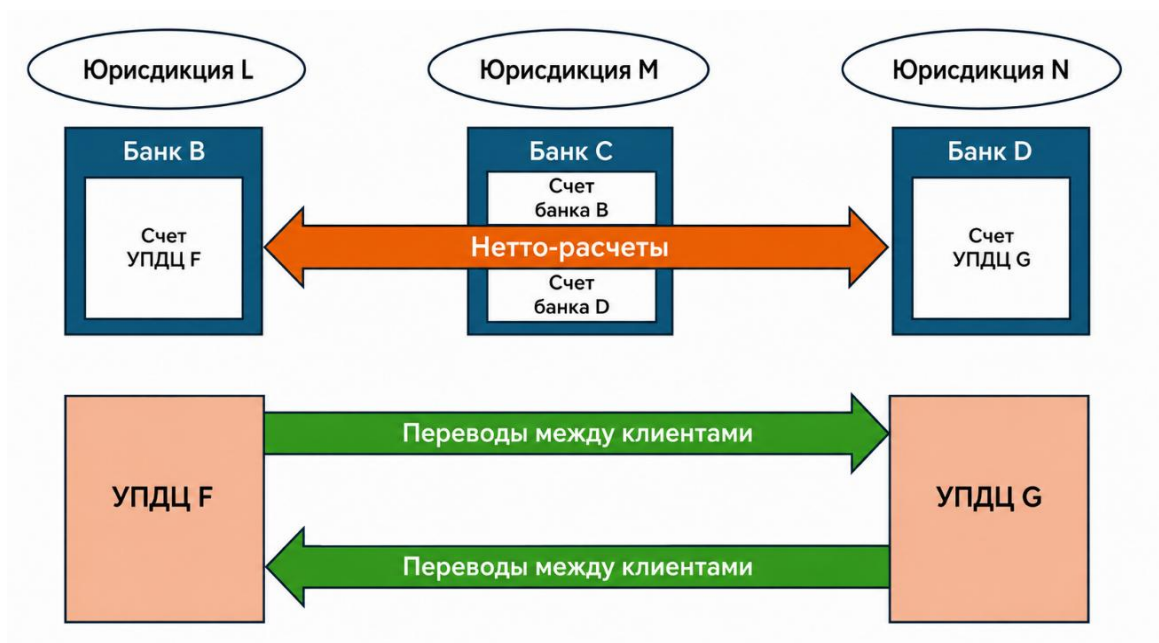
65. Исключение, предусмотренное для нетто-расчетов, не распространяется на покрытые платежи, как они определены в Пояснительной записке к Рекомендации 16. При осуществлении покрытого платежа перевод осуществляется между финансовым учреждением плательщика и финансовым учреждением получателя по двум маршрутам: непосредственно между указанными финансовыми учреждениями и параллельно - через финансовые учреждения-посредники, участвующие в расчетах по переводу. В отличие от платежа, осуществляемого в рамках нетто-расчетов, сообщение о покрытом платеже

¹⁷ Пункт 14 Пояснительной записки к Рекомендации 16

¹⁸ Нетто-расчет осуществляется после проведения соответствующих клиентских операций, лежащих в его основе. Иные виды расчетных переводов могут осуществляться до их проведения (например, в рамках отдельных бизнес-моделей операторов услуг по переводу денежных средств) либо одновременно с ними. Такие переводы не относятся к нетто-расчетам, однако также могут не подпадать под действие Рекомендации 16, если представляют собой переводы между финансовыми учреждениями, действующими от собственного имени и за свой счет.

содержит соответствующие сведения о клиентском платеже или переводе. Соответственно, как сообщение о покрытом платеже, так и соответствующий клиентский платеж или перевод должны сопровождаться требуемой информацией о плательщике и получателе в соответствии с Рекомендацией 16¹⁹.

Пример схемы нетто-расчетов между двумя УПДЦ



66. В данном примере клиенты УПДЦ F, расположенной в юрисдикции L, осуществляют переводы клиентам УПДЦ G, расположенной в юрисдикции N, и наоборот. Такие переводы в полном объеме подпадают под требования Рекомендации 16. По каждому из них вся предусмотренная информация должна передаваться по всей платежной цепочке от УПДЦ F к УПДЦ G и от УПДЦ G к УПДЦ F (зеленые стрелки на схеме).

67. Для проведения расчетов по переводам между своими клиентами УПДЦ F направляет своему банку - Банку В - распоряжение о переводе денежных средств на счет УПДЦ G, открытый в Банке D (либо УПДЦ G направляет своему банку - Банку D - распоряжение о переводе денежных средств на счет УПДЦ F, открытый в Банке В). При этом УПДЦ, направившая распоряжение, информирует банк о том, что данный перевод представляет собой нетто-расчет между финансовыми учреждениями.

68. Поскольку такой перевод представляет собой нетто-расчет, требования Рекомендации 16 на него не распространяются. Банк С, расположенный в юрисдикции М, также не несет обязанностей, предусмотренных Рекомендацией 16, в связи с выполнением функций финансового учреждения-посредника при осуществлении

¹⁹ Согласно пункту 3 Пояснительной записки к Рекомендации 16 требования Рекомендации 16 распространяются на трансграничные и внутренние платежи и переводы, включая последовательные и покрытые платежи.

перевода между Банком В и Банком D по поручению УПДЦ F и G (оранжевая стрелка на схеме).

Пакетные переводы²⁰

69. Пакетный перевод представляет собой передачу нескольких платежей от одного плательщика нескольким получателям в составе одного файла. Типичным примером пакетного перевода является перечисление государством пенсионных выплат нескольким получателям пенсии, находящимся в иностранном государстве.

70. Рекомендация 16 предусматривает возможность применения упрощенного порядка в отношении файла, сопровождающего трансграничный пакетный перевод. В таком пакетном переводе достаточно указать номер счета плательщика либо уникальный идентификатор операции при условии, что сопровождающий файл содержит всю необходимую информацию о плательщике и получателе, предусмотренную Рекомендацией 16 для каждого отдельного перевода, входящего в пакет, а информация о получателе может быть полностью прослежена в пределах юрисдикции получателя. Такое исключение позволяет повысить эффективность обработки большого количества переводов, устраняя необходимость дублирования информации о плательщике в каждом отдельном переводе.

4.4 Обязанности финансовых учреждений

4.4.1 Общие обязанности, распространяющиеся на все финансовые учреждения

71. Рекомендация 16 требует своевременно передавать информацию о плательщике и получателе всем финансовым учреждениям, участвующим в платежной цепочке. Такая информация необходима для выявления подозрительных операций, направления сообщений о них и соблюдения требований, связанных с применением целевых финансовых санкций.

72. Например, соблюдение требований Рекомендации 16 позволяет финансовым учреждениям выявлять подозрительные схемы, при реализации которых отсутствует информация о плательщике или получателе либо предпринимаются попытки скрыть такую информацию или истинный характер операций. Кроме того, проверка достоверности информации о плательщике и подтверждение личности получателя могут способствовать выявлению подозрительных операций.²¹

4.4.2 ФИНАНСОВОЕ УЧРЕЖДЕНИЕ ПЛАТЕЛЬЩИКА

73. Согласно Стандартам ФАТФ *финансовым учреждением плательщика* является финансовое учреждение, которое получает от плательщика распоряжение о переводе

²⁰ Пункт 15 Пояснительной записки к Рекомендации 16

²¹ Применительно к целевым финансовым санкциям Рекомендация 16 разъясняет, что соблюдение соответствующих требований может обеспечиваться различными механизмами. При этом Рекомендация 16 не устанавливает, должна ли информация о плательщике и получателе проверяться по санкционным перечням и каким образом такая проверка должна осуществляться.

средств получателю. Таким образом, в контексте применения Рекомендации 16 финансовое учреждение плательщика является начальным звеном платежной цепочки.

74. Обязанности финансового учреждения плательщика в целом можно разделить на три основные категории: (1) включение в платежные сообщения всей требуемой информации и их передачи финансовым учреждениям-посредникам (либо, если таковые отсутствуют, финансовому учреждению получателя); (2) хранение собранной при совершении платежа или перевода информации о плательщике и получателе; и (3) выполнение необходимых проверок до исполнения платежей или переводов. Указанные обязанности в обновленной редакции Рекомендации 16 не изменились.

(1) Включение в платежные сообщения всей требуемой информации

75. Объем информации о плательщике и получателе, которой должен сопровождаться платеж или перевод, зависит от того, является ли он трансграничным или внутренним, а также от применимого порогового значения.

76. При осуществлении трансграничных и внутренних платежей и переводов, превышающих пороговое значение *de minimis*, финансовое учреждение плательщика обязано обеспечить достоверность информации о плательщике. По платежам и переводам, совершаемым разовыми клиентами и превышающим указанное пороговое значение, достоверность информации о плательщике должна проверяться по каждой операции с использованием надежных и независимых источников. Если же плательщик является клиентом финансового учреждения, как правило, используется информация, достоверность которой уже была подтверждена при установлении деловых отношений или в ходе последующей надлежащей проверки клиента, без повторной проверки при совершении каждой операции.²²

77. Финансовое учреждение плательщика обязано передать финансовому учреждению-посреднику всю предусмотренную информацию о плательщике и получателе.²³ При этом:

- Информация должна быть по возможности структурирована в соответствии с применимым стандартом обмена платежными сообщениями.
- информация, сопровождающая исходящее платежное сообщение, должна отражать конечную точку платежной цепочки в соответствии с распоряжением плательщика, что позволяет определить, является ли платеж или перевод трансграничным или внутренним.

(2) Хранение информации о плательщике и получателе

²² Следует также отметить, что даже при осуществлении платежей и переводов, не превышающих пороговое значение, достоверность информации о плательщике должна проверяться при наличии подозрений в ОД/ФТ. [Практические примеры проверки информации о плательщике приведены в главе 5.]

²³ При этом финансовое учреждение плательщика не обязано обеспечивать достоверность информации о получателе.

78. Информация о плательщике и получателе, собираемая в целях выполнения требований Рекомендации 16, подлежит хранению в соответствии с требованиями Рекомендации 11 ФАТФ. Финансовое учреждение плательщика обязано хранить информацию обо всех платежах и переводах не менее пяти лет.

(3) Меры, принимаемые при решении вопроса об исполнении платежей и переводов

79. Финансовое учреждение плательщика не должно исполнять платеж или перевод, не соответствующий требованиям Рекомендации 16. Для этого финансовое учреждение плательщика должно убедиться, что платежное сообщение содержит всю необходимую информацию. При отсутствии обязательной информации финансовое учреждение плательщика самостоятельно определяет дальнейшие действия. Если при осуществлении трансграничного платежа или перевода плательщик указывает только имя получателя, не предоставляя сведения о стране и городе получателя либо номере его счета, исполнение платежа или перевода должно быть приостановлено до получения недостающей информации. Если плательщик не может предоставить запрошенную информацию, платеж или перевод не должен исполняться

4.4.3 ФИНАНСОВОЕ УЧРЕЖДЕНИЕ-ПОСРЕДНИК

80. Согласно Стандартам ФАТФ финансовым учреждением-посредником является финансовое учреждение, которое в рамках платежной цепочки принимает и передает платеж или перевод от имени финансового учреждения плательщика и финансового учреждения получателя либо другого финансового учреждения-посредника. Финансовые учреждения-посредники играют ключевую роль в сохранности всей обязательной информации при передаче платежного сообщения.

81. В соответствии с Рекомендацией 16 финансовые учреждения-посредники обязаны принимать меры, перечисленные ниже. Указанные обязанности в обновленной редакции Рекомендации 16 не изменились.

(1) Сохранность информации о плательщике и получателе

82. Финансовое учреждение-посредник должно сохранять неизменной всю информацию, полученную от финансового учреждения плательщика и подлежащую передаче вместе с платежом или переводом.

83. Согласно Рекомендации 16, если вследствие технических ограничений невозможно сохранить обязательную информацию, сопровождающую трансграничный платеж или перевод при его передаче через внутреннюю платежную систему, финансовое учреждение-посредник должно хранить в течение не менее пяти лет всю информацию, полученную от финансового учреждения плательщика или другого финансового учреждения-посредника. Такие технические ограничения могут быть обусловлены использованием устаревших систем, не поддерживающих передачу всей обязательной информации, либо отсутствием совместимости между различными платежными сетями, используемыми в платежной цепочке. При наличии нескольких

возможных решений финансовые учреждения должны использовать те из них, которые в наибольшей степени обеспечивают соблюдение требований Рекомендации 16.

(2) Меры в отношении переводов, по которым отсутствует обязательная информация

84. При осуществлении трансграничных переводов финансовые учреждения-посредники должны принимать разумные меры для выявления платежей или переводов, по которым отсутствует обязательная информация о плательщике и получателе. Финансовым учреждениям-посредникам следует учитывать, что Рекомендация 16 допускает использование альтернативных механизмов для отдельных информационных полей, например указание года рождения вместо полной даты рождения либо страны и населенного пункта вместо полного адреса. Платеж, в котором используются такие альтернативные механизмы, соответствует требованиям Рекомендации 16 и должен рассматриваться как содержащий полный объем обязательной информации. Рекомендация 16 не требует безусловного отклонения платежей, по которым отсутствует или является неполной обязательная информация. К разумным мерам относятся, например, основанные на оценке рисков автоматизированные средства контроля или внутренние процедуры, позволяющие выявлять случаи отсутствия или неполноты обязательной информации, в том числе использование правил проверки данных для выявления отсутствующей информации, а также последующий выборочный контроль и процедуры контроля качества для выявления системных недостатков

85. Финансовые учреждения-посредники должны разработать и применять риск-ориентированные политики и процедуры, определяющие: (а) в каких случаях исполнять, отклонять или приостанавливать платежи или переводы, по которым отсутствует обязательная информация о плательщике и (или) получателе; и (б) какие последующие меры следует принять.

86. При разработке указанных политик следует учитывать уровень риска операций²⁴, допустимый уровень риска, определенный финансовым учреждением, а также характер и частоту случаев отсутствия обязательной информации по операциям конкретных клиентов. Финансовое учреждение-посредник должно иметь возможность на основе оценки рисков принимать решение об исполнении, отклонении или приостановлении платежа или перевода, если отсутствие обязательной информации выявлено до его исполнения. Надзорным органам настоятельно рекомендуется препятствовать практике, подрывающей применение упрощенных альтернативных механизмов, допускаемых Рекомендацией 16. Например, при применении риск-ориентированного подхода исполнение операции может быть оправданным, если отсутствующая информация носит несущественный характер либо плательщик относится к категории низкого риска, а причина отсутствия информации является обоснованной (например, связана с ошибкой

²⁴ Например, платеж или перевод средств из юрисдикции с высоким уровнем риска, на крупную сумму, с участием подозрительных контрагентов.

форматирования или утратой части текста вследствие того, что используемая система не позволяет передать полное имя физического лица). Вместе с тем финансовое учреждение-посредник может принять решение о приостановлении исполнения или удержании перевода, если отсутствие информации вызывает сомнения, которые могут быть устранены после получения дополнительных разъяснений. Финансовое учреждение-посредник может отклонить перевод, если отсутствие информации создает существенный риск ОД/ФТ (например, при неоднократном и необоснованном несоблюдении требований со стороны конкретного финансового учреждения плательщика).

87. Надлежащей последующей мерой может быть, например, запрос недостающей информации у финансового учреждения плательщика либо взаимодействие с финансовым учреждением плательщика или другим финансовым учреждением-посредником в целях устранения выявленных систематических нарушений. При наличии признаков того, что характер или обстоятельства таких нарушений могут свидетельствовать о возможной связи с ОД/ФТ, соответствующий случай подлежит дальнейшему рассмотрению.

4.4.4 ФИНАНСОВОЕ УЧРЕЖДЕНИЕ ПОЛУЧАТЕЛЯ

88. Стандарты ФАТФ определяют финансовое учреждение получателя как финансовое учреждение, обслуживающее счет получателя или осуществляющее выдачу наличных денежных средств получателю. Финансовое учреждение получателя является конечным звеном платежной цепочки.

89. Финансовое учреждение получателя является единственным финансовым учреждением, непосредственно взаимодействующим с получателем в рамках установленных деловых отношений либо при проведении разовой операции. Финансовое учреждение получателя является основным финансовым учреждением, в отношении которого компетентные органы государства, в котором завершается платежная цепочка, осуществляют регулирование и надзор.

(1) Меры в отношении переводов, по которым отсутствует обязательная информация

90. Финансовые учреждения получателя должны принимать разумные меры для выявления трансграничных операций, по которым отсутствует обязательная информация о плательщике или получателе. Такие меры могут включать последующий мониторинг, а также мониторинг в режиме реального времени, если это практически осуществимо.

91. Финансовые учреждения получателя должны разработать и применять риск-ориентированные политики и процедуры, определяющие: (i) в каких случаях исполнять, отклонять или приостанавливать операцию, по которой отсутствует обязательная информация о плательщике или получателе, либо если операция могла быть ошибочно

направлена не тому получателю; и (ii) какие последующие меры следует принять²⁵. К числу таких мер могут относиться запрос недостающей информации у финансового учреждения плательщика или финансового учреждения-посредника, а также взаимодействие с соответствующим финансовым учреждением плательщика или финансовым учреждением-посредником для устранения выявленных систематических нарушений. При наличии признаков того, что характер или обстоятельства таких нарушений могут свидетельствовать о возможной связи с ОД/ФТ, соответствующий случай подлежит дальнейшему рассмотрению.

(2) Проверка личности получателя и хранение информации

92. При осуществлении трансграничных операций, превышающих порог *de minimis*, финансовое учреждение получателя должно провести проверку личности получателя, если она ранее не проводилась, и хранить соответствующую информацию не менее пяти лет в соответствии с Рекомендацией 11.

93. Как предусмотрено Рекомендацией 10, проверка личности предполагает подтверждение личности получателя на основании надежной независимой информации, данных или документов. Объем таких мер может корректироваться в пределах, допускаемых или предусмотренных национальным законодательством, с учетом рисков ОД/ФТ/ФРОМУ (например, с учетом результатов оценки соответствующих рисков, включая, помимо прочего, национальную оценку рисков).

94. Кроме того, финансовые учреждения получателя обязаны проводить проверки соответствия данных о получателе при осуществлении трансграничных операций, превышающих порог *de minimis*. Подробная информация приведена в главе 10.

4.5 Особенности применения требований к услугам по переводу денежных средств или ценностей (УПДЦ)

95. Операторы УПДЦ должны соблюдать все применимые требования Рекомендации 16 во всех государствах, в которых они осуществляют деятельность непосредственно либо через своих агентов²⁶.

96. В Глоссарии ФАТФ термин «услуги по переводу денег или ценностей (УПДЦ)» определен широко и охватывает различные модели оказания таких услуг. Операторы УПДЦ могут осуществлять деятельность по модели, аналогичной модели традиционных финансовых учреждений, либо использовать иные способы перевода денежных средств или ценностей, включая взаимозачетные механизмы.

97. УПДЦ не включают услуги, связанные исключительно с осуществлением переводов виртуальных активов от имени клиентов. Лица, оказывающие такие услуги, относятся к ПУВА, деятельность которых рассматривается в других разделах настоящего Руководства, а требования к платежам и переводам применяются к ним в соответствии с

²⁵ Включая требования к действиям финансовых учреждений получателя, предусмотренные пунктами 30 и 31 Пояснительной записки к Рекомендации 16

²⁶ Пункт 32 Пояснительной записки к Рекомендации 16

Рекомендацией 15. Вместе с тем государства вправе применять единый режим регулирования к операторам УПДЦ и ПУВА, оказывающим услуги по осуществлению платежей или переводов, при условии соблюдения требований Рекомендаций 15 и 16.

Требования, распространяющиеся на УПДЦ

98. В соответствии с Рекомендацией 16 государства должны распространять на УПДЦ все требования, относящиеся к платежам или переводам. При определении требований, распространяющихся на операторов УПДЦ, компетентным органам, как правило, необходимо учитывать используемые ими технологии, функциональные возможности операторов УПДЦ в соответствующей юрисдикции, а также факторы, снижающие риски. Учитывая разнообразие операторов УПДЦ, единый подход к применению указанных требований едва ли возможен. Например, см. приведенное ниже описание особенностей применения требований к УПДЦ при использовании структурированных данных.

99. Требования, относящиеся к платежам и переводам, не должны создавать препятствий для доступа к финансовым услугам. Применение Рекомендации 16 к операторам УПДЦ также не должно ограничивать доступ к таким услугам.

УПДЦ в цепочке платежей и переводов

100. Операторы УПДЦ могут выступать в качестве финансового учреждения плательщика, финансового учреждения-посредника и финансового учреждения получателя, если они выполняют соответствующие функции, определенные Рекомендацией 16.

101. В отношении операторов УПДЦ необходимо учитывать следующие особенности:

- При оказании некоторых услуг УПДЦ, включая услуги, предоставляемые с использованием системы «хавала» и других аналогичных систем (например, «хунди» и «фей чен»), финансовое учреждение плательщика и (или) финансовое учреждение получателя, оказывающее услуги УПДЦ, ни на одном из этапов цепочки осуществления платежа или перевода непосредственно не получает средства, подлежащие переводу, и не осуществляет контроль над ними. Вместо этого финансовое учреждение плательщика и финансовое учреждение получателя, оказывающие услуги УПДЦ, осуществляют расчеты между собой посредством взаимозачета (то есть нетто-расчетов), а не путем перевода средств по каждой отдельной операции.
- Финансовое учреждение-посредник, оказывающее услуги УПДЦ, также может не получать средства, подлежащие переводу, и не осуществлять контроль над ними, однако на него распространяются требования Рекомендации 16, если оно получает и передает информацию, сопровождающую платеж или перевод.²⁷

²⁷ Определение термина «услуги по переводу денежных средств или ценностей» в Глоссарии ФАТФ: «Настоящее определение не распространяется на физических или юридических лиц, которые предоставляют финансовым учреждениям исключительно

102. Как отмечается в определении УПДЦ, содержащемся в Глоссарии ФАТФ, некоторые финансовые учреждения получателя, оказывающие услуги УПДЦ, осуществляют выдачу перевода получателю не только в форме наличных денежных средств. Например, сумма перевода может быть зачислена на счет получателя, обслуживаемый таким финансовым учреждением. Кроме того, перевод может быть выдан получателю в форме чеков, иных денежных инструментов или средств сохранения стоимости (например, драгоценных металлов).

УПДЦ и структурированные данные

103. При применении требований к структурированию данных необходимо учитывать разнообразие бизнес-моделей, используемых операторами УПДЦ, а также необходимость сохранения доступности финансовых услуг. Многие операторы УПДЦ, особенно работающие в рамках небольших сетей УПДЦ, могут использовать форматы обмена сообщениями, отличные от ISO 20022. Стандарты ФАТФ допускают гибкий подход к структурированию информации, сопровождающей платежи или переводы. Это отражено в формулировке «по мере возможности»: информация должна быть структурирована настолько, насколько это возможно, и содержать достаточный объем сведений для идентификации плательщика и получателя. Под структурированными данными понимается такой способ представления информации, при котором каждый обязательный элемент данных размещается в отдельном поле платежного сообщения, а не объединяется с другими сведениями в одном поле произвольного текста.

Требования к сетям операторов УПДЦ

104. В соответствии с Рекомендацией 16 оператор УПДЦ, осуществляющий контроль над сетью УПДЦ, охватывающей как финансовое учреждение плательщика, так и финансовое учреждение получателя, а также любой оператор УПДЦ, входящий в такую сеть, должны:

- учитывать всю информацию, имеющуюся как у финансового учреждения плательщика, так и у финансового учреждения получателя, при принятии решения о необходимости направления сообщения о подозрительной операции; и
- направлять сообщение о подозрительной операции в подразделение финансовой разведки любой страны, затрагиваемой подозрительным платежом или переводом, а также предоставлять ему соответствующую информацию об операции.

105. Для целей настоящего Руководства под сетью УПДЦ понимается:

Под сетью УПДЦ понимается любой из следующих элементов либо их сочетание: (i) оператор УПДЦ и его агенты; или (ii) два или более операторов УПДЦ, связанных

системы передачи сообщений или иные вспомогательные системы для осуществления перевода средств. См. Пояснительную записку к Рекомендации 16».

одним или несколькими соглашениями об осуществлении платежей или переводов, включая, помимо прочего, взаиморасчеты по таким переводам.

106. В соответствии с Рекомендацией 14 агенты операторов УПДЦ подлежат лицензированию или регистрации в качестве самостоятельных субъектов либо на оператора УПДЦ возлагается обязанность вести актуальный перечень своих агентов, доступный компетентным органам государств, в которых осуществляют деятельность оператор УПДЦ и его агенты.

107. Как минимум на операторов УПДЦ, включая операторов сетей УПДЦ, учрежденных или осуществляющих деятельность на территории соответствующего государства, возлагается обязанность направлять сообщения о подозрительных операциях в подразделение финансовой разведки этого государства. При этом Стандарты ФАТФ не устанавливают обязательного порядка регулирования деятельности операторов сетей УПДЦ. Вместе с тем государства могут, в частности:

- распространять на операторов сетей УПДЦ требования законодательства в сфере ПОД/ФТ/ФРОМУ в качестве самостоятельных субъектов; или
- распространять на операторов сетей УПДЦ требования о направлении сообщений о подозрительных операциях, если они выступают в качестве финансовых учреждений-посредников в цепочке платежей или переводов.

108. Учитывая трансграничный характер деятельности многих операторов УПДЦ, основания для направления сообщений о подозрительных операциях должны охватывать случаи, когда оператор УПДЦ подозревает или имеет разумные основания подозревать, что переводимые средства являются доходами, связанными с ОД или предикатными преступлениями, либо используются для ФТ или иным образом связаны с указанными преступлениями. Обязанность по направлению сообщения о подозрительной операции не должна ограничиваться случаями, когда подозрение связано с возможной преступной деятельностью только в той юрисдикции, где осуществляет деятельность оператор УПДЦ. Такая обязанность должна распространяться и на случаи, когда подозрение связано с преступной деятельностью в других юрисдикциях.²⁸

109. Требования к направлению сообщений о подозрительных операциях должны распространяться на случаи, когда подозрения возникают в связи с деятельностью как плательщика, так и получателя независимо от того, являются ли они непосредственными клиентами оператора УПДЦ.

²⁸ В соответствии с Рекомендацией 20 при оценке возможной преступной деятельности в другой юрисдикции следует учитывать как минимум случаи, когда переводимые средства являются доходами, полученными в результате преступлений, либо связаны с преступлениями, которые в юрисдикции оператора УПДЦ признавались бы ОД, ФТ или предикатными преступлениями, а также с преступлениями, относящимися к одной из «установленных категорий преступлений», приведенных в Глоссарии к Рекомендациям ФАТФ.

110. Рекомендация 16 не требует от государств обязывать операторов сетей УПДЦ или иных операторов УПДЦ направлять сообщения о подозрительных операциях в подразделения финансовой разведки иностранных государств. Законодательство государств, включая положения, запрещающие информировать клиента или иных лиц о направлении сообщения о подозрительной операции либо о проведении проверки в связи с такой операцией, не должно препятствовать операторам УПДЦ, осуществляющим деятельность в нескольких юрисдикциях, направлять сообщения о подозрительных операциях в соответствии с требованиями законодательства каждой из таких юрисдикций.

4.6 Платежные инфраструктуры

4.6.1 Сфера применения и цели

111. Платежные инфраструктуры обеспечивают технологическую и процедурную основу для передачи, клиринга и расчетов по платежным инструкциям. В соответствии со Стандартами ФАТФ на платежные инфраструктуры не распространяются требования по ПОД/ФТ/ПРОМУ. Вместе с тем они обеспечивают инфраструктурную основу для деятельности финансовых учреждений. Технические спецификации, правила проверки данных и форматы обмена сообщениями, применяемые платежными инфраструктурами, непосредственно влияют на способность финансовых учреждений выполнять требования Рекомендации 16. Поэтому архитектура платежных инфраструктур и правила их функционирования являются важными элементами, обеспечивающими соблюдение финансовыми учреждениями требований Рекомендации 16. В настоящем разделе приведен обзор практик, имеющих значение для соблюдения требований Рекомендации 16. Платежным инфраструктурам настоятельно рекомендуется учитывать их при организации своей деятельности.

112. Ограничения, связанные с функционированием платежных инфраструктур, имеют наибольшее значение при осуществлении трансграничных платежей или переводов, поскольку могут препятствовать сохранению информации о трансграничном характере платежа, а также прослеживаемости информации об операции на всем протяжении платежной цепочки. В этой связи платежным инфраструктурам рекомендуется проектировать свои системы таким образом, чтобы они не ограничивали возможность финансовых учреждений определять:

- финансовые учреждения, участвующие в платежной цепочке;
- плательщика и получателя; а также
- юрисдикционный характер транзакции (например, является ли она трансграничной или внутренней).

4.6.2 Практические меры по реализации Рекомендации 16

113. Особое значение имеют три направления: (i) завершающий этап трансграничной платежной цепочки, на котором внутренним платежным инфраструктурам может потребоваться обеспечить техническую поддержку передачи данных, которая первоначально не была предусмотрена их архитектурой; (ii) техническая возможность

платежных инфраструктур передавать полный объем сведений о плательщике и получателе, предусмотренный обновленной Рекомендацией 16; и (iii) потенциальная роль платежных инфраструктур, например в качестве дополнительной услуги, в проведении проверок соответствия данных, в частности с использованием механизмов предварительной проверки.

Доступность и качество данных, обеспечиваемые на этапе проектирования

114. Платежным инфраструктурам рекомендуется, насколько это практически осуществимо:

- поддерживать передачу данных, предусмотренных Рекомендацией 16, в структурированных форматах (например, ISO 20022 или совместимых с ним форматах);
- предусмотреть достаточное количество полей данных для передачи обязательных сведений о плательщике и получателе;
- поддерживать единообразное использование идентификаторов в различных системах;
- избегать усечения или преобразования данных, которое может привести к потере информации в платежных сообщениях;
- обеспечивать прослеживаемость операций и возможность проведения аудита на всех этапах платежной цепочки, включая случаи использования нескольких платежных инфраструктур; и
- применять единообразные подходы к преобразованию данных при их передаче между различными платежными инфраструктурами во избежание утраты или искажения информации.

4.6.3 Сопоставление данных и выявление технических ограничений

115. Операторам платежных инфраструктур и национальным компетентным органам рекомендуется анализировать, каким образом обязательная информация сохраняется: (1) при инициировании платежа; (2) на всем протяжении платежной цепочки, включая (3) ее завершающий этап («последнюю милю»). Такой анализ позволяет выявить технические ограничения, в частности:

- Невозможность передачи отдельных элементов данных
- Использование форматов платежных сообщений, не поддерживающих структурированные данные
- Невозможность передачи информации о трансграничном характере перевода

116. Рекомендуется проводить такой анализ применительно к максимально широкому кругу операций, включая платежи, проходящие через различные платежные системы (например, из трансграничной платежной сети во внутреннюю платежную систему на завершающем этапе платежной цепочки).

4.6.4 Правила платежных инфраструктур и их функционирования

117. В правилах платежных инфраструктур и технических спецификациях рекомендуется четко определять: виды платежей и последовательность операций, поддерживаемых платежной инфраструктурой; стандарты данных и требования к платежным сообщениям (включая порядок заполнения отсутствующих данных); правила проверки соответствия требованиям для участия в платежной инфраструктуре; а также способы, позволяющие участвующим финансовым учреждениям идентифицировать все финансовые учреждения, задействованные в платежной цепочке, и юрисдикции, в которых они осуществляют деятельность. Это позволяет участвующим финансовым учреждениям применять платежную инфраструктуру в соответствии с требованиями Рекомендации 16 и снижает риск неоднозначного толкования информации на всем протяжении платежной цепочки.

118. Платежным инфраструктурам также рекомендуется определить наиболее эффективные способы содействия проведению проверок соответствия данных. В частности, где это практически осуществимо, они могут обеспечивать участвующим финансовым учреждениям возможность проверки соответствия имени получателя номеру счета до исполнения платежа (например, через механизмы предварительной проверки).

119. Если платежная инфраструктура, предназначенная преимущественно для осуществления внутренних платежей, используется также для обработки трансграничных платежей или переводов, в ее правилах рекомендуется прямо указывать, что на такие операции в полном объеме распространяются требования Рекомендации 16. Если финансовое учреждение или платежная инфраструктура преднамеренно направляет трансграничные платежи или переводы через инфраструктуру, не обеспечивающую выполнение указанных требований, компетентным органам рекомендуется рассмотреть вопрос о целесообразности применения надзорных мер или мер оверсайта²⁹.

4.6.5 Технические ограничения платежных инфраструктур

120. Рекомендация 16 не содержит прямого запрета на использование финансовыми учреждениями платежной инфраструктуры, которая не обеспечивает передачу всей обязательной информации. Вместе с тем финансовые учреждения по-прежнему отвечают за сбор обязательной информации на всем протяжении платежной цепочки. Если передать такую информацию по всей платежной цепочке невозможно, она должна предоставляться по запросу.

121. В странах с ограниченными ресурсами внедрение требований может осуществляться поэтапно, с последовательным повышением прозрачности платежей без

²⁹ Меры, принимаемые органом, осуществляющим наблюдение (oversight) за функционированием платежной инфраструктуры или платежной системы, например требования об устранении выявленных недостатков, рекомендации, ограничения или иные меры в рамках такого наблюдения (в отличие от классического пруденциального надзора за финансовыми учреждениями).

создания препятствий для доступа к платежным услугам. На первоначальном этапе усилия целесообразно сосредоточить на наиболее значимых и высокорисковых видах платежей, платежных коридорах и платежных продуктах. В отношении внутренних платежей с низким уровнем риска допускается применение упрощенного риск-ориентированного подхода.

122. В переходный период до 2030 года, пока платежные инфраструктуры не обеспечивают передачу всех обязательных элементов данных, могут применяться следующие подходы:

- (a) Для сохранения обязательной информации до завершения модернизации существующих инфраструктур могут использоваться механизмы сопоставления и преобразования данных, а также временные спецификации платежных сообщений. Это особенно актуально в случаях, когда внутренние платежные инфраструктуры используются для обработки завершающего этапа трансграничных платежей.
- (b) временные решения должны применяться только на переходном этапе. Их использование должно сопровождаться определением конечной целевой модели, сроков и контрольных этапов перехода к полной реализации требований обновленной Рекомендации 16, включая переход на структурированные стандарты обмена сообщениями (например, ISO 20022 или совместимые с ним форматы).

123. Эффективному внедрению требований в странах с ограниченными ресурсами могут способствовать скоординированные меры по развитию потенциала, дополняющие проводимые на национальном уровне реформы и модернизацию платежной инфраструктуры. В частности, ускорить этот процесс и обеспечить равные условия для всех участников рынка могут адресная поддержка модернизации национальных платежных инфраструктур, разработка практических рекомендаций по использованию структурированных данных и применению временных решений, а также повышение компетенций органов надзора и участников рынка в вопросах прозрачности платежной цепочки. Сотрудничество государственных органов, платежных инфраструктур, финансовых учреждений и международных партнеров позволит обеспечить устойчивое устранение инфраструктурных ограничений и достижение целей по повышению прозрачности платежей без ущерба для финансовой доступности. Организациям, оказывающим техническую помощь, настоятельно рекомендуется учитывать ограничения, описанные в настоящем разделе, при разработке программ поддержки, особенно для стран с ограниченными ресурсами.

Глава 5. Требования к информации

5.1 Общие положения о требованиях Рекомендации 16 к информации

124. Требования Рекомендации 16 к информации направлены на то, чтобы финансовые учреждения и компетентные органы могли идентифицировать плательщика и получателя платежа или перевода. Рекомендация 16 предусматривает включение финансовыми учреждениями в платежи или переводы и связанные с ними сообщения обязательной информации о получателе, а также обязательной и достоверной информации о плательщике. Под достоверной понимается информация, точность которой подтверждена в результате проверки и которая относится к платежам или переводам, превышающим порог *de minimis* (порядок проверки достоверности информации рассмотрен в разделе 5.3).

125. Стандартизация информации и повышение качества данных способствуют более надежной идентификации плательщика и получателя, а также повышению эффективности обработки платежей за счет автоматизации процессов и сокращения количества ложных срабатываний при проверке по санкционным перечням. Это также способствует выявлению подозрительных операций и проведению расследований.

126. В настоящей главе изложены требования Рекомендации 16 к составу информации, необходимой для эффективного соблюдения требований в сфере ПОД/ФТ/ФРОМУ. В соответствии с Дорожной картой «Группы двадцати» по совершенствованию трансграничных платежей требования к информации о плательщике и получателе направлены на повышение ее определенности и единообразия за счет сокращения объема необязательных сведений и повышения качества информации, сопровождающей платежи. При этом учтена необходимость сохранения доступа к финансовым услугам: если отдельные сведения отсутствуют, допускается использование альтернативных механизмов, например указание года рождения вместо полной даты рождения либо наименования населенного пункта и страны при отсутствии стандартизированного почтового адреса.

5.2 Структурированные данные в соответствии со стандартами обмена сообщениями (например, ISO 20022)

127. В современной платежной системе как трансграничные, так и внутренние платежи или переводы осуществляются с использованием различных платежных систем и платежных инфраструктур, отличающихся техническими возможностями, правилами функционирования и форматами сообщений. Международный стандарт обмена финансовыми сообщениями ISO 20022 позволяет использовать более единообразные и структурированные данные при обработке платежей. Платежные системы во всем мире постепенно переходят на использование ISO 20022 в качестве единого стандарта обмена сообщениями, а Комитет по платежам и рыночным инфраструктурам (CPMI) содействует его гармонизированному применению при осуществлении трансграничных платежей. Использование единого гармонизированного стандарта обмена сообщениями

и структурированного формата ISO 20022 способствует повышению эффективности обработки платежей и их прозрачности.

128. Все участники платежной цепочки (в частности, финансовые учреждения, ПУВА и платежные инфраструктуры) должны содействовать прозрачности и последовательно повышать качество информации, сопровождающей платежи и переводы. Согласно Рекомендации 16 такая информация должна:

- по возможности иметь структурированный формат в соответствии со стандартами обмена сообщениями, используемыми соответствующей платежной инфраструктурой (например, ISO 20022);
- содержать сведения, достаточные для идентификации плательщика и получателя³⁰.

129. Информация, сопровождающая платеж или перевод, должна быть достаточной для идентификации плательщика и получателя. В частности, при определении объема сведений, включаемых в имя плательщика или получателя, финансовым учреждениям следует учитывать риск неоднозначной идентификации (например, при указании только инициалов и фамилии вместо полного имени).

130. При реализации требований Рекомендации 16 финансовым учреждениям рекомендуется использовать платежные инфраструктуры, обеспечивающие сквозную передачу всей обязательной информации без ее утраты или усечения, а также сохранение целостности данных при преобразовании сообщений из одного формата в другой (например, между устаревшим форматом сообщений MT и ISO 20022 либо проприетарными форматами). При использовании сообщений стандарта ISO 20022 информацию рекомендуется указывать в специально предназначенных для этого структурированных полях (например, «окончательный дебитор» (ultimate debtor), «окончательный кредитор» (ultimate creditor), «назначение платежа», «информация для получателя», идентификаторы счета и адресные поля), а не в полях произвольного назначения или свободного текста.

131. Отсутствие структурированных данных в платежных сообщениях либо их ограниченное использование создает ряд проблем. К ним относятся сложности с идентификацией участников операций с участием нескольких сторон, увеличение количества ложных срабатываний при проверке по санкционным перечням, а также необходимость проведения трудоемких и фрагментарных расследований, поскольку финансовым учреждениям приходится восстанавливать информацию об операциях на основе данных, содержащихся в полях свободного текста, и дополнительных запросов о предоставлении информации.

132. Если технические ограничения не позволяют передать всю обязательную информацию, финансовым учреждениям следует руководствоваться четкими правилами определения приоритетности передаваемых сведений. В качестве примера могут

³⁰ Термины «плательщик» (originator) и «получатель» (beneficiary) используются в Рекомендации 16 и Пояснительной записке к ней. Соответственно, они являются эквивалентами терминов «дебитор» (debtor) и «кредитор» (creditor).

использоваться рекомендации Базельского комитета по банковскому надзору для банковского сектора.³¹ В частности:

- Физические лица: если технические ограничения не позволяют передать все имена клиента из-за ограничений по длине поля, финансовому учреждению плательщика рекомендуется передавать как минимум первое имя и фамилию клиента.
- Несколько участников платежа или перевода (например, совместные счета): если передача сведений обо всех участниках невозможна, финансовому учреждению плательщика рекомендуется передавать имя владельца счета в том виде, в котором оно указано в его клиентских данных.
- Юридические лица: если передача полного официального наименования невозможна, финансовому учреждению плательщика рекомендуется передавать коммерческое (фирменное) наименование при условии, что оно позволяет идентифицировать юридическое лицо и соответствует наименованию, содержащемуся в официальных реестрах. При наличии соответствующего идентификатора **BIC** или **LEI** информация о юридическом лице может быть получена из общедоступных источников.

Вставка 2. Рекомендуемые практики использования структурированных данных в платежных сообщениях

Эффективному внедрению структурированных данных способствуют: (1) включение требований Рекомендации 16 в процедуры идентификации и обслуживания клиентов, проектирование платежных сервисов и процессы обработки платежей и переводов; (2) корректное формирование информации при ее вводе и сохранение в неизменном виде на всем протяжении платежной цепочки; и (3) прослеживаемость обработки данных во внутренних платежных и контрольных системах финансового учреждения, позволяющая свести к минимуму их преобразование или изменение до передачи следующему финансовому учреждению в платежной цепочке.

Реализация требований к использованию структурированных данных предполагает координацию действий регуляторов, платежных инфраструктур и иных участников, осуществляющих платежи и переводы.

Возможности стандарта ISO 20022 позволяют, в частности:

- Использовать отдельные структурированные поля для указания информации о плательщике и получателе, кодов назначения платежа, информации о переводе, а также отдельные поля для имени и отдельных элементов адреса;

³¹ В качестве примера отраслевых рекомендаций можно привести Руководство Базельского комитета по банковскому надзору «Надлежащее управление рисками, связанными с легализацией (отмыванием) преступных доходов и финансированием терроризма» (январь 2014 года, редакция от июля 2020 года).

- При использовании национальных идентификаторов (например, национального идентификационного номера юридического лица) применять единые подходы к их формированию для последовательной и надежной идентификации участников платежной цепочки. Финансовым учреждениям также рекомендуется указывать государственный реестр, из которого получен соответствующий идентификатор;
- использовать стандартизированные сообщения о запросе информации ISO 20022 Request for Information (RFI) для получения недостающих сведений (например, адреса или дополнительных идентификаторов) в структурированном формате.

5.3 Обязательства в отношении трансграничных платежей и переводов

133. Пункты 8 и 9 Пояснительной записки к Рекомендации 16 определяют состав информации о плательщике и получателе, которая должна сопровождать трансграничные платежи и переводы. Государства вправе установить порог *de minimis*, не превышающий 1 000 долларов США/евро. В последующих разделах рассматриваются требования к информации, сопровождающей трансграничные платежи и переводы, а также возможные способы решения проблем, возникающих при реализации требований Рекомендации 16.

134. Передача и хранение отдельных категорий персональных данных, таких как адрес и дата рождения, могут создавать риски для защиты неприкосновенности частной жизни и персональных данных, если при обработке такой информации не соблюдаются надлежащие меры защиты. Рекомендации по обработке информации, предусмотренной Рекомендацией 16, в соответствии с принципами защиты неприкосновенности частной жизни и персональных данных приведены в главе 9.

Пороговые значения	
Ниже порогового значения	На уровне порога или выше
Платеж или перевод должны сопровождаться следующей информацией: (a) Имя (наименование) плательщика и получателя; и (b) Номер счета плательщика и получателя, если при проведении операции используется счет*. При отсутствии счета указывается уникальный идентификатор операции, позволяющий обеспечить ее прослеживаемость. Проверка достоверности указанной информации не требуется, за исключением случаев, когда имеются подозрения в ОД/ФТ. * Если средства списываются со счета, открытого	Платеж или перевод должны сопровождаться следующей информацией: (a) Имя (наименование) плательщика и получателя; (b) номер счета плательщика и получателя, если при проведении операции используется счет*. При отсутствии счета указывается уникальный идентификатор операции, позволяющий обеспечить ее прослеживаемость;

в финансовом учреждении, отличном от финансового учреждения плательщика, также должны быть указаны номер такого счета и наименование финансового учреждения, в котором открыт этот счет [сноски 50 и 51 Пояснительной записки к Рекомендации 16].	(с) Адрес плательщика³², а также страна и населенный пункт получателя (либо ближайший возможный аналог); (d) Дата рождения плательщика, если плательщик является физическим лицом (если полная дата рождения неизвестна, достаточно указать год рождения); и (е) При наличии - следующие сведения, если плательщик и (или) получатель являются юридическими лицами: (i) соответствующий идентификационный код юридического лица BIC, или (ii) идентификатор юридического лица LEI, или (iii) уникальный официальный идентификатор. Финансовое учреждение плательщика обязано проверить достоверность указанной выше информации о плательщике. Проверка достоверности информации о получателе не требуется. * Если средства списываются со счета, открытого в финансовом учреждении, отличном от финансового учреждения плательщика, также должны быть указаны номер такого счета и наименование финансового учреждения, в котором открыт этот счет.
--	---

Проверка достоверности информации при трансграничных переводах

135. В пункте 20 Пояснительной записки к Рекомендации 16 предусмотрено, что финансовое учреждение плательщика должно сопровождать трансграничные платежи и переводы, превышающие порог *de minimis*, обязательной и достоверной информацией о

³² См. сноску 52 к Пояснительной записке к Рекомендации 16: «При отсутствии стандартизированной информации о почтовом адресе плательщика достаточно указать страну и населенный пункт (либо ближайший возможный аналог)». Более подробно данный вопрос рассматривается в следующих пунктах.

плательщике, а также обязательной информацией о получателе. Согласно определению, приведенному в Глоссарии ФАТФ, под «достоверной» понимается информация, достоверность которой была проверена. Таким образом, при осуществлении трансграничных платежей и переводов, превышающих порог *de minimis*, информация о плательщике подлежит проверке на достоверность. При осуществлении трансграничных платежей и переводов ниже указанного порога такая проверка не требуется, за исключением случаев возникновения подозрений в ОД/ФТ.

136. Проверка, предусмотренная Рекомендацией 16, направлена на подтверждение достоверности информации. Она отличается от проверки, предусмотренной Рекомендацией 10 (надлежащая проверка клиента (CDD)), которая направлена на подтверждение личности клиента. Для проверки достоверности информации финансовые учреждения могут использовать надежные документы, данные или сведения, полученные из независимых источников. При этом объем проверочных мероприятий может различаться в зависимости от уровня риска. Вместе с тем термин «проверка достоверности», используемый в Рекомендации 16, не означает, что финансовое учреждение обязано заново проверять достоверность информации при каждом трансграничном платеже или переводе, превышающем порог *de minimis*. Например, если плательщик является действующим клиентом финансового учреждения, получение дополнительных сведений может не потребоваться. Финансовое учреждение плательщика вправе проверить информацию на основании уже имеющихся данных о клиенте и особенностях его поведения. Это особенно актуально в отношении клиентов с низким уровнем риска, к которым применяются упрощенные меры. Обязанность по проверке достоверности информации считается выполненной, если

- обязательная информация о плательщике соответствует сведениям, имеющимся у финансового учреждения о данном клиенте;
- у финансового учреждения имеются разумные основания считать такую информацию достоверной (в частности, на основании результатов постоянного мониторинга в рамках надлежащей проверки клиента); и
- информация представлена в корректном формате (например, указанный адрес не вызывает очевидных сомнений в его существовании).

Имя

137. Хотя сами по себе сведения об имени (наименовании) не позволяют устранить все случаи ложных срабатываний, они являются необходимой основой для целей ПОД/ФТ/ПРОМУ. Вместе с тем существующее разнообразие правил формирования имен (например, различный порядок указания имени и фамилии, составные родовые имена) усложняет обработку таких данных и повышает вероятность несовпадений при проверке по перечням целевых финансовых санкций или в ходе проверки данных. Например, для учета различий в написании имен или их транслитерации финансовые учреждения могут применять алгоритмы нечеткого сопоставления или внутренние процедуры проверки данных (например, проверку соответствия имени номеру счета).

138. Кроме того, финансовые учреждения могут устанавливать внутренние правила, определяющие порядок указания имен (наименований) в своих информационных системах, а также какое из них должно использоваться при осуществлении платежей. Как правило, такие сведения проверяются в рамках надлежащей проверки клиента и фиксируются следующим образом:

- Для клиентов-физических лиц - полное имя
- Для совместных счетов - имена (наименования) всех владельцев счета
- Для клиентов-юридических лиц - зарегистрированное наименование, коммерческое (фирменное) наименование или общепринятое сокращенное наименование

Номер счета

139. Номер счета, а при его отсутствии - уникальный идентификатор операции, позволяет проследить операцию. По уникальному идентификатору операции можно получить полную информацию о клиенте и операции. Использование в качестве такого идентификатора только даты и суммы операции недостаточно.³³

Адрес

140. Платежи и переводы, превышающие порог *de minimis*, сопровождаются информацией об адресе плательщика и получателя. Согласно Глоссарию ФАТФ, под адресом понимается физический адрес места жительства или места осуществления деятельности.

141. В отношении юридических лиц полезным ориентиром могут служить отраслевые рекомендации. Например, Комитет по банковскому надзору Базеля в своих рекомендациях³⁴ для банковского сектора рекомендует указывать адрес основного места осуществления деятельности. Информация об адресе должна быть достаточной для однозначного определения местонахождения в целях эффективной проверки по санкционным перечням и мониторинга в сфере ПОД/ФТ/ФРОМУ.

142. Стандарт обмена сообщениями ISO 20022 предусматривает передачу структурированных и детализированных данных. Согласно гармонизированным требованиям CPMI к данным ISO 20022 все организации и физические лица, участвующие в трансграничном платеже, указываются в стандартизированном и

³³ В небанковских сервисах, таких как сервисы электронных денег или мобильных денег, функцию номера банковского счета могут выполнять другие идентификаторы, например номер мобильного телефона, идентификатор электронного кошелька или иной соответствующий идентификатор, если они позволяют обеспечить аналогичную прослеживаемость. Дополнительные разъяснения приведены в главе 6.

³⁴ Рекомендации «Sound management of risks related to money laundering and financing of terrorism» («Надлежащее управление рисками, связанными с отмыванием денег и финансированием терроризма»), Комитет по банковскому надзору Базеля, январь 2014 г. (редакция от июля 2020 г.)

структурированном виде³⁵. При этом в соответствии с Рекомендацией 16 к информации об адресе плательщика и получателя предъявляются разные требования.

Адрес плательщика

- Стандартизированный почтовый адрес. По возможности он должен быть полностью структурирован. При отсутствии стандартизированного почтового адреса достаточно указать страну и населенный пункт (или ближайший возможный аналог).

Адрес получателя

- Название страны и города (или ближайший аналог).

143. В отдельных случаях, особенно в удаленных районах, сведения о населенном пункте могут отсутствовать. В таких случаях Рекомендация 16 допускает указание ближайшей возможной альтернативы - административно-территориальной единицы, например провинции, штата, региона или округа, в соответствии со стандартом ISO 3166-2. В сообщениях ISO 20022 поле, предназначенное для указания административно-территориальной единицы, является следующей структурированной альтернативой полю «Населенный пункт».

Вставка 3. Проверка адреса при отсутствии стандартной адресной системы

В отдельных случаях формальная или стандартизированная адресная система отсутствует, а физические лица могут проживать в сельской местности или неформальных поселениях, где невозможно указать структурированный почтовый адрес.

Плательщик может сообщить адрес, однако не иметь возможности подтвердить его достоверность надежными источниками информации из-за отсутствия структурированной адресной системы, ограниченного доступа к документам, подтверждающим адрес (например, счетам за коммунальные услуги или банковским выпискам), либо иных ограничений, связанных с ведением государственных и административных реестров.

Компетентным органам и финансовым учреждениям следует четко разграничивать ситуации, когда плательщик:

- не имеет структурированного или официально зарегистрированного адреса; и тех, в которых он
- имеет адрес, но не располагает документами, подтверждающими его.

Если клиент не может предоставить структурированный адрес, финансовое учреждение может использовать альтернативные способы определения соответствующего населенного пункта, страны или ближайшей административно-территориальной единицы.

³⁵ Требования к данным 9 и 10: [Обновленный доклад: Гармонизированные требования к данным ISO 20022 для совершенствования трансграничных платежей](#)

Если плательщик может сообщить сведения об адресе, но не имеет возможности подтвердить их надежными источниками информации, это само по себе не препятствует соблюдению требований Рекомендации 16 при условии применения и документирования разумных альтернативных способов проверки.

Компетентным органам следует предоставить разъяснения, предусматривающие, что:

- Отсутствие традиционных документов, подтверждающих адрес, само по себе не является основанием для отказа в проведении платежа, если могут быть использованы альтернативные способы проверки.
- Требования к проверке должны учитывать практические условия осуществления деятельности и не приводить к установлению избыточных требований, препятствующих финансовой доступности или создающих необоснованные сложности при осуществлении платежей.
- Финансовым учреждениям получателя не следует систематически отклонять платежи исключительно потому, что адрес был подтвержден с использованием альтернативных способов проверки, если переданная информация является полной и соответствует требованиям Рекомендации 16.

К альтернативным способам проверки могут относиться:

- Подтверждение адреса местным агентом, представителем сообщества или органом местного самоуправления на основании имеющихся у них сведений или подтверждающих материалов.
- Сверка с административными реестрами местного уровня (например, реестрами населенных пунктов или сельских поселений), если содержащиеся в них сведения могут быть надежно соотнесены с конкретным населенным пунктом или административно-территориальной единицей.
- Использование описательного или неструктурированного адреса (например, «желтый дом рядом с рынком»), если такое описание позволяет определить конкретный населенный пункт или административно-территориальную единицу и может быть подтверждено на основе местных сведений.
- Использование информации, полученной при регистрации SIM-карты или абонентского номера мобильной связи, если она позволяет надежно установить связь с определенным местом или сообществом. Такая информация может использоваться в качестве дополнительного средства проверки, но не заменяет сведения об адресе, подлежащие включению в платежное сообщение.
- Заявление о месте жительства, удостоверенное уполномоченным органом, если официальные документы отсутствуют.
- Государственные системы цифровой идентификации или биометрические базы данных, если они позволяют финансовому учреждению подтвердить зарегистрированное место нахождения клиента.

- Данные геолокации или сведения о местоположении устройства (например, местоположение мобильного устройства при установлении деловых отношений или инициировании операции). Такие данные могут использоваться как дополнительное средство проверки адреса, населенного пункта или иной местности, указанных плательщиком, если документальное подтверждение адреса отсутствует. Они позволяют оценить достоверность и согласованность сведений об адресе, но не заменяют обязанность указывать адрес в платежном сообщении в соответствии с требованиями Рекомендации 16.
- Инструменты на основе искусственного интеллекта, позволяющие определить ближайший соответствующий населенный пункт и страну на основе неструктурированных либо устаревших данных об адресе.

Во всех перечисленных случаях финансовым учреждениям следует применять риск-ориентированный подход, используя упрощенные способы проверки при низком уровне риска и небольшой сумме операции, а при повышенном уровне риска - усиленные меры проверки.

Дата рождения

144. При осуществлении платежей и переводов, превышающих порог *de minimis*, финансовое учреждение плательщика обязано указывать дату рождения плательщика, если плательщиком является физическое лицо. Если полная дата рождения неизвестна, достаточно указать только год рождения. Указывать дату рождения получателя не требуется. Финансовое учреждение плательщика обязано обеспечить достоверность включаемых в платежное сообщение сведений о дате рождения плательщика.

145. Указание места рождения Рекомендацией 16 не предусмотрено, поскольку в отдельных случаях, в частности в странах с ограниченными ресурсами, достоверность таких сведений сложно проверить. В связи с этим Рекомендация 16 требует указывать только дату рождения. Вместе с тем для реализации этого подхода потребуется внести изменения в стандарт ISO 20022, который в настоящее время требует указывать одновременно дату и место рождения.

146. При проверке даты рождения лиц в условиях нестабильности или в странах с ограниченными ресурсами следует применять риск-ориентированный подход и использовать разумные способы проверки. При этом меры проверки не должны создавать необоснованных препятствий для доступа к финансовым услугам. Для платежей и переводов ниже порога *de minimis* проверка достоверности сведений о плательщике не требуется, если только операция не связана с рисками ОД/ФТ.

Вставка 4. - Проверка даты рождения при отсутствии подтверждающих документов

В отдельных случаях сведения в полном объеме о регистрации рождения могут отсутствовать. Если полные сведения о регистрации рождения отсутствуют, может использоваться год рождения. Если документально подтвердить год рождения невозможно, регуляторам

рекомендуется применять альтернативные способы идентификации и проверки, например проведение собеседований, подтверждение сведений на уровне местного сообщества либо сопоставление с имеющимися административными или регистрационными данными о населении. Такие способы позволяют установить или подтвердить год рождения в случаях, когда использование традиционных официальных документов невозможно или существенно затруднено.

На практике могут применяться, в частности, следующие подходы:

- Подтверждение сведений о возрасте местными представителями или уполномоченными лицами, располагающими соответствующей информацией, с учетом имеющихся подтверждающих материалов.
- Заявления под присягой, данные в присутствии уполномоченного органа, если официальные документы отсутствуют.
- использование цифровых удостоверений личности или биометрических систем, если они позволяют достоверно установить связь между лицом и содержащимися в государственных либо административных реестрах сведениями о возрасте.
- Применение упрощенных процедур проверки при проведении низкорисковых операций на небольшие суммы и более тщательной проверки в случаях повышенного риска.

Идентификатор юридического лица

147. Если плательщиком и (или) получателем является юридическое лицо, финансовое учреждение плательщика должно включать в платежное сообщение, сопровождающее платеж или перевод, превышающий порог *de minimis*, по крайней мере один из следующих идентификаторов (при его наличии):

- i) идентификационный код юридического лица (BIC) или
- ii) идентификатор юридического лица (LEI), или
- iii) уникальный официальный идентификатор

148. В целях эффективной и надежной идентификации плательщика и получателя финансовым учреждениям рекомендуется использовать идентификатор юридического лица (LEI). LEI представляет собой широко признанный общедоступный идентификатор, разработанный на основе стандарта ISO. Он содержит стандартизированные справочные сведения о юридических лицах, используемые на международном уровне, что способствует повышению эффективности проверки и мониторинга. В отличие от LEI, использование уникального официального идентификатора не всегда позволяет получить доступ к стандартизированным данным, и такие данные могут быть недоступны для публичного использования.

149. В Рекомендации 16 под *уникальным официальным идентификатором* понимается идентификатор, присваиваемый государственным органом в рамках официальной системы идентификации, которая обеспечивает однозначное соответствие между идентификатором и юридическим лицом: каждому юридическому лицу

соответствует только один идентификатор, а каждый идентификатор относится только к одному юридическому лицу. Наиболее распространенным примером такого идентификатора является идентификационный номер налогоплательщика (ИНН).

150. Если в одной юрисдикции используется несколько систем идентификации, государственным органам рекомендуется отдавать предпочтение тем из них, которые обеспечивают надежность и доступность идентификаторов. При необходимости такие системы должны также обеспечивать доступ к справочным данным, необходимым для проверки идентификаторов, в том числе при трансграничных платежах и переводах.

151. Формулировка *«если такой идентификатор существует»*, используемая в пункте 9 Пояснительной записки к Рекомендации 16, означает, что отсутствие идентификатора юридического лица не может служить основанием для отказа в проведении платежа. Финансовое учреждение плательщика обязано указать такой идентификатор, если ему стало известно о его наличии, даже если ранее он не был получен этим финансовым учреждением. Обязанность по предоставлению сведений о получателе в первую очередь возлагается на плательщика. Если сведения об идентификаторе получателя ранее отсутствовали, финансовому учреждению плательщика рекомендуется уточнить у плательщика, присвоен ли получателю такой идентификатор. При этом финансовое учреждение плательщика не обязано проверять достоверность сведений о получателе.

152. Для платежей и переводов, превышающих порог *de minimis*, финансовое учреждение плательщика обязано проверить достоверность связанных с плательщиком BIC, LEI или уникального официального идентификатора. Такая проверка может проводиться при установлении деловых отношений с клиентом, в рамках проведения надлежащей проверки клиента или при осуществлении платежа либо перевода. Для этих целей могут использоваться общедоступные официальные источники информации, например система LEI.

Вставка 5. - Использование идентификаторов юридических лиц

Использование идентификаторов LEI пока остается ограниченным, а связанными BIC располагает лишь небольшое число организаций. В данном контексте под «связанными» BIC понимаются BIC, используемые в качестве опубликованных международных стандартизированных идентификаторов (ISO 9362), которые могут быть проверены на всех этапах платежной цепочки.

Некоторые категории организаций, например общественные объединения, ассоциации и неформальные клубы, могут не иметь какого-либо официального идентификатора юридического лица. Учитывая, что такие идентификаторы доступны не для всех юридических лиц, Пояснительная записка к Рекомендации 16 допускает использование более распространенных уникальных официальных идентификаторов (например, ИНН) в качестве эквивалента LEI или BIC. Настоящее Руководство дополнительно разъясняет, что отсутствие таких идентификаторов само по себе не должно служить основанием для отказа в проведении

платежа. В соответствии со Стандартами ФАТФ, касающимися прозрачности юридических лиц и юридических образований (Рекомендации 24 и 25), при наличии таких идентификаторов они должны быть получены и включены юридическим лицом или юридическим образованием в состав базовой информации о себе.

ФАТФ рекомендует государственным органам расширять доступ к национальным системам идентификации и, где это возможно, обеспечивать возможность проверки выданных идентификаторов. При внедрении требований об использовании идентификаторов таким образом, чтобы они не ограничивали доступ к финансовым услугам, государства с ограниченными ресурсами и финансовые учреждения, осуществляющие деятельность в таких государствах, могут применять эти требования с учетом признания эквивалентных региональных идентификаторов (например, African Entity Identifier), если уровень финансирования, цифровизации и развития инфраструктуры связи позволяет обеспечить разумный доступ к таким идентификаторам. Финансовым учреждениям рекомендуется учитывать такую гибкость в своих внутренних политиках, в том числе применяемых на уровне группы компаний.

5.4 Внутренние переводы

153. Обновленная Рекомендация 16 сохраняет действующие минимальные требования к внутренним платежам и переводам, устанавливая порог *de minimis* в размере не более 1 000 долларов США/евро как для внутренних, так и для трансграничных платежей и переводов. Такой подход позволяет применять требования соразмерно уровню риска и без излишней нагрузки на участников платежей.

154. При регулировании внутренних платежей и переводов Рекомендация 16 исходит из принципа соразмерности и устанавливает для финансовых учреждений ограниченный круг обязанностей. При осуществлении внутренних платежей и переводов финансовое учреждение плательщика не обязано включать в платежное сообщение сведения о получателе. Вместе с тем включение в платежное сообщение обязательной информации о плательщике имеет ключевое значение для прозрачности внутренних платежей и переводов, поскольку номер счета плательщика либо уникальный номер операции позволяют однозначно установить связь операции с плательщиком или получателем.

В таблице ниже представлен обзор требований Рекомендации 16 в отношении внутренних платежей и переводов.

	Пороговое значение	
	Ниже порога	На уровне порога или выше
Упрощенные требования (при условии, что соответствующая информация о плательщике может быть предоставлена иным способом в течение трех рабочих дней)	Платеж или перевод должны сопровождаться номером счета плательщика либо уникальным номером операции, обеспечивающими возможность проследить операцию.	
Если указанные выше условия не соблюдаются (то есть если информация о плательщике не может быть предоставлена иным способом в течение трех рабочих дней)	Платеж или перевод должны сопровождаться следующей информацией о плательщике: (a) Имя (наименование); и (b) Номер счета либо уникальный номер операции, позволяющий проследить операцию Проверка достоверности указанной информации не требуется, если отсутствуют подозрения в ОД/ФТ	Платеж или перевод должны сопровождаться следующей информацией о плательщике: (a) Имя (наименование); (b) Номер счета, если при осуществлении операции используется счет. При отсутствии счета - уникальный номер операции, позволяющий проследить операцию; (c) Адрес; (d) Дата рождения плательщика, если плательщиком является физическое лицо (если полная дата рождения отсутствует, указывается только год рождения); и (e) При наличии и если плательщиком является юридическое лицо - следующая информация: (i) связанный идентификационный код юридического лица (BIC), или (ii) идентификатор

		юридического лица (LEI), или (iii) уникальный официальный идентификатор. Финансовое учреждение плательщика обязано проверить достоверность указанной информации.
--	--	--

Внутренние платежи и переводы, по которым обязательная информация может быть предоставлена иным способом (при любой сумме перевода)

155. Указанный выше упрощенный режим применяется, если финансовое учреждение плательщика может предоставить информацию о плательщике иным способом в течение трех рабочих дней с момента получения соответствующего запроса от финансового учреждения-посредника, финансового учреждения получателя либо компетентного органа. В этом случае в платежное сообщение достаточно включить только номер счета плательщика либо уникальный номер операции. К числу таких способов относятся, например, централизованные базы данных об операциях, создаваемые платежными инфраструктурами (например, национальными платежными коммутаторами или клиринговыми системами), каналы обмена информацией между финансовыми учреждениями, а также предусмотренные законодательством механизмы оперативного обмена данными между финансовыми учреждениями.

156. Хотя Рекомендация 16 не устанавливает, в какой именно момент финансовое учреждение плательщика должно собирать или хранить полную информацию о плательщике, оно в любом случае должно иметь возможность предоставить такую информацию по запросу в течение трех рабочих дней.

5.5 Виртуальные номера счетов

Общая информация

157. Виртуальный номер счета (например, виртуальный IBAN (vIBAN)) ³⁶ представляет собой идентификатор счета, используемый в качестве псевдонима и связанный с основным банковским счетом, которому присвоен другой номер (идентификатор) счета (например, IBAN). Таким образом, одному банковскому счету может соответствовать несколько различных идентификаторов. Так, например, виртуальный номер vIBAN имеет тот же формат, что и стандартный IBAN (начинается с

³⁶ Согласно новому Регламенту ЕС о противодействии легализации (отмыванию) преступных доходов, виртуальный IBAN (vIBAN) определяется как идентификатор, при использовании которого платеж перенаправляется на платежный счет, имеющий иной IBAN (статья 2(1)(26) Регламента (ЕС) 2024/1624 (AMLR)).

двухбуквенного кода страны и контрольных разрядов, однако при этом связан с основным счетом).³⁷

158. Виртуальные номера счетов широко используются для упрощения обработки платежей, а также для идентификации и сверки поступающих средств в рамках структур с объединенными (пуловыми) или omnibusными счетами. Например, торгово-сервисное предприятие может присвоить каждому покупателю уникальный виртуальный номер счета. В этом случае при поступлении платежа оно сразу определяет, в счет какой задолженности (какого счета на оплату) поступили средства. После этого платеж, направленный на виртуальный номер счета, автоматически зачисляется на основной счет.

159. Хотя некоторые эмитенты виртуальных номеров счетов используют специальные признаки, позволяющие отличить их от обычных номеров счетов, в большинстве случаев другие финансовые учреждения не могут определить, является ли тот или иной номер счета виртуальным. При этом финансовое учреждение, обслуживающее счет, может не являться эмитентом виртуальных номеров счетов.

Риски для прозрачности платежей

160. В большинстве случаев виртуальные номера счетов используются в законных целях и способствуют повышению эффективности обработки платежей, сверки поступающих средств и управления счетами. Кроме того, их использование может стимулировать развитие инноваций в сфере платежей. Вместе с тем применение виртуальных номеров счетов может создавать риски ОД/ФТ/ФРОМУ, поскольку не всегда позволяет определить, какое финансовое учреждение обслуживает счет плательщика или получателя и в какой стране оно находится³⁸. Степень риска зависит от конкретной ситуации и может возрастать, если использование виртуального номера счета не позволяет соответствующим финансовым учреждениям или компетентным органам определить, какое финансовое учреждение обслуживает счет плательщика или получателя и в какой стране оно находится. Рекомендация 16 не требует включения информации о стране в состав любых номеров счетов и не запрещает правомерное использование виртуальных номеров счетов, включая vIBAN. Вместе с тем идентификатор счета (в том числе виртуальный номер счета) не должен затруднять определение:

³⁷ Следует отметить, что единое общепринятое определение понятия «основной счет» отсутствует. Вместе с тем под основным счетом, как правило, понимается счет, на который зачисляются платежи, направленные с использованием виртуальных счетов.

³⁸ При осуществлении выплат с виртуального счета (исходящие платежи) финансовое учреждение плательщика осведомлено о том, что перевод является трансграничным, и обязано соблюдать требования Рекомендации 16, включая передачу необходимой информации. Настоящее Руководство посвящено выполнению соответствующих требований в случаях, когда виртуальный номер счета используется на стороне получателя платежа или перевода.

- финансового учреждения, обслуживающего счет плательщика или получателя, и
- страны, в которой находится такое финансовое учреждение.

161. С точки зрения Рекомендации 16 финансовое учреждение плательщика, располагая только виртуальным номером счета и при отсутствии иной информации или дополнительных механизмов, не всегда может определить, какое финансовое учреждение обслуживает счет получателя и в какой стране оно находится. Это затрудняет определение финансового учреждения, обслуживающего счет получателя, и юрисдикции, в которой оно находится. В результате финансовые учреждения и компетентные органы могут быть лишены возможности применять меры ПОД/ФТ/ФРОМУ, соответствующие фактическому характеру операции. Поэтому возможность определить, какие страны участвуют в переводе, имеет ключевое значение для установления того, является ли перевод внутренним или трансграничным в контексте Рекомендации 16.

Требования к прозрачности платежей

162. Рекомендация 16 предусматривает следующее: *«Информация, содержащаяся в платежном сообщении, должна позволять всем финансовым учреждениям и компетентным органам [...] определить, какое финансовое учреждение обслуживает счет плательщика и счет получателя соответственно, а также в каких странах находятся такие финансовые учреждения. Использование номеров счетов не должно препятствовать определению страны, в которой находится финансовое учреждение, обслуживающее соответствующий счет».*

163. Требование Рекомендации 16 носит рамочный характер. Его цель не заключается в запрете или ограничении использования виртуальных счетов, а также во включении информации о стране в состав любых номеров счетов. Рекомендация 16 не устанавливает конкретных способов выполнения этого требования, однако предусматривает наличие механизмов, позволяющих определить финансовое учреждение, обслуживающее счет плательщика или получателя, и страну, в которой оно находится, даже при использовании виртуального номера счета.

- (1) Настоящее Руководство содержит исчерпывающий перечень мер, направленных на снижение риска использования виртуальных номеров счетов способами, препятствующими выполнению требований Рекомендации 16. Поскольку финансовые учреждения плательщика и финансовые учреждения-посредники не могут отличить виртуальные номера счетов от обычных номеров счетов, для соблюдения требований Рекомендации 16 могут применяться одна или несколько из приведенных ниже мер. **Включение дополнительной информации в платежное сообщение.** Финансовое учреждение плательщика должно заполнять соответствующие поля платежного сообщения таким образом, чтобы можно было однозначно определить финансовое учреждение получателя, и страну, в которой оно находится. Вместе с тем финансовому учреждению плательщика неизвестно, используется ли при совершении платежа виртуальный номер счета. Поэтому прозрачность платежей должна начинаться с финансового учреждения,

выпускающего виртуальные номера счетов. Такое финансовое учреждение должно требовать от своих клиентов указывать в счетах на оплату или платежных инструкциях необходимую информацию, в частности сведения о фактическом владельце счета и финансовом учреждении, обслуживающем основной счет.

На практике для этого может использоваться платежное сообщение стандарта ISO 20022, позволяющее разграничить организацию, на имя которой открыт счет, и лицо, в интересах которого она действует.

Вставка 6. – Пример

Агент по приему платежей (например, маркетплейс) предоставляет виртуальный номер счета (например, vIBAN) для приема средств в пользу продавцов.

При инициировании перевода плательщик поручает финансовому учреждению перевести средства получателю (агенту по приему платежей), который принимает их в пользу конечного кредитора (продавца). В платежном сообщении финансовое учреждение плательщика может указать в качестве получателя (кредитора) агента по приему платежей, а в поле «Конечный кредитор» (*Ultimate Creditor*) - продавца, в интересах которого действует получатель (кредитор), с указанием соответствующего идентификатора (например, LEI или национального идентификатора) и адресной информации.

Виртуальные номера счетов могут использоваться и на стороне плательщика. Если плательщик использует виртуальный номер счета, связанный с основным счетом (например, vIBAN, предоставленный небанковским финансовым учреждением, корпоративным казначейским центром или в рамках иной аналогичной схемы), платежное сообщение должно содержать информацию, позволяющую однозначно определить лицо, в интересах которого осуществляется списание средств со счета. В таких случаях финансовое учреждение плательщика должно указывать в поле «Конечный дебитор» (*Ultimate Debtor*) сведения о фактическом плательщике (то есть лице, которому в конечном итоге принадлежат средства или которое осуществляет над ними контроль). Это позволяет определить, какое финансовое учреждение обслуживает счет плательщика и в какой стране оно находится.

- (2) **Роль финансового учреждения, выпускающего виртуальные номера счетов, в повышении прозрачности платежей.** Одним из возможных решений является рассмотрение виртуального номера счета в качестве самостоятельного номера счета с функцией перенаправления платежей. В этом случае виртуальный номер счета используется для перенаправления средств в финансовое учреждение, отличное от того, в котором открыт счет, на который фактически зачисляются средства. Хотя такой подход не устраняет риски, связанные с перенаправлением платежей, он позволяет избежать ситуации, при которой третьи лица, включая компетентные органы, неверно определяют финансовое учреждение, обслуживающее соответствующий счет, и страну его нахождения.

Данный подход может применяться в сочетании с мерами, реализуемыми

финансовым учреждением, выпускающим виртуальные номера счетов. На финансовое учреждение, выпускающее виртуальные номера счетов, возлагается обязанность поддерживать прозрачность операций с их использованием. Финансовым учреждениям, выпускающим виртуальные номера счетов, рекомендуется (i) выпускать виртуальные номера счетов только при наличии четко определенной и документально подтвержденной законной цели их использования; (ii) идентифицировать пользователя виртуального номера счета, а не только владельца основного счета; (iii) осуществлять мониторинг операций на уровне каждого виртуального номера счета, а не только на уровне основного счета; и (iv) если организация предоставляет виртуальные номера счетов своим клиентам, предусматривать в договоре с такой организацией ее обязанность по запросу собирать и предоставлять информацию о пользователе соответствующего виртуального номера счета. Это позволит финансовым учреждениям плательщика корректно заполнять платежные сообщения, а финансовым учреждениям получателя и компетентным органам - определять фактический характер операции.

- (3) **Риск-ориентированные меры, применяемые финансовым учреждением, выпускающим виртуальные номера счетов.** Настоящие рекомендации относятся исключительно к финансовому учреждению, выпускающему виртуальные номера счетов, и не распространяются на финансовое учреждение плательщика или финансовое учреждение-посредник. Финансовому учреждению, выпускающему виртуальные номера счетов, следует применять риск-ориентированный подход при оказании соответствующих услуг, в том числе проводить оценку рисков ОД/ФТ, связанных с такими услугами, до начала их оказания и внедрять соразмерные меры по снижению выявленных рисков. Такое финансовое учреждение также должно на постоянной основе осуществлять мониторинг использования виртуальных номеров счетов, чтобы удостовериться, что оно соответствует цели, определенной при установлении деловых отношений, и при выявлении отклонений принимать соответствующие меры с учетом уровня риска.

164. Изменения соответствующих стандартов также могут способствовать повышению прозрачности использования виртуальных номеров счетов. Например, виртуальным номерам счетов может присваиваться специальный префикс, указывающий на то, что номер счета, указанный в платежном сообщении, является виртуальным. Вместе с тем реализация такой меры возможна только после внесения соответствующих изменений в указанные стандарты.

Вставка 7.

Пример из практики 1 - Повышение прозрачности vIBAN

В настоящее время кредитные организации Германии обязаны безотлагательно, точно и в полном объеме вносить сведения о каждом виртуальном IBAN, выданном небанковскому финансовому учреждению, в соответствующий реестр. При этом финансовое учреждение должно быть указано в качестве владельца счета, а соответствующий конечный клиент либо

конечный бенефициарный владелец-физическое лицо - в качестве уполномоченного пользователя или бенефициарного владельца.

Источник: Германия.

Пример из практики 2 - Поставщик услуг в сфере криптоактивов (CASP)

CASP принимает от своих клиентов платежи в фиатной валюте для их последующей конвертации в криптоактивы. Такие платежи поступают на основной счет, открытый на имя CASP в финансовом учреждении, обслуживающем счет. Для каждого клиента используется отдельный виртуальный IBAN, что позволяет CASP корректно идентифицировать и учитывать поступающие для конвертации средства. Надлежащей практикой является указание CASP в качестве получателя в платежном сообщении, а клиента - в качестве «конечного кредитора» (Ultimate Creditor) (в форматах SWIFT gpi или pacs.008). Реестры виртуальных IBAN позволяют установить связь между виртуальным IBAN и основным счетом.

Источник: Франция

5.6 Сноски об источнике средств

5.6.1 Цель и обоснование политики

165. Сноски 50 и 51 направлены на устранение специфического риска, возникающего в случаях, когда клиент направляет платеж через финансовое учреждение, с которым у него отсутствуют постоянные деловые отношения, а средства для совершения операции в разовом порядке привлекаются со счета, открытого в другом финансовом учреждении. В таких случаях в платежном сообщении отсутствует информация о финансовом учреждении, в котором фактически находятся средства, используемые для совершения платежа. Это может снижать эффективность риск-ориентированных мер контроля и затруднять получение информации о плательщике. Сноски предусматривают включение в платежное сообщение информации об источнике средств (в частности, номера счета и наименования финансового учреждения), чтобы всегда можно было определить финансовое учреждение, которое поддерживает с плательщиком постоянные отношения и располагает информацией, полученной в рамках надлежащей проверки клиента.

5.6.2 Сфера применения

166. Сноски 50 и 51 применяются к трансграничным платежам и переводам независимо от того, превышает ли сумма операции порог *de minimis*, при одновременном соблюдении следующих условий:

- (1) Финансовое учреждение плательщика не поддерживает с плательщиком постоянные деловые отношения, предусматривающие возможность хранения средств (например, на счете или в электронном кошельке). И

(2) По платежному распоряжению плательщика трансграничный перевод осуществляется путем списания средств со счета, открытого в финансовом учреждении, отличном от финансового учреждения плательщика, либо с использованием платежной карты.

167. Вышеупомянутые сноски не применяются, если операция осуществляется за счет наличных денежных средств.

168. Если плательщик ранее внес денежные средства на счет, открытый в финансовом учреждении плательщика, и последующие трансграничные переводы осуществляются с этого счета, сноски также не применяются.

5.6.3 Требования к информации, включаемой в платежное сообщение

169. В случаях, когда применяются сноски 50 и 51, платежное сообщение должно содержать дополнительную информацию, позволяющую определить счет, с которого списываются средства, а именно:

- номер счета, с которого списываются средства; и
- наименование финансового учреждения, обслуживающего этот счет.

170. В случаях, когда сноски 50 и 51 применяются к операциям, совершаемым с использованием платежных карт, в платежном сообщении вместо номера счета, с которого списываются средства, указывается номер платежной карты (то есть основной номер счета (Primary Account Number, PAN)), а также наименование финансового учреждения-эмитента.

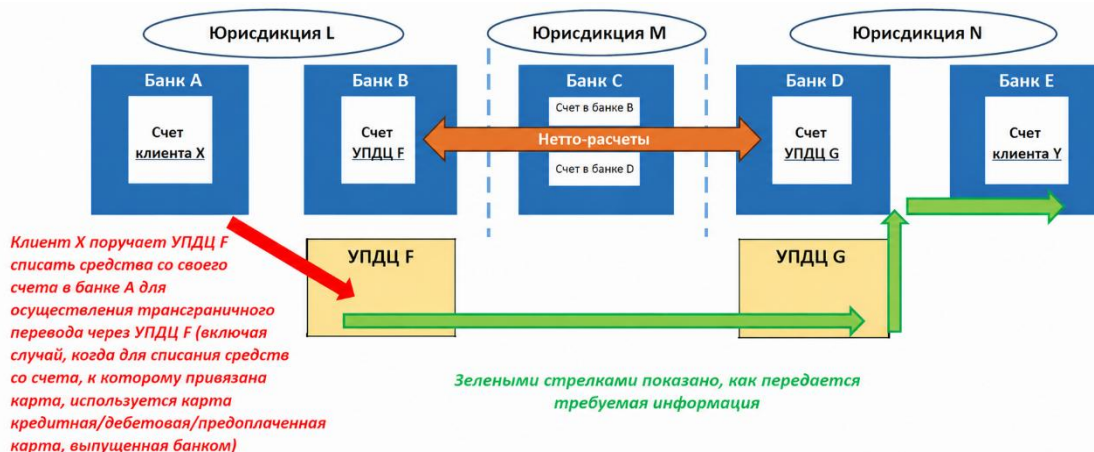
171. На практике информацию, предусмотренную сносками, финансовое учреждение, инициирующее платеж, получает от плательщика при получении платежного распоряжения на осуществление платежа или перевода. Если операция осуществляется с использованием платежной карты, сведения о финансовом учреждении-эмитенте карты передаются финансовому учреждению, инициирующему платеж, через карточную платежную систему.

5.6.4 Пример

172. Сноски регулируют особый случай, когда платеж направляется через финансовое учреждение, клиентом которого плательщик не является. Такая ситуация может возникать, в частности, в деятельности операторов УПДЦ, поставщиков цифровых кошельков и эмитентов электронных денежных средств, особенно при осуществлении разовых трансграничных операций или предоставлении клиентам транзитных счетов.

- Клиент X не имеет счета у оператора УПДЦ F и поручает ему списать необходимые для осуществления трансграничного перевода средства со своего счета, открытого в банке А.
- В данном случае средства списываются со счета, открытого в банке А, по поручению клиента X, направленному оператору УПДЦ F. Поскольку оператор УПДЦ F, получивший платежное распоряжение, и банк А, в котором открыт счет, с которого списываются средства, не совпадают, применяются сноски 50 и 51.

- Оператор УПДЦ F должен определить, в каких случаях в платежное сообщение необходимо включить дополнительную информацию, а именно номер счета, с которого списываются средства, и наименование банка А, в котором открыт этот счет.



173. Одним из возможных способов передачи информации, предусмотренной сносками 50 и 51, в платежном сообщении может стать доработка стандарта ISO 20022 путем введения отдельного поля (например, «Финансовое учреждение - источник средств»). Такое поле позволит финансовым учреждениям-посредникам и финансовым учреждениям получателя, когда это применимо, определить финансовое учреждение, со счета в котором списываются средства.

Случаи, когда средства списываются со счета, открытого в финансовом учреждении, находящемся в третьей юрисдикции

174. Если средства списываются со счета, открытого в финансовом учреждении, находящемся в юрисдикции, отличной от юрисдикции финансового учреждения, инициирующего платеж (например, со счета в финансовом учреждении, расположенном в третьей юрисдикции, на основании распоряжения, представленного УПДЦ F в юрисдикции L), финансовому учреждению, инициирующему платеж (УПДЦ F), следует применять соответствующие риск-ориентированные меры (например, мониторинг операций) для снижения рисков ОД/ФТ, связанных с источником средств, в том числе в случаях, когда сноски не применяются (например, при внутренних переводах).

Вставка 8.

Пример применения сносок об источнике средств при пополнении счета с использованием платежной карты

Ниже приведен пример ситуации, в которой сноски 50 и 51 применяются при пополнении счета с использованием платежной карты:

Платежное поручение

- УПДЦ F получает платежное распоряжение от разового клиента - плательщика X, находящегося в юрисдикции L, о переводе средств на счет получателя Y, открытый в юрисдикции N.
- В платежном распоряжении клиент X указывает, что трансграничный перевод должен быть осуществлен путем списания средств с кредитной карты.

Информация, которую УПДЦ F должен передать по платежной цепочке

- информация о плательщике и получателе, предусмотренная для трансграничного перевода, а также
- номер платежной карты и наименование финансового учреждения -
- эмитента карты

Применение понятия платежной цепочки в контексте главы 4

Пополнение счета кредитной, дебетовой или prepaid картой представляет собой перевод средств на счет, электронный кошелек или иной платежный инструмент. Для целей Рекомендации 16 такая операция рассматривается как платеж или перевод и представляет собой P2P-перевод между физическими лицами, а не оплату товаров или услуг (подробная информация приведена в главе 6).

Платежная цепочка начинается с платежного распоряжения плательщика. В отдельных случаях, когда финансовое учреждение, инициирующее платеж, не поддерживает с плательщиком постоянных деловых отношений, в платежное сообщение должна включаться дополнительная информация, включая сведения об источнике средств.

В рассматриваемом примере формируются две платежные цепочки.

Цепочка 1 - пополнение счета платежной картой

- Начальным участником является банк А - эмитент платежной карты. Банк А выступает финансовым учреждением, инициирующим платеж, на этапе пополнения счета с использованием платежной карты, поскольку получает от финансового учреждения-эквайера запрос на авторизацию операции, отражающий намерение плательщика перевести средства в пользу УПДЦ F.
- Информация о плательщике и получателе³⁹, предусмотренная для данной операции, должна передаваться по всей платежной цепочке от банка А до УПДЦ F.

Цепочка 2 - трансграничный перевод, инициированный УПДЦ F

- Начальным участником является УПДЦ F. УПДЦ F выступает финансовым учреждением, инициирующим платеж, при последующем трансграничном переводе, поскольку получает платежное распоряжение. Финансовым учреждением-посредником

³⁹ Состав передаваемой информации зависит от того, является ли перевод внутренним или трансграничным.

является УПДЦ G, а финансовым учреждением получателя - банк E, который является конечной точкой платежной цепочки.

- По платежной цепочке от УПДЦ F до банка E должны передаваться информация о плательщике и получателе, а также сведения, предусмотренные сносками 50 и 51.

5.7 Вопросы финансовой доступности, связанные с применением порога *de minimis*

175. Изменение или расширение состава платежной информации не должно создавать необоснованных препятствий для доступа к финансовым услугам. Если предоставление или подтверждение такой информации затруднено либо связано с чрезмерными затратами, отдельные лица могут оказаться исключенными из сферы финансовых услуг. Это может привести к усилению финансовой изоляции и, как следствие, повышению рисков ОД/ФТ/ФРОМУ, что противоречит целям политики ФАТФ и «Группы двадцати».

176. До пересмотра Рекомендации 16 в 2025 году в ней содержалось следующее положение: «Страны вправе устанавливать требование о том, чтобы входящие трансграничные электронные переводы на сумму ниже порогового значения сопровождалась необходимой и достоверной информацией о плательщике». При пересмотре Рекомендации 16 это положение было исключено. Его сохранение могло привести к установлению требований, выходящих за рамки Стандартов ФАТФ. В действующей редакции Рекомендации 16 для переводов средств на сумму ниже порога *de minimis* предусмотрен упрощенный режим передачи информации. Такой подход распространяется на широкий круг платежей. Например, подавляющее большинство операций, совершаемых через системы мгновенных платежей, подпадает под упрощенные требования. Применение порога *de minimis* способствует повышению финансовой доступности. Кроме того, оно снижает риск исключения отдельных категорий пользователей из сферы финансовых услуг, что соответствует целям ФАТФ и «Группы двадцати».

177. На практике применение разных порогов *de minimis* в различных юрисдикциях создает для финансовых учреждений существенные операционные сложности. Так, если в одной юрисдикции установлен порог в размере 500 долларов США, а в другой - 1 000 долларов США, при осуществлении трансграничного перевода по платежной цепочке может передаваться неполная информация. В результате финансовым учреждениям приходится запрашивать дополнительные сведения, что может приводить к задержкам при обработке платежей или даже к отказу в проведении операции.

178. Для минимизации указанных проблем юрисдикциям рекомендуется по возможности согласовывать порог *de minimis* с другими юрисдикциями, особенно в рамках основных платежных коридоров. Соответствующие положения рекомендуется закреплять в национальном законодательстве. Если согласовать размер порога невозможно, государственным органам следует обеспечить открытость и доступность информации о применяемом пороге. Кроме того, рекомендуется предложить финансовым учреждениям практические решения для организации необходимых

процедур контроля и оценивать эффективность выбранного подхода, включая его возможное влияние на риск исключения отдельных категорий пользователей из сферы финансовых услуг. При отсутствии гармонизации финансовым учреждениям следует руководствоваться наиболее строгими из потенциально применимых требований.

Вставка 9. Применение порога *de minimis*

Установление порога *de minimis* позволяет применять упрощенный режим передачи информации при осуществлении платежей или переводов на небольшие суммы (например, денежных переводов физических лиц). Такой подход способствует расширению доступа к официальным платежным услугам и их более широкому использованию, в том числе за счет снижения стоимости таких операций. Применение порога *de minimis* помогает соблюсти баланс между задачами повышения финансовой доступности и целями в области ПОД/ФТ. ФАТФ настоятельно рекомендует странам рассмотреть возможность его применения с учетом риск-ориентированного подхода.

При определении порога *de minimis* рекомендуется учитывать следующие аспекты:

1. Различия в размере порога *de minimis*, применяемого в разных юрисдикциях, существенно затрудняют применение Рекомендации 16. Поэтому ФАТФ рекомендует странам взаимодействовать друг с другом, прежде всего в рамках основных платежных коридоров, в целях:
 - а. согласования подходов к определению порога, включая возможность его установления на максимальном уровне, предусмотренном Рекомендацией 16, - 1 000 долларов США/евро; или
 - б. выработки единых риск-ориентированных подходов к решению практических вопросов, например возникающих при резких колебаниях валютных курсов.
2. Следует четко определить размер порога *de minimis* и требования, применяемые к переводам, сумма которых не превышает установленный порог (например, в части состава передаваемой информации).
3. Финансовым учреждениям должны быть предоставлены понятные разъяснения о том, в каких случаях и каким образом следует применять указанные требования, включая ожидания надзорных органов, необходимые для их единообразного применения и предотвращения как избыточного, так и недостаточного применения требований.

Глава 6. Требования, применяемые к карточным операциям

6.1 Сфера применения

179. При оплате товаров или услуг с использованием кредитных, дебетовых или предоплаченных платежных карт требования Рекомендации 16 о передаче полного объема информации не применяются (далее - «исключение для карточных операций»). Оно действует независимо от суммы операции и от того, является ли она внутренней или трансграничной.

180. Развитие платежного рынка постепенно стерло границу между оплатой товаров и услуг и иными платежами и переводами, что привело к неопределенности в отношении сферы применения исключения для карточных операций. Поэтому при пересмотре Рекомендации 16 ФАТФ уточнила сферу его применения, чтобы исключить возможность использования такого исключения не по его первоначальному назначению. Для этого в сноску 54 к пункту 16 Пояснительной записки было включено разъяснение понятия «оплата товаров или услуг».

181. Одной из целей пересмотра Рекомендации 16 стало повышение прозрачности платежных цепочек, в том числе при оплате товаров и услуг с использованием платежных карт. В этой связи Рекомендация 16 предусматривает обязательную передачу номера платежной карты. Кроме того, по запросу должны предоставляться сведения о наименовании и местонахождении финансового учреждения-эмитента карты и финансового учреждения-эквайера торгово-сервисного предприятия.

182. Исключение для карточных операций применяется при оплате товаров или услуг кредитной, дебетовой или предоплаченной платежной картой независимо от способа инициирования операции. Если платежная карта используется для иных платежей или переводов, не связанных с оплатой товаров или услуг (например, при P2P-переводе между физическими лицами), применяются соответствующие требования Рекомендации 16.⁴⁰

Определение карт

183. Технологии проведения карточных операций постоянно развиваются. Первые карты изготавливались из картона, затем появились пластиковые карты с магнитной полосой, на которой данные хранились в открытом виде. Позднее им на смену пришли карты, соответствующие стандарту EMV⁴¹, в которых информация хранится в

⁴⁰ Для операций по снятию наличных денежных средств с платежных карт Рекомендация 16 устанавливает отдельные требования. Они рассматриваются в главе 7.

⁴¹ EMV - международный стандарт проведения карточных операций, оснащенных встроенным микрочипом, обеспечивающий более высокий уровень безопасности карточных операций. Стандарт был разработан в середине 1990-х годов и сегодня широко применяется во всем мире. Его развитием и сопровождением занимается организация EMVCo, участниками которой являются международные платежные системы Mastercard, Visa, American Express, Discover, JCB и UnionPay.

зашифрованном виде, что обеспечивает более высокий уровень защиты. С развитием электронной торговли получили распространение новые цифровые платежные инструменты, в частности виртуальные платежные карты. Они существуют только в электронном виде и позволяют скрыть реквизиты физической карты, снижая риск мошенничества.

184. Виды платежных карт. Для оплаты товаров и услуг могут использоваться кредитные⁴², дебетовые⁴³ и prepaid⁴⁴ платежные карты как в физической, так и в цифровой форме. Рекомендация 16 устанавливает единые требования для всех указанных видов карт. Вместе с тем prepaid карты имеют ряд особенностей. Например, в отношении их держателей в отдельных случаях может не проводиться надлежащая проверка клиента. Кроме того, такие карты могут передаваться третьим лицам, неизвестным эмитенту (например, если в рамках одной регистрации выпускается несколько карт). Пополнение prepaid карт также может осуществляться через небольшие торговые точки, не являющиеся субъектами, на которых распространяются требования в сфере ПОД/ФТ/ФРОМУ. В связи с этим, помимо требований Рекомендации 16, рекомендуется применять дополнительные риск-ориентированные меры контроля, например устанавливать ограничения на сумму операций и частоту их совершения.

185. Независимо от формы выпуска - физической или цифровой - операции с использованием платежных карт имеют общие характеристики, обусловленные правилами соответствующей платежной системы. Карточной считается операция, инициированная плательщиком с использованием реквизитов платежной карты, выпущенной в рамках такой системы, которая, как правило, предусматривает участие эмитента и эквайера. Если кредитная, дебетовая или prepaid платежная карта

⁴² Согласно глоссарию Банка международных расчетов (БМР), кредитная карта — это карта, указывающая на то, что держателю предоставлен кредитный лимит. Она позволяет держателю совершать покупки и/или снимать наличные в пределах заранее установленного лимита; предоставленный кредит может быть погашен в полном объеме к концу установленного периода или частично, при этом остаток считается продленным кредитом. На сумму любого продленного кредита начисляются проценты, а с держателя иногда взимается годовая комиссия. Глоссарий доступен по адресу: https://www.bis.org/cpmi/glossary_030301.pdf

⁴³ Согласно глоссарию, опубликованному БМР, дебетовая карта — это платежная карта, позволяющая списывать денежные средства непосредственно со счета ее держателя, открытого в кредитной организации. Может совмещать функции других платежных инструментов, например карты для получения наличных денежных средств или карты с функцией гарантии чека. Глоссарий доступен по адресу: https://www.bis.org/cpmi/glossary_030301.pdf

⁴⁴ Согласно глоссарию, опубликованному БМР, prepaid карта — это платежная карта, на которой хранится предварительно внесенная стоимость. Держатель такой карты заранее перечисляет эмитенту денежные средства, которые впоследствии используются для совершения операций. См. также «электронный кошелек», «prepaid карта ограниченного назначения», «многоцелевая prepaid карта», «карта с накопленным балансом». Глоссарий доступен по адресу: https://www.bis.org/cpmi/glossary_030301.pdf

используется для оплаты товаров или услуг, такая операция подпадает под исключение для карточных операций, предусмотренное Рекомендацией 16.

186. Операции с использованием карт закрытых платежных систем могут не подпадать под сферу применения Рекомендации 16. Такие карты, как правило, предназначены для ограниченного круга целей и не используются для осуществления платежей или переводов⁴⁵ общего назначения. К ним относятся, например, подарочные карты, карты лояльности и карты магазина, выпускаемые торгово-сервисными предприятиями или организациями розничной торговли, а также карты, выпускаемые государственными органами для предоставления отдельных услуг населению, например транспортные карты, предназначенные исключительно для оплаты проезда. Все эти инструменты функционируют только в пределах собственной ограниченной сети.

Разъяснение понятия «покупка товаров или услуг»

187. Исключение для карточных операций распространяется на операции по оплате товаров или услуг. При этом получателем платежа должно быть юридическое или физическое лицо, принимающее оплату с использованием платежных карт и прошедшее надлежащую проверку клиента в соответствующем финансовом учреждении или организации, действующей от его имени (сноска 54 к пункту 16 Пояснительной записки⁴⁶). Иными словами, речь идет о торгово-сервисных предприятиях в понимании правил соответствующей платежной системы.

188. Под торгово-сервисным предприятием понимается организация, включая индивидуального предпринимателя, принимающая карточные платежи в рамках одной или нескольких платежных систем. Такое предприятие имеет договорные отношения с соответствующим финансовым учреждением-эквайером либо организацией, действующей от его имени⁴⁷. Такие отношения могут быть как прямыми, так и осуществляться через платежного агрегатора или платежного фасилитатора⁴⁸. В свою очередь, эквайер имеет договорные отношения с платежной системой, если только она

⁴⁵ Под платежом или переводом ценностей понимается любая операция, осуществляемая финансовым учреждением, инициирующая платеж, по поручению плательщика с использованием электронных средств в целях предоставления денежных средств получателю через финансовое учреждение получателя независимо от того, совпадают ли плательщик и получатель. К таким операциям относится также выдача наличных денежных средств.

⁴⁶ Под оплатой товаров или услуг понимается оплата в пользу юридических или физических лиц, принятых на обслуживание соответствующим финансовым учреждением для приема карточных платежей после проведения надлежащей проверки клиента в отношении такой деятельности.

⁴⁷ Торгово-сервисное предприятие может иметь договорные отношения не с эквайером, а с платежным агрегатором (платежным фасилитатором). Такая модель может именоваться Sponsored Merchant Agreement.

⁴⁸ Если платежный агрегатор (платежный фасилитатор) имеет прямые договорные отношения с торгово-сервисным предприятием, именно на него распространяются требования Рекомендации 16.

не осуществляет эквайринг своих торгово-сервисных предприятий самостоятельно. Фактическая деятельность торгово-сервисного предприятия и место ее осуществления должны соответствовать сведениям, на основании которых оно было принято на обслуживание.

Дополнительные разъяснения

189. Исключение для карточных операций не применяется, если кредитная, дебетовая или предоплаченная платежная карта используется для осуществления платежей или переводов, не связанных с оплатой товаров или услуг (например, при P2P-переводе между физическими лицами). В таких случаях применяются все требования Рекомендации 16, установленные для внутренних или трансграничных платежей и переводов.

190. Исключение для карточных операций, как правило, не применяется к переводам с использованием платежной карты, не связанным с оплатой товаров или услуг (например, при пополнении электронного кошелька⁴⁹). К таким переводам в полном объеме применяются требования Рекомендации 16, если одновременно выполняются следующие условия:

- Средства переводятся на счет или в электронный кошелек и не зачисляются непосредственно торгово-сервисному предприятию; и
- Переведенные средства могут использоваться не только для оплаты товаров или услуг, но и для иных целей, включая P2P-переводы между физическими лицами и снятие наличных денежных средств.

Вставка 10. Примеры карточных переводов

Случай 1 (оплата товаров или услуг, исключение применяется). Платежная карта используется для пополнения электронного кошелька (или иного счета с предварительно внесенными средствами), открытого торгово-сервисным предприятием (например, магазином, оператором общественного транспорта или поставщиком цифрового контента по подписке). В этом случае средства зачисляются торгово-сервисному предприятию и могут использоваться исключительно для оплаты предоставляемых им товаров или услуг.

Случай 2 (P2P-перевод между физическими лицами, исключение не применяется). Платежная карта используется для пополнения электронного кошелька (или иного счета с

⁴⁹ С учетом положений Рекомендации 16, относящихся к оплате товаров или услуг, а также определения понятия «платеж или перевод ценностей», карточная операция, используемая для перевода средств от плательщика получателю по поручению плательщика, должна рассматриваться как P2P-перевод между физическими лицами, за исключением случаев, когда такая операция совершается исключительно в целях оплаты товаров или услуг. Это правило применяется и в тех случаях, когда плательщик и получатель являются одним и тем же лицом.

предварительно внесенными средствами), средства с которого впоследствии могут использоваться для P2P-переводов между физическими лицами. Такие электронные кошельки, как правило, открываются в финансовых учреждениях.

Случай 3 (P2P-перевод между физическими лицами, исключение не применяется): Платежная карта используется для финансирования последующего P2P-перевода между физическими лицами. Например, физическое лицо обращается в пункт обслуживания оператора УПДЦ и использует дебетовую карту для внесения средств, которые затем переводятся другому физическому лицу через этого оператора УПДЦ.

191. В рамках каждой карточной платежной системы могут осуществляться и иные операции, не связанные с оплатой товаров или услуг. Если финансовые учреждения, участвующие в платежной цепочке, привлекают посредников (например, платежных агрегаторов или платежных фасилитаторов) для обработки операций, эмитент и эквайер должны убедиться, что такие посредники обеспечивают целостность и конфиденциальность информации по каждой операции.

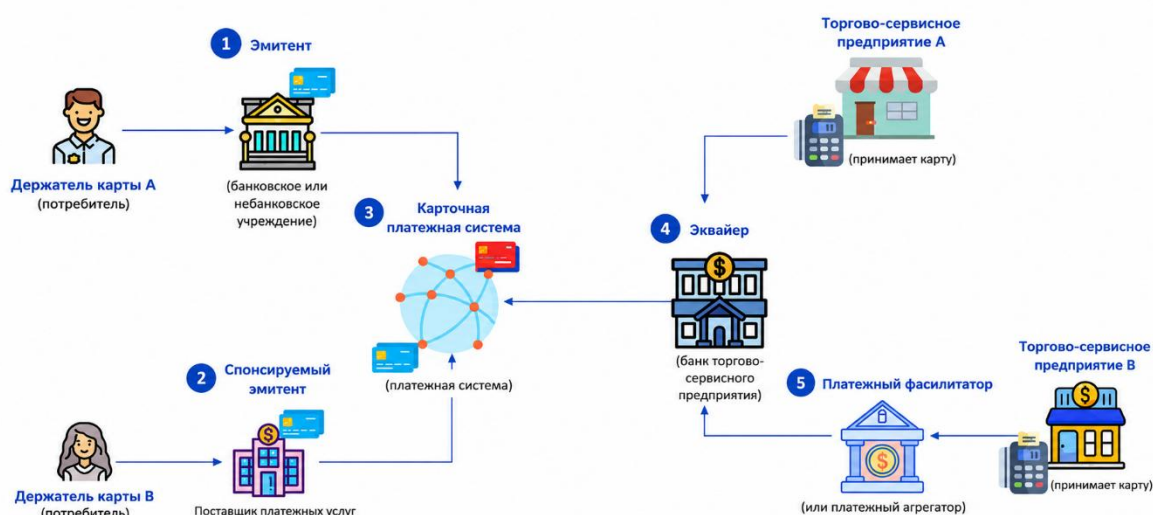
6.2 Обязанности участников платежной цепочки

192. **Основные участники.** При осуществлении карточных платежей ключевую роль играют два участника: эмитент, выпускающий платежную карту и ведущий счет, к которому она привязана, и эквайер, обеспечивающий торгово-сервисным предприятиям возможность принимать карточные платежи. Для целей Рекомендации 16 эмитент и эквайер рассматриваются как финансовые учреждения в соответствии со Стандартами ФАТФ. Их деятельность осуществляется на основании договорных отношений и в соответствии с едиными правилами, установленными оператором карточной платежной системы. Такая модель обычно называется системой открытого типа (open loop network). В рамках такой системы держатель карты может использовать ее для оплаты у любого торгово-сервисного предприятия, подключенного к карточной платежной системе через эквайера либо через платежного агрегатора (платежного фасилитатора), который по поручению эквайера может выполнять отдельные его функции в рамках карточной платежной системы. Платежный агрегатор (платежный фасилитатор) обеспечивает торгово-сервисным предприятиям возможность принимать карточные платежи и заключает договор с эквайером, который сохраняет ответственность за предоставление торгово-сервисным предприятиям доступа к карточной платежной системе. Спонсируемый эмитент, также называемый сторонним эмитентом, выпускает платежные карты на основании соглашения о спонсорстве, заключенного с основным эмитентом соответствующей крупной карточной платежной системы.

193. **Карточные платежные системы.** Платежные карты выпускаются в рамках карточной платежной системы, которая устанавливает единые стандарты обмена сообщениями, требования к безопасности и иные технические требования, необходимые для обработки внутренних и трансграничных операций. При совершении карточной операции перевод средств осуществляется в соответствии с установленными платежной системой процедурами авторизации, клиринга и расчетов. Для этого используется

идентификатор, определенный правилами платежной системы (например, номер платежной карты или его токенизированный эквивалент), независимо от технологии, с помощью которой инициируется платеж (например, контактным способом, бесконтактным способом, через Интернет, с использованием платежных приложений или цифровых кошельков). Как правило, карточные платежи осуществляются с участием эмитента и эквайера, состоящих в договорных отношениях соответственно с держателем карты и торгово-сервисным предприятием и действующих в соответствии с едиными правилами, установленными оператором платежной системы. Вместе с тем некоторые карточные платежные системы, например American Express и JCB, самостоятельно осуществляют как эмиссию платежных карт, так и эквайринг торгово-сервисных предприятий.

194. На приведенной ниже схеме показаны основные участники карточной операции:



195. В соответствии с Рекомендацией 16 при оплате товаров или услуг перевод должен сопровождаться номером кредитной, дебетовой или предоплаченной платежной карты. Кроме того, по запросу должна предоставляться информация о наименовании и местонахождении финансового учреждения-эмитента карты и финансового учреждения-эквайера торгово-сервисного предприятия. На приведенной ниже схеме показано, какой информацией располагает каждый участник платежной цепочки при осуществлении карточного платежа.

- (1) Эмитент - хранит всю информацию о держателях выпущенных им платежных карт. В отношении спонсируемых организаций эмитент хранит информацию об их наименовании и местонахождении. Хотя эмитент может не располагать информацией о держателях карт, обслуживаемых его спонсируемыми организациями, он несет ответственность за качество, точность и безопасность информации, относящейся к таким организациям.
- (2) Карточная платежная система - располагает информацией о внутренних и трансграничных карточных операциях, обрабатываемых в рамках платежной

системы, а также информацией, полученной в рамках надлежащей проверки клиента (KYC), в отношении эмитентов и эквайеров.

- (3) Эквайер - хранит всю информацию о торгово-сервисных предприятиях, которые он непосредственно принимает на обслуживание. В отношении спонсируемых организаций эквайер хранит информацию об их наименовании и местонахождении. Хотя эквайер может не располагать информацией о торгово-сервисных предприятиях, обслуживаемых его спонсируемыми организациями, он несет ответственность за качество, точность и безопасность информации, относящейся к таким организациям.
- (4) Платежный фасилитатор (или платежный агрегатор) - хранит всю информацию о торгово-сервисном предприятии, включая сведения о его местонахождении и осуществляемой деятельности.
- (5) Спонсируемый эмитент (или сторонний эмитент) - хранит всю информацию о держателях платежных карт.

6.2.1 Номер карты

196. В соответствии с Рекомендацией 16 номер платежной карты должен сопровождать все переводы, осуществляемые в рамках карточной операции. Это означает, что полный номер платежной карты, использованной для оплаты товаров или услуг, должен включаться во все относящиеся к такой операции сообщения между эмитентами и эквайерами (а также их спонсируемыми организациями, например платежными агрегаторами или эмитентами, осуществляющими деятельность на основании спонсорского соглашения с другим эмитентом). Для целей настоящего Руководства под номером платежной карты также понимается его токенизированный эквивалент.

197. **Роль эквайеров и эмитентов.** Эмитенты и эквайеры должны предоставлять информацию о номере платежной карты по каждой операции. Это требование распространяется как на традиционные номера платежных карт, так и на их токенизированные эквиваленты, позволяющие однозначно определить финансовое учреждение - эмитента.

198. **Токенизированные номера платежных карт.** Токенизированные номера платежных карт могут использоваться для безопасной авторизации операций без раскрытия данных держателя карты⁵⁰. Токенизированный номер представляет собой замену исходного номера платежной карты и используется при проведении операций вместо него. При этом только участники карточной платежной системы, обладающие необходимыми полномочиями, могут установить соответствие между токенизированным и исходным номером платежной карты. Использование

⁵⁰ Номер платежной карты соответствует международным стандартам. Международный стандарт ISO 8583, регулирующий обмен сообщениями при совершении финансовых операций с использованием платежных карт, использует для обозначения номера платежной карты специальный термин - *Primary Account Number (PAN)*.

токенизированных номеров платежных карт не должно препятствовать выполнению требований Рекомендации 16. При необходимости компетентные органы должны иметь доступ к информации, позволяющей установить личность держателя карты, а также определить финансовое учреждение - эмитента или эквайера, участвующее в операции. Услуги по предоставлению токенизированных номеров платежных карт могут оказываться как эмитентами своим держателям карт, так и эквайерами обслуживаемым ими торгово-сервисным предприятиям. Эмитенты и эквайеры должны использовать токенизированные номера платежных карт таким образом, чтобы по ним можно было определить исходный номер платежной карты.

6.2.2 Наименование и местонахождение эмитента и эквайера

199. **Идентификация участников операции.** При анализе операций с использованием платежных карт у компетентных органов нередко возникают сложности с установлением участников конкретной операции, прежде всего личности держателя платежной карты.

200. Сведения о держателе платежной карты находятся в распоряжении финансового учреждения - эмитента. Поэтому для получения такой информации путем направления судебного запроса или иным предусмотренным способом (аналогично - в отношении эквайера) необходимо сначала установить эмитента. При этом из данных об операции не всегда можно определить, какое финансовое учреждение выпустило платежную карту или какое финансовое учреждение обслуживает счет торгово-сервисного предприятия.

201. **Требование.** Рекомендация 16 устанавливает требование о предоставлении по запросу сведений о наименовании и местонахождении финансового учреждения - эмитента и финансового учреждения-эквайера торгово-сервисного предприятия при оплате товаров или услуг кредитной, дебетовой или предоплаченной платежной картой (пункт 16 Пояснительной записки к Рекомендации 16). Указанные сведения предоставляются всем финансовым учреждениям, участвующим в платежной цепочке, а через них - компетентным органам, причем без необоснованных задержек (сноски 55 и 56 к Стандартам ФАТФ). На основании этих сведений правоохранные органы, органы прокуратуры, подразделения финансовой разведки, а также финансовые учреждения, участвующие в платежной цепочке, устанавливают, какие финансовые учреждения располагают полной информацией о держателе платежной карты и торгово-сервисном предприятии, а также в каком государстве находятся такие финансовые учреждения (сноска 55 к Стандартам ФАТФ). Финансовые учреждения, участвующие в карточной операции, предоставляют компетентным органам и другим участникам платежной цепочки сведения о наименовании и местонахождении эмитента и (или) эквайера. Эти сведения должны однозначно указывать на финансовое учреждение, располагающее полной информацией о держателе платежной карты или торгово-сервисном предприятии. Если выпуск платежных карт или подключение торгово-сервисных предприятий осуществляет спонсируемая организация, указываются сведения именно о ней, поскольку она располагает полной информацией о соответствующем держателе карты или торгово-сервисном предприятии.

202. Банковский идентификационный номер (BIN), входящий в состав номера платежной карты (PAN), позволяет однозначно определить эмитента. При этом официальные справочники BIN, которые ведут карточные платежные системы, не находятся в открытом доступе. Идентификация соответствующих финансовых учреждений может дополнительно осложняться использованием механизмов спонсорского BIN и спонсорского эквайринга. В таких случаях эмитент и эквайер, указанные в BIN и данных платежного сообщения, не являются организациями, непосредственно взаимодействующими соответственно с держателем платежной карты и торгово-сервисным предприятием. В этих случаях при поступлении запроса о предоставлении информации необходимо дополнительно установить организацию, непосредственно взаимодействующую с держателем платежной карты или торгово-сервисным предприятием. Так, если поставщик платежных услуг, например небанковское финансовое учреждение, выпускает платежные карты в рамках соглашения о спонсорском BIN с банком-участником карточной платежной системы, при этом именно поставщик платежных услуг привлек держателя платежной карты на обслуживание, в предоставляемой информации должны указываться его наименование и местонахождение, а не наименование и местонахождение банка-спонсора. Аналогичным образом, если торгово-сервисное предприятие принимает платежные карты через платежного фасилитатора, который обслуживается у эквайера-участника карточной платежной системы, в предоставляемой информации указывается организация, привлекающая торгово-сервисное предприятие на обслуживание и располагающая полной информацией о нем. В таких случаях организация-спонсор при получении запроса от компетентных органов указывает спонсируемую организацию, которая привлекла на обслуживание держателя платежной карты или торгово-сервисное предприятие и располагает полной информацией соответственно о держателе платежной карты или торгово-сервисном предприятии.

203. **Роль карточных платежных систем.** При обработке карточной операции карточная платежная система передает номер платежной карты. По запросу финансового учреждения либо компетентного органа, направленному через соответствующее финансовое учреждение, карточная платежная система также предоставляет сведения о наименовании и местонахождении эмитента или эквайера в читаемом виде (независимо от того, представлены они в зашифрованном или незашифрованном виде). Карточные платежные системы могут содействовать получению сведений об эмитентах и эквайерах, поскольку располагают информацией о своих участниках, полученной в рамках процедур КУС, а также уже выполняют центральную роль в обмене сообщениями между эмитентами и эквайерами. Для этого могут использоваться различные технические решения, например механизмы поиска BIN или API. Настоящее Руководство не устанавливает требований к выбору конкретного технического решения. Настоящий пункт следует рассматривать во взаимосвязи с разделом, посвященным платежным инфраструктурам, в главе 4.

204. **Пример.** Правоохранительные органы государства А получают от торгово-сервисного предприятия данные по карточным операциям, свидетельствующие о возможной

противоправной деятельности (например, мошенничестве). С этими данными они обращаются к эквайеру торгово-сервисного предприятия или к организации, осуществляющей деятельность на основании спонсорского соглашения с эквайером (например, платежному фасилитатору), и запрашивают сведения о наименовании и местонахождении эмитента, обслуживающего счет держателя платежной карты, с использованием которой были совершены указанные операции. Если эквайер или спонсируемая организация уже располагают такой информацией, они предоставляют ее непосредственно. В противном случае они запрашивают ее через карточную платежную систему, которая передает сведения эквайеру, а тот – компетентным органам. Если правила карточной платежной системы не предусматривают возможность такого обмена информацией, рекомендуется рассмотреть вопрос об их пересмотре.



Глава 7. Выдача наличных денежных средств за рубежом

7.1 Обоснование применения специальных требований к операциям по выдаче наличных денежных средств за рубежом

206. Для противодействия финансовым преступлениям правоохранительные органы должны иметь возможность установить личность держателя платежной карты, совершившего операцию. Анализ практических примеров показал, что операции по выдаче наличных денежных средств за рубежом наиболее часто используются в схемах незаконной финансовой деятельности. В связи с этим Рекомендация 16 устанавливает специальные требования к данной категории карточных операций. При этом на такие операции не распространяются все требования, предусмотренные для иных платежей и переводов.

7.2 Проблемы в сфере ПОД/ФТ, связанные с выдачей наличных денежных средств за рубежом

207. Правоохранительные органы государства, на территории которого осуществлена выдача наличных денежных средств, не имеют оперативного и систематизированного доступа к информации о держателе платежной карты. Это создает сложности как для финансовых учреждений, так и для компетентных органов. Финансовое учреждение, обеспечившее выдачу наличных денежных средств за рубежом, не располагает сведениями о личности держателя платежной карты, инициировавшего операцию. Например, если компетентному органу необходима информация об операции по выдаче наличных денежных средств за рубежом, ему приходится направлять несколько запросов иностранным компетентным органам, чтобы установить участников операции и проследить движение денежных средств. Это затрудняет расследование и уголовное преследование, значительно увеличивая их продолжительность по сравнению с ситуацией, когда основная информация о держателе платежной карты может быть оперативно получена в государстве, на территории которого была совершена операция. Ниже приведен пример, иллюстрирующий сложности, возникающие при расследовании случаев выдачи наличных денежных средств за рубежом.

Вставка 11.

Пример

- Лицо X, проживающее в государстве А, открывает один или несколько счетов в государствах В и С, вносит на них денежные средства и получает одну или несколько платежных карт.
- После этого лицо X возвращается в государство А.
- Используя платежные карты, выпущенные в государствах В и С, лицо X регулярно снимает крупные суммы наличных денежных средств в банкоматах на территории государства А.
- Финансовые учреждения государства А не располагают сведениями о личности

держателя платежной карты. Такая информация имеется только у эмитентов платежных карт в государствах В и С.

- Информация о деятельности лица X оказывается распределена между несколькими государствами, что затрудняет выявление незаконной деятельности. В результате лицо X может обходить меры ПОД/ФТ, применяемые финансовыми учреждениями и компетентными органами государства А. Правоохранительные органы не могут своевременно получить необходимую информацию из-за недостаточной прозрачности таких операций.

7.3 Требования к информации при снятии наличных

208. Требования к информации при выдаче наличных денежных средств с использованием платежной карты, выпущенной в государстве совершения операции. При выдаче наличных денежных средств с использованием платежной карты, выпущенной в государстве совершения операции, требуется передача только номера счета или номера платежной карты. Данное требование распространяется как на традиционные номера платежных карт, так и на их токенизированные эквиваленты, указанные в главе 6 настоящего Руководства.

209. Требования к информации при трансграничной выдаче наличных денежных средств. При снятии наличных денежных средств с кредитной, дебетовой или предоплаченной платежной карты за рубежом, если выдача наличных денежных средств осуществляется организацией, не являющейся эмитентом платежной карты, применяются следующие требования:

- (a) При снятии наличных должен указываться номер карты,⁵¹ и
- (b) По запросу организации-эквайера имя держателя платежной карты должно быть направлено в течение трех рабочих дней с момента получения такого запроса.

210. Исключение для операций в рамках одного финансового учреждения. Как отмечалось выше, требования к трансграничной выдаче наличных денежных средств обусловлены трудностями, с которыми сталкиваются компетентные органы при получении информации о держателе платежной карты, снимающем наличные денежные средства за пределами государства, в котором была выпущена его платежная карта. Вместе с тем в отдельных случаях требования, применяемые к трансграничной выдаче наличных денежных средств, могут не применяться. Такие требования не распространяются на операции по выдаче наличных денежных средств в банкоматах, принадлежащих тому же финансовому учреждению, в котором открыт счет, при условии, что номер платежной карты и имя ее держателя могут передаваться между филиалами и

⁵¹ Практически это означает, что при всех трансграничных операциях по выдаче наличных денежных средств номер платежной карты должен передаваться финансовым учреждениям-эквайерам. Данное требование соответствует требованиям Рекомендации 16, применяемым к карточным платежам за товары и услуги, а также к операциям по выдаче наличных денежных средств с использованием платежной карты, выпущенной в государстве совершения операции.

дочерними организациями в соответствии с внутригрупповыми политиками и процедурами (сноска 57 к Стандартам ФАТФ). При этом должен обеспечиваться эквивалентный уровень доступа к информации, как и при трансграничной выдаче наличных денежных средств вне банковской группы, то есть имя держателя платежной карты должно быть доступно компетентным органам по их запросу в течение трех рабочих дней.

211. Роли участников. Запрос о предоставлении имени держателя платежной карты должен направляться эмитенту, поскольку именно он поддерживает отношения с клиентом-держателем платежной карты. Такой запрос должен направляться организацией-эквайером либо от собственного имени, либо по поручению компетентного органа, запросившего указанную информацию. Запросы должны направляться в случаях, когда дополнительная информация необходима в связи с выявлением подозрительных операций или в рамках расследований, проводимых правоохранительными органами. Финансовое учреждение-эквайер должна указывать эмитенту цель запроса. При выдаче наличных денежных средств через банкомат под финансовым учреждением-эквайером (финансовым учреждением получателя) понимается финансовое учреждение, обслуживающее банкомат, в котором были выданы наличные денежные средства, или выступающее спонсором такого банкомата. На оператора банкомата, который предоставляет финансовому учреждению-эквайеру (финансовому учреждению получателя) исключительно банкоматы или системы их поддержки, не распространяется требование о получении информации о держателе платежной карты. Эмитент должен направить организации-эквайеру имя держателя платежной карты в течение трех рабочих дней с момента получения запроса. Предполагается, что финансовое учреждение-эквайер использует полученную информацию исключительно для целей, указанных в запросе. Рекомендация 16 не требует от организации-эквайера выполнения каких-либо дополнительных действий, таких как проверка по санкционным перечням, применение усиленных мер надлежащей проверки клиента или проведение дополнительного расследования на основании раскрытых сведений. Обязанности, предусмотренные Рекомендацией 16, возлагаются на финансовые учреждения, участвующие в цепочке карточного платежа, а не на торгово-сервисное предприятие. В соответствии с Рекомендацией 16 торгово-сервисное предприятие не обязано получать информацию о держателе платежной карты или участвовать в ее предоставлении финансовому учреждению-эквайеру либо компетентным органам.

212. Виды операций. Указанные требования применяются к операциям по выдаче наличных денежных средств. К таким операциям относятся выдача наличных денежных средств через банкомат, а также операции *кэшбэк* (выдача наличных денежных средств в торгово-сервисном предприятии). Указанные требования применяются независимо от суммы операции.

213. Ожидаемая роль карточных платежных систем. Несмотря на то, что Рекомендация 16 устанавливает требования только к обязанным субъектам, предполагается, что карточные платежные системы будут играть важную роль в передаче

информации о держателе платежной карты между эмитентами и эквайерами. Заключение двусторонних соглашений между эмитентами и эквайерами без координации со стороны карточных платежных систем, вероятнее всего, повлечет чрезмерные затраты и не позволит обеспечить эффективный обмен такой информацией. Настоящее Руководство не устанавливает требований к конкретному техническому решению.

214. Обработка информации о держателе платежной карты. Информация о держателе платежной карты подлежит защите на всех этапах ее обработки финансовыми учреждениями, карточными платежными системами и компетентными органами. Для предотвращения неправомерного доступа к информации о держателе платежной карты, в частности к его имени, должны использоваться защищенные системы передачи и хранения данных.

215. Эквайеры должны обеспечивать защиту информации о держателе платежной карты в соответствии с требованиями Рекомендации 16. Кроме того, они должны соблюдать требования законодательства о защите персональных данных и неприкосновенности частной жизни, действующего в соответствующей юрисдикции, а также правила международных карточных платежных систем, регулирующие порядок обращения с конфиденциальной информацией. (Подробнее см. главу 9.)

216. Эквайерам следует принимать меры по защите получаемой ими информации о держателе платежной карты в соответствии с отраслевыми стандартами безопасности, например стандартами индустрии платежных карт (PCI), устанавливающими требования к защите данных о держателях платежных карт при их хранении, обработке и передаче. В частности, такие меры могут предусматривать раздельное хранение номера платежной карты и имени ее держателя в записях о совершенных операциях.

217. Кроме того, важную роль в защите информации о держателе платежной карты играют компетентные органы, запрашивающие и получающие такую информацию. Они должны обрабатывать такую информацию в соответствии с механизмами защиты неприкосновенности частной жизни и персональных данных, действующими в соответствующей юрисдикции, например путем внедрения Стандарта безопасности данных индустрии платежных карт (PCI DSS) и (или) соблюдения иных применимых требований, регулирующих порядок обработки, использования и защиты такой информации.

218. Финансовое учреждение-эмитент платежной карты несет ответственность за качество и достоверность информации о держателе платежной карты, передаваемой в ответ на запросы эквайеров. Карточные платежные системы, не имеющие прямых отношений с держателем платежной карты, хотя и играют важную роль в передаче такой информации, не несут ответственности за ее качество и достоверность.

Глава 8. Применение Рекомендации 16 к различным способам оплаты и переводов

8.1 Основные принципы

219. Настоящая глава разъясняет особенности применения Рекомендации 16 к отдельным способам оплаты и перевода, приобретающим все большее значение в современной платежной сфере, включая мгновенные платежи, цифровые кошельки и мобильные деньги. Она не устанавливает отдельных требований для рассматриваемых способов оплаты и перевода и должна применяться во взаимосвязи с другими главами, в частности с главой 4 (платежная цепочка), главой 5 (требования к информации), главой 9 (защита неприкосновенности частной жизни и персональных данных) и главой 10 (проверки соответствия данных). К указанным способам оплаты и перевода в полном объеме применяются требования Рекомендации 16, в том числе при их использовании для оплаты товаров и услуг. Приведенные в настоящей главе примеры носят иллюстративный характер и не ограничивают возможные случаи применения Рекомендации 16.

220. Требования Рекомендации 16 применяются независимо от используемых технологий и технических решений. Использование проху-идентификаторов (псевдонимов), а также иных решений, направленных на ускорение проведения платежей, повышение удобства пользователей или совместимости платежных систем, не освобождает финансовые учреждения от соблюдения указанных требований. При этом в платежной системе должны быть предусмотрены механизмы, обеспечивающие передачу обязательной информации в составе платежного сообщения, а также ее доступность для финансовых учреждений, участвующих в платежной цепочке, и компетентных органов. Объем требований Рекомендации 16, применяемых к каждому финансовому учреждению, определяется его ролью в платежной цепочке при осуществлении конкретного перевода.

8.2 Применение Рекомендации 16 к мгновенным платежам

8.2.1 Понятие системы мгновенных платежей

221. В настоящей главе используется терминология, разработанная Комитетом по платежам и рыночным инфраструктурам Банка международных расчетов (CPMI BIS⁵²). Термины «мгновенные», «быстрые» и «осуществляемые в режиме реального времени» используются как равнозначные. Под мгновенными платежами в настоящем Руководстве понимаются платежи, при которых передача платежного сообщения и зачисление средств получателю осуществляются в режиме реального времени либо с минимальной задержкой. Такие платежи, как правило, осуществляются круглосуточно, без выходных дней. Отдельные особенности, рассматриваемые в настоящем разделе, в частности использование проху-идентификаторов, могут быть характерны и для других способов оплаты.

⁵² [CPMI-BIS, ноябрь 2016 г. - «Быстрые платежи - повышение скорости и доступности розничных платежей»](#)

8.2.2 Основные аспекты применения Рекомендации 16 к мгновенным платежам

Использование проху-идентификаторов вместо номеров счетов

222. Во многих цифровых платежных сервисах для повышения удобства пользователей и совместимости между платежными системами все чаще используются такие идентификаторы, как номера мобильных телефонов, виртуальные платежные адреса (VPA⁵³), псевдонимы и токены. Несмотря на то что такие проху-идентификаторы эффективно используются для маршрутизации платежей и упрощают взаимодействие пользователей с платежными сервисами, они не всегда позволяют выполнить требование о передаче имен плательщика и получателя. Эту проблему можно решить, если до направления платежного сообщения сопоставить проху-идентификаторы с соответствующими счетами и именами клиентов, чтобы платежное сообщение содержало всю необходимую информацию.

Вставка 12. Использование проху-идентификаторов без ущерба для прозрачности платежей

Индия

В системе Unified Payments Interface (UPI) сопоставление проху-идентификаторов с соответствующими реквизитами осуществляется до формирования платежного сообщения. После этого в платежное сообщение включаются сведения о клиенте (номер счета, имя и другие идентификаторы). Такой подход позволяет использовать проху-идентификаторы без замены обязательной информации о плательщике и получателе и обеспечивает прослеживаемость платежа для финансовых учреждений, участвующих в его дальнейшей обработке.

Европейский Союз

Платежные решения, использующие мгновенные кредитовые переводы в евро с применением проху-идентификаторов (например, номеров мобильных телефонов), осуществляют обработку операций в соответствии с правилами схемы SCT Inst. Согласно указанным правилам обязательная информация о плательщике и получателе должна включаться в платежное сообщение независимо от того, используются ли проху-идентификаторы для инициирования операции.

Гонконг, Китай

Система Faster Payment System (FPS) предоставляет сервис адресации, позволяющий использовать проху-идентификаторы (например, номера мобильных телефонов, адреса электронной почты или уникальные идентификаторы, присваиваемые системой FPS) вместо номера банковского счета. Плательщик может инициировать перевод денежных средств, указав проху-идентификатор получателя. После этого система FPS предоставляет плательщику частично скрытое имя владельца счета получателя для

⁵³ VPA (Virtual Payment Address) - уникальный идентификатор пользователя, используемый при работе с платежным сервисом.

подтверждения правильности реквизитов. При завершении перевода платежное сообщение включает всю обязательную информацию о плательщике и получателе.

Возможность передачи всей необходимой информации

223. Некоторые системы мгновенных платежей, прежде всего предназначенные для внутренних платежей, изначально создавались для максимально быстрой обработки операций. Поэтому в них нередко используются форматы сообщений с фиксированной длиной или собственные форматы обмена сообщениями, предусматривающие ограниченный набор полей данных. Такие решения позволяют обрабатывать большое количество операций в режиме реального времени, однако не всегда поддерживают передачу структурированной информации о плательщике и получателе в объеме, предусмотренном обновленной Рекомендацией 16 (например, не содержат всех обязательных полей данных). Это особенно актуально в случаях, когда внутренние системы мгновенных платежей используются для завершения последнего этапа трансграничного перевода (см. раздел 4.6 «Платежные инфраструктуры»).

224. Государства должны уже на этапе проектирования и внедрения систем мгновенных платежей закладывать требования к совместимости систем и целостности передаваемых данных, чтобы минимизировать риски, связанные с фрагментацией платежной инфраструктуры.

Вставка 13. Пример - Проектирование системы с учетом требований к передаче всех необходимых данных.

Платформа UPI в Индии использует собственный формат обмена сообщениями, разработанный для быстрой обработки операций и гибкой адаптации к различным сценариям использования. Для поддержки расширенного состава передаваемых данных и совместимости с трансграничными платежами в ней применяются механизмы структурированного преобразования данных, которые при взаимодействии с системами, использующими стандарт ISO 20022, преобразуют элементы данных UPI в совместимый с ним формат.

Источник: Индия

Проверка информации о получателе

225. Финансовые учреждения получателя должны принимать разумные меры для проверки личности получателя (пункт 29 Пояснительной записки к Рекомендации 16), а также выявлять ошибочно направленные или потенциально подозрительные платежи, в том числе с использованием проверок соответствия данных (пункт 30 Пояснительной записки к Рекомендации 16). В системах мгновенных платежей особенно важно организовать эти процессы таким образом, чтобы они не замедляли проведение операций и не создавали для их участников излишних затруднений. Эта задача приобретает особое значение, поскольку мгновенные платежи исполняются практически сразу и, как

правило, являются безотзывными. В результате ошибочно направленный или мошеннический платеж после его исполнения может оказаться невозможно вернуть. Поэтому особую роль играют предварительные проверки, например подтверждение реквизитов получателя платежа, а также мониторинг операций в режиме реального времени или с минимальной задержкой. Такие меры позволяют выявлять несоответствия до исполнения платежа и тем самым снижать риски, характерные для мгновенных платежей (см. главу 10). Это подчеркивает важность включения в системы мгновенных платежей эффективных механизмов управления рисками, позволяющих сохранить баланс между скоростью проведения операций, их стоимостью и безопасностью.

Вставка 14. Проверка получателя и контроль операций в режиме реального времени при осуществлении мгновенных платежей

Индия

В системе UPI финансовые учреждения применяют различные подходы к проверке получателей и согласованию данных в режиме реального времени, в том числе:

- интегрируют инструменты ПОД/ФТ и противодействия мошенничеству непосредственно в процессы обработки платежей, что позволяет автоматически выполнять необходимые проверки без задержки исполнения операций; и
- используют результаты ранее проведенной надлежащей проверки клиентов (CDD), а также механизмы, связывающие платежные идентификаторы со счетами, открытыми на имя уже проверенных клиентов.

8.3 Платежи с использованием цифровых кошельков

8.3.1 Общие положения и сфера применения

226. Для целей настоящего Руководства под цифровым кошельком (также именуемым электронным кошельком или e-wallet и включающим различные формы электронных денежных средств) понимается приложение или сервис, предназначенные для хранения денежных средств в электронной форме (за исключением инструментов, связанных с виртуальными активами), а также для осуществления платежей или переводов (например, PayPal, Alipay). Цифровые кошельки также могут предоставлять технические сервисы, позволяющие пользователям инициировать платежи с использованием банковских счетов (например, Wero, Bizum) или платежных карт (например, Google Pay или Apple Pay).

227. Цифровые кошельки могут различаться по способу проведения платежей и роли, которую их оператор играет в движении денежных средств. В частности, возможны следующие модели:

- a) платежи, осуществляемые с использованием привязанных к цифровому кошельку способов оплаты (например, банковских счетов или платежных карт);
- b) платежи за счет денежных средств, хранящихся у оператора цифрового кошелька; или

- с) платежи, при которых пополнение цифрового кошелька и последующее осуществление платежа представляют собой отдельные этапы.

228. Цифровые кошельки могут поддерживать переводы между счетами, открытыми у одного оператора цифрового кошелька (переводы внутри одного цифрового кошелька), а также между счетами, открытыми у разных операторов цифровых кошельков (переводы между цифровыми кошельками).

229. В настоящем разделе рассматриваются особенности применения требований Рекомендации 16 к наиболее распространенным видам операций. Его следует читать во взаимосвязи с главой 4, посвященной цепочке проведения платежа. Для целей Рекомендации 16 определяющее значение имеет не сам цифровой кошелек как продукт, а способ осуществления конкретного платежа или перевода и роль оператора цифрового кошелька в такой операции. В зависимости от модели проведения операции оператор цифрового кошелька может выполнять функции финансового учреждения либо исключительно функции поставщика технических услуг - в зависимости от того, хранит ли он денежные средства пользователя и участвует ли в проведении платежа или лишь обеспечивает его техническую обработку.

Вставка 15. Пример - Прозрачность использования ргоху-идентификаторов при платежах и переводах через цифровые кошельки.

Для номеров счетов цифровых кошельков используются единые правила формирования. Номер счета содержит закодированную информацию, например о стране, валюте и финансовом учреждении. При переводах между цифровыми кошельками разных операторов передается номер счета плательщика. Если перевод осуществляется между клиентами одного оператора цифрового кошелька, для инициирования перевода вместо номера счета используются ргоху-идентификаторы (например, адрес электронной почты или номер мобильного телефона). При этом оператор самостоятельно определяет, какому номеру счета соответствует указанный ргоху-идентификатор.

Источник: Китай

8.3.2. Основные принципы применения требований Рекомендации 16 к различным моделям функционирования цифровых кошельков

230. Для целей применения Рекомендации 16 значение имеет не вид цифрового кошелька, а роль каждого участника в цепочке проведения платежа. При этом финансовым учреждением, к которому применяются требования Рекомендации 16, считается то, которое получает платежное распоряжение непосредственно от плательщика. Если эту функцию выполняет оператор цифрового кошелька, к нему также применяются соответствующие требования.

231. Финансовое учреждение, инициирующее платеж, - это организация, которая получает платежное распоряжение от плательщика и осуществляет перевод средств. Оператор цифрового кошелька может оказывать только технические услуги, например обеспечивать безопасную передачу платежного распоряжения от имени клиента. В этом случае платежное распоряжение получает и перевод средств осуществляет другое финансовое учреждение, обслуживающее банковский счет или платежную карту клиента. Тогда именно оно считается финансовым учреждением, инициирующим платеж.

232. Если оператор цифрового кошелька самостоятельно получает платежное распоряжение и осуществляет перевод средств, он считается финансовым учреждением, инициирующим платеж. Это правило применяется в следующих случаях:

- a. оператор цифрового кошелька хранит денежные средства клиента и осуществляет платеж за счет этих средств; и
- b. оператор цифрового кошелька инициирует платеж путем списания денежных средств непосредственно с банковского счета или с использованием платежного инструмента, находящегося в другом финансовом учреждении.

В обоих случаях определяющее значение имеет то, какое финансовое учреждение получает платежное распоряжение и исполняет его. Источник денежных средств при этом значения не имеет. Они могут находиться как у оператора цифрового кошелька, так и списываться с банковского счета или с использованием платежного инструмента, открытого (выпущенного) другим финансовым учреждением (например, банком-эмитентом платежной карты или финансовым учреждением, в котором открыт привязанный банковский счет).⁵⁴

233. Еще одним важным аспектом при анализе модели функционирования цифрового кошелька является количество платежных распоряжений клиента, на основании которых оператор цифрового кошелька, выполняющий функции финансового учреждения, осуществляет операции. Он может выполнять одну или несколько операций как на основании одного платежного распоряжения, так и на основании нескольких отдельных платежных распоряжений.

⁵⁴ Общие разъяснения по применению требований к информации об источнике происхождения средств приведены в разделе 4.6 главы 4.

234. Если на основании одного платежного распоряжения клиента осуществляются две самостоятельные операции - пополнение цифрового кошелька и последующий платеж, - в соответствии с Рекомендацией 16, как правило, возникают две самостоятельные платежные цепочки. При этом требования к информации об источнике происхождения средств применяются только ко второй из них. Исключение составляют случаи, когда организация выполняет исключительно технические функции, передавая платежное распоряжение финансовому учреждению, осуществляющему перевод средств, без формирования нового платежного распоряжения. В такой ситуации возникает одна платежная цепочка. Если для пополнения цифрового кошелька используется платежная карта, применяются те же требования, что и при непосредственной оплате товаров или услуг этой платежной картой. Если клиент сначала пополняет цифровой кошелек, а затем на основании отдельного платежного распоряжения осуществляет перевод средств с остатка, каждая из этих операций образует самостоятельную платежную цепочку. Требования Рекомендации 16 применяются к каждой платежной цепочке независимо. При этом сведения, переданные в рамках первой платежной цепочки, не требуется передавать во вторую.

8.3.3 Переводы между цифровыми кошельками

235. При осуществлении переводов между цифровыми кошельками одного оператора и между цифровыми кошельками разных операторов применяются следующие правила:

- а. если счета плательщика и получателя находятся в одной юрисдикции и обслуживаются одним и тем же финансовым учреждением, необходимая информация о плательщике и получателе уже имеется у этого финансового учреждения. В этом случае передавать такую информацию вместе с переводом не требуется. Вместе с тем она должна быть доступна компетентным органам в соответствии с требованиями Рекомендации 16.
- б. если счета плательщика и получателя обслуживаются разными операторами цифровых кошельков, финансовые учреждения, участвующие в переводе, должны передавать по платежной цепочке необходимую информацию о плательщике и получателе в соответствии с требованиями Рекомендации 16. Это правило также применяется к переводам между цифровым кошельком и банковским счетом в обоих направлениях.

8.4 Платежи с использованием сервисов мобильных денег

8.4.1 Определения

236. В настоящем разделе используются определения, соответствующие терминологии Обзора по доступности финансовых услуг Международного валютного фонда (IMF Financial Access Survey), а также профильных отраслевых документов

(например, GSMA⁵⁵). Под сервисами мобильных денег понимаются платежные услуги, предоставляемые оператором мобильной связи, его партнером либо независимой организацией, оказывающей аналогичные услуги. Такие сервисы позволяют пользователям хранить денежные средства на счетах, открытых в сервисах мобильных денег, и осуществлять их переводы с использованием мобильного телефона (например, M-Pesa, Orange Money, MTN Mobile Money, GCash, Tigo Money). Регистрация пользователей, а также операции по внесению и выдаче наличных денежных средств, как правило, осуществляются через агентов, функции которых обычно выполняют предприятия розничной торговли.

8.4.2 Основные аспекты применения Рекомендации 16 к платежам с использованием сервисов мобильных денег

237. Операции, осуществляемые с использованием сервисов мобильных денег, подпадают под действие требований Рекомендации 16 наравне с другими платежами и переводами. Системы сервисов мобильных денег должны передавать требуемую информацию о плательщике и получателе либо надежно связывать такую информацию с соответствующей операцией.⁵⁶

238. В некоторых сервисах мобильных денег для инициирования операций используются такие каналы связи, как USSD (неструктурированные дополнительные сервисные данные) или SMS (служба коротких сообщений). Эти каналы предназначены для передачи простых сообщений и могут не поддерживать передачу полностью структурированных платежных данных в составе платежного сообщения. Поэтому операции могут инициироваться с использованием идентификаторов, например номера мобильного телефона, выступающего в качестве гроху-идентификатора. В таких случаях до передачи платежного сообщения по другим каналам связи к гроху-идентификатору должна быть добавлена требуемая информация о плательщике и получателе, сформированная по результатам надлежащей проверки клиента⁵⁷. В течение переходного периода надзорным органам рекомендуется подготовить для операторов сервисов

⁵⁵ Руководство и методические рекомендации по проведению Обзора по доступности финансовых услуг Международного валютного фонда (IMF's Financial Access Survey Guidelines and Manual, [2019 г.](#)); а также [Глоссарий GSMA](#).

⁵⁶ Согласно пункту 2 Пояснительной записки к Рекомендации 1 государства могут в отдельных случаях, если по результатам оценки установлены низкие риски ОД/ФТ, принять решение не применять отдельные рекомендации к определенному виду финансовых учреждений или финансовой деятельности. Вместе с тем такая возможность носит ограниченный характер и не освобождает юрисдикции от обязанности выполнять требования Рекомендации 16 в системах мобильных денег в более широком масштабе.

⁵⁷ С учетом территориального охвата и особенностей клиентской базы сервисов мобильных денег, которые нередко функционируют в условиях ограниченной доступности документов, удостоверяющих личность, получение или проверка полного объема информации, предусмотренной Рекомендацией 16, могут быть затруднены (например, для счетов, открываемых с применением многоуровневой надлежащей проверки клиента (tiered CDD), может отсутствовать возможность получения полной даты рождения или адреса клиента). Кроме того, в сервисах мобильных денег регистрация клиентов часто осуществляется через агентов, что может приводить к различиям в качестве и полноте собираемой информации о клиентах.

мобильных денег разъяснения по вопросам выполнения требований Рекомендации 16, в том числе по применению доступных упрощенных мер (например, альтернативных механизмов и альтернативных методов проверки), а также по проведению проверок соответствия данных (подробнее см. главу 10).

239. В отношении внутренних переводов Рекомендация 16 допускает предоставление необходимой информации иными способами. Поэтому использование в сервисах мобильных денег при передаче платежного сообщения только идентификатора (например, номера мобильного телефона) может соответствовать требованиям Рекомендации 16, если сведения о плательщике и получателе автоматически и надежно связываются с этим идентификатором и могут быть без промедления предоставлены финансовому учреждению получателя и компетентным органам. Если цифровые кошельки плательщика и получателя открыты в одном и том же финансовом учреждении и находятся в одной юрисдикции, передавать такие сведения вместе с переводом не требуется. При этом они должны оставаться доступными для компетентных органов в соответствии с требованиями Рекомендации 16. К трансграничным платежам и переводам применяются соответствующие требования, включая пороговые значения *de minimis*.

Глава 9. Вопросы защиты неприкосновенности частной жизни и персональных данных

9.1 Правовые основания для сбора, обработки и передачи информации в соответствии с Рекомендацией 16

240. Рекомендация 16 предусматривает обязанность субъектов, на которых распространяются ее требования, собирать и передавать информацию о плательщике и получателе. Поскольку такая информация зачастую содержит персональные данные⁵⁸, их обработка должна осуществляться с соблюдением требований защиты неприкосновенности частной жизни и персональных данных, при этом достижение целей реализации Рекомендации 16 не должно противоречить указанным требованиям. Реализация этих целей должна осуществляться с соблюдением изложенных ниже принципов и без ущерба для защиты неприкосновенности частной жизни и персональных данных. Особое значение такие вопросы имеют применительно к: (i) сбору и трансграничной передаче информации о плательщике и получателе, предусмотренной Рекомендацией 16; (ii) требованиям, касающимся выдачи наличных денежных средств за рубежом; и (iii) предоставлению по запросу информации об эмитенте и эквайере платежной карты. При необходимости юрисдикциям следует пересмотреть действующую нормативно-правовую базу в данной сфере с учетом целей ПОД/ФТ/ФРОМУ, предусмотренных Рекомендацией 16.

241. Ниже приведены основные условия, которым должны соответствовать сбор, обработка, передача, хранение и защита персональных данных:

- а) **Законность:** Финансовые учреждения осуществляют сбор, обработку и передачу персональных данных в целях реализации государственной политики в сфере ПОД/ФТ/ФРОМУ в соответствии с требованиями Рекомендации 16, закрепленными в национальном законодательстве. Указанные цели служат основанием для требования о сопровождении платежа или перевода определенным объемом информации и формируют правовую основу для обработки таких данных. Странам следует обеспечивать согласованность

⁵⁸ Термин «персональные данные», также именуемый «информацией, позволяющей установить личность», в большинстве правовых систем имеет широкое толкование. Согласно определению Национального института стандартов и технологий США (NIST), персональные данные - это «информация, которая может использоваться для установления личности физического лица либо отслеживания сведений о нем как самостоятельно, так и в сочетании с иной информацией, связанной или потенциально связанной с конкретным физическим лицом». NIST SP 800-37, Rev. 2, p. 102. Аналогичным образом Общий регламент Европейского союза по защите данных (GDPR) определяет персональные данные как «любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу...; идентифицируемым считается физическое лицо, которое может быть прямо или косвенно идентифицировано, в частности посредством таких идентификаторов, как имя, идентификационный номер, данные о местоположении, онлайн-идентификатор либо одного или нескольких признаков, характеризующих физическую, физиологическую, генетическую, психическую, экономическую, культурную или социальную идентичность такого физического лица». GDPR, ст. 4(1).

законодательства в сфере ПОД/ФТ/ФРОМУ и защиты персональных данных, а также развивать взаимодействие между компетентными органами в целях подготовки единообразных и последовательных разъяснений.

- b) **Эффективная и результативная обработка транзакций:** Сбор, обработка и передача персональных данных в соответствии с Рекомендацией 16 необходимы для осуществления платежей и переводов по распоряжению плательщика. Кроме того, такие данные используются финансовыми учреждениями при мониторинге операций, проверке по целевым финансовым санкциям (TFS) и выявлении несоответствий, которые могут свидетельствовать об ошибках, направлении средств ненадлежащему получателю или подозрительной деятельности (например, мошенничестве). Передача структурированных данных по платежной цепочке также обеспечивает компетентным органам, прежде всего подразделениям финансовой разведки (ПФР) и правоохранительным органам, своевременный доступ к необходимой информации в соответствии с законодательством.

9.2 Основные принципы

242. **Минимизация объема данных.** Рекомендация 16 предусматривает сбор и передачу только тех персональных данных, которые необходимы для соблюдения требований ПОД/ФТ/ФРОМУ. Перечень таких данных приведен в главе 5 настоящего Руководства⁵⁹. Сбор и передача дополнительных персональных данных, не требуемых для достижения указанных целей, Рекомендацией 16 не предусмотрены.

243. **Соразмерность.** Рекомендация 16 предусматривает обработку только тех персональных данных, которые необходимы и соразмерны целям осуществления платежа или перевода, а также целям ПОД/ФТ/ФРОМУ. Объем обрабатываемых данных не должен превышать необходимый для достижения указанных целей. В зависимости от вида и суммы операции Рекомендация 16 устанавливает дифференцированные требования к составу передаваемой информации. Такие требования предусматривают применение альтернативных механизмов (например, упрощенных требований к сведениям об адресе либо использование только года рождения в отдельных случаях), а также пороговых значений *de minimis*. Эти положения должны найти отражение в национальном регулировании. Регуляторам рекомендуется предусмотреть в национальном законодательстве и надзорной практике:

⁵⁹ Например, в ходе двух публичных консультаций, проведенных при пересмотре Рекомендации 16 (в 2024 и 2025 годах), участники отмечали, что включение даты рождения в платежные сообщения способствует более эффективной обработке результатов проверки операций. Это позволяет точнее отличать лиц, включенных в санкционные перечни, от клиентов с совпадающими или схожими именами, сокращает количество ложных срабатываний и объем ручной проверки, тем самым повышая эффективность применения целевых финансовых санкций и обеспечивая соблюдение принципа соразмерности при обработке персональных данных.

- возможность применения указанных альтернативных механизмов, которые в соответствующих случаях являются столь же необходимыми, обоснованными и разумными, как и основные требования; и
- недопустимость необоснованного ограничения применения таких механизмов положениями о защите неприкосновенности частной жизни и персональных данных (DPP), особенно в странах с ограниченными возможностями или при осуществлении трансграничных платежей с участием нескольких юрисдикций.

244. Точность данных. В соответствии со Стандартами ФАТФ персональные данные, собираемые, передаваемые и хранимые в рамках выполнения требований Рекомендации 16, должны быть точными, полными и актуальными в той мере, в какой это необходимо для целей их обработки. Выполнение требований Рекомендации 10 о надлежащей проверке клиента также способствует поддержанию точности и актуальности таких данных. Точные и структурированные персональные данные сокращают количество операционных ошибок, ложных срабатываний, случаев ошибочного направления средств и подозрительных операций, в частности связанных с мошенничеством. Они также повышают эффективность мониторинга в целях ПОД/ФТ/ФРОМУ, ускоряют проведение расследований подразделениями финансовой разведки и правоохранительными органами, а также способствуют пресечению противоправной деятельности. При выявлении ошибок в персональных данных финансовым учреждениям следует вносить необходимые исправления в соответствии с внутренними процедурами ведения учета.

245. Аудит и хранение информации. Финансовые учреждения должны документально подтверждать законность обработки персональных данных. Для этого могут использоваться журналы регистрации, содержащие сведения о целях обработки персональных данных, выполненных действиях по их обработке, а также иные документы, подтверждающие соблюдение требований законодательства. Финансовые учреждения должны установить сроки хранения персональных данных. Персональные данные подлежат хранению в течение срока, установленного законодательством, но не дольше, чем это необходимо для целей их обработки. При установлении сроков хранения принимаются во внимание цели обработки персональных данных, требования законодательства, характер обрабатываемых данных, полномочия лица или органа, осуществляющего их обработку, влияние на права и законные интересы субъектов персональных данных, а также иные требования национального законодательства.

246. Прозрачность. Финансовые учреждения обязаны информировать физических лиц об обработке их персональных данных в случаях, предусмотренных законодательством. Такая информация, как правило, включает:

- цели обработки персональных данных;
- случаи, в которых персональные данные могут передаваться другим лицам, включая государственные органы;
- законодательные и иные нормативные положения, на основании которых осуществляется обработка персональных данных; и

- сведения о правах на доступ к персональным данным, их исправление или уточнение, а также о доступных способах защиты нарушенных прав.

9.3 Имплементация требований Рекомендации 16 в национальное законодательство

247. Для эффективной реализации Рекомендации 16 регуляторам необходимо закрепить в национальном законодательстве правовые основания, объем и условия, при которых финансовые учреждения вправе собирать, обрабатывать, передавать и хранить персональные данные, сопровождающие платежи и переводы.

248. Оценка согласованности законодательства в сфере ПОД/ФТ/ФРОМУ и защиты неприкосновенности частной жизни и персональных данных позволяет на раннем этапе выявить противоречия и правовую неопределенность. В целях гармонизации указанных правовых режимов и устранения препятствий для выполнения требований Рекомендации 16 в национальном законодательстве рекомендуется предусмотреть:

- Четкие правовые основания для обработки персональных данных, предусмотренной Рекомендацией 16, если такая обработка необходима для исполнения требований законодательства или договорных обязательств.
- Перечень персональных данных, которые финансовые учреждения обязаны собирать, передавать и хранить в соответствии с Рекомендацией 16, а также возможность применения альтернативных механизмов в случаях, предусмотренных Стандартами ФАТФ.
- Порядок применения положения о «доступности информации иными способами» (availability by other means) при осуществлении внутренних переводов, исключающий возникновение препятствий для предоставления финансовыми учреждениями информации в сроки, установленные Рекомендацией 16.
- Правовые основания для трансграничной передачи персональных данных между финансовыми учреждениями и компетентными органами в целях ПОД/ФТ/ФРОМУ.
- Административные, технические и физические меры защиты персональных данных, обрабатываемых, передаваемых и хранимых в соответствии с Рекомендацией 16, включая защиту от несанкционированного доступа, утечек и хищения данных, а также киберугроз и иных рисков информационной безопасности. Такие меры должны соответствовать требованиям национального законодательства и учитывать установленные сроки хранения персональных данных.

249. При реализации указанных положений органам, осуществляющим регулирование и надзор в сфере ПОД/ФТ/ФРОМУ, а также органам, ответственным за защиту неприкосновенности частной жизни и персональных данных (DPP), рекомендуется координировать свою деятельность и вырабатывать единые подходы к применению требований Рекомендации 16. При этом следует учитывать опыт применения

действующей редакции Рекомендации 16 в части передачи данных. Вместе с тем в переходный период до 2030 года возможны случаи, когда требования законодательства государства назначения в сфере защиты неприкосновенности частной жизни и персональных данных (DPP) не позволяют однозначно определить возможность передачи отдельных сведений, предусмотренных Рекомендацией 16. Дополнительные сложности могут возникать и в связи с тем, что требования Рекомендации 16 будут внедряться в различных юрисдикциях не одновременно.

250. Во многих правовых системах трансграничная передача персональных данных допускается только при наличии гарантий, обеспечивающих их защиту на всех этапах обработки, передачи и хранения независимо от того, в какую страну они передаются⁶⁰. В ряде государств уполномоченный орган по защите персональных данных оценивает, обеспечивает ли законодательство государства-получателя надлежащий уровень защиты персональных данных. Такая оценка может оформляться в виде решения о достаточности или эквивалентности уровня защиты. Если государство не признано обеспечивающим надлежащий уровень защиты, некоторые правовые режимы допускают применение дополнительных гарантий. В частности, такие гарантии могут предусматриваться договорами между участниками передачи данных, включая финансовое учреждение плательщика, посредников, участвующих в обработке данных, и финансовое учреждение получателя. Кроме того, законодательством могут предусматриваться и иные механизмы, обеспечивающие защиту персональных данных при их трансграничной передаче.

251. В целях создания четкой правовой основы для трансграничной передачи персональных данных государствам рекомендуется прямо закрепить в национальном законодательстве, нормативных актах и разъяснениях, что передача персональных данных в целях ПОД/ФТ/ФРОМУ осуществляется во исполнение требований законодательства в интересах правоохранительной деятельности и в интересах национальной безопасности, а также относится к передаче данных в общественных интересах. В ряде правовых систем это может служить основанием для неприменения отдельных ограничений на трансграничную передачу персональных данных. Такой подход позволит финансовым учреждениям иметь четкие правовые основания для передачи за рубеж сведений, предусмотренных Рекомендацией 16.

252. Если сохраняется правовая неопределенность, органам, осуществляющим регулирование и надзор в сфере ПОД/ФТ/ФРОМУ, а также органам, ответственным за защиту неприкосновенности частной жизни и персональных данных, рекомендуется координировать свою деятельность в целях устранения противоречий между требованиями Рекомендации 16 и национальным законодательством. При необходимости такая координация может осуществляться с компетентными органами иностранных государств. При этом компетентным органам следует учитывать, что

⁶⁰ В некоторых юрисдикциях действуют [требования о локализации данных](#), существенно ограничивающие их трансграничную передачу, что может приводить к фрагментации рынка финансовых услуг.

выполнение требований Рекомендации 16 предполагает передачу определенных категорий сведений, включая персональные данные, независимо от государства назначения.

253. Если законодательство государства назначения не предусматривает сопоставимый уровень защиты неприкосновенности частной жизни и персональных данных, особое значение приобретают меры по защите персональных данных, принимаемые до их передачи. К таким мерам относятся передача только тех сведений, которые предусмотрены Рекомендацией 16, без дополнительных персональных данных, включение положений о защите персональных данных в соглашения с финансовыми учреждениями - получателями информации, использование переданных данных исключительно в целях ПОД/ФТ/ПРОМУ, а также ведение учета передаваемых данных с указанием состава переданной информации, получателя и даты передачи. Если противоречия между требованиями Рекомендации 16 и нормами в сфере защиты неприкосновенности частной жизни и персональных данных сохраняются, финансовым учреждениям рекомендуется обращаться за разъяснениями к компетентным органам.

Вставка 16. – Пример реализации на национальном уровне требований в сфере защиты неприкосновенности частной жизни и персональных данных и Рекомендации 16

Европейский союз

В частности, Регламент регулирует вопросы законности обработки персональных данных, получения согласия субъекта персональных данных, обработки специальных категорий персональных данных и реализации прав субъектов персональных данных. Кроме того, он устанавливает требования к минимизации данных, учету требований по защите персональных данных при разработке информационных систем и процессов обработки данных, применению настроек защиты персональных данных по умолчанию, а также их безопасности. Предусмотренные GDPR меры защиты применяются независимо от способа передачи персональных данных, включая их передачу в составе платежных сообщений и предоставление по запросу.

Одновременно Европейский союз имплементировал положения предыдущей редакции Рекомендации 16, приняв Регламент о сведениях, сопровождающих переводы денежных средств и отдельных криптоактивов (Transfer of Funds Regulation, TFR). Статья 25 TFR прямо предусматривает, что обработка персональных данных при применении этого Регламента осуществляется с соблюдением требований GDPR. Тем самым была сформирована единая правовая основа, позволяющая финансовым учреждениям одновременно соблюдать требования законодательства в сфере ПОД/ФТ и законодательства о защите персональных данных. При подготовке TFR Европейская комиссия также провела ряд консультаций с Европейским инспектором по защите данных.

Согласно GDPR, в случае утечки персональных данных об этом необходимо

незамедлительно уведомить контролера персональных данных, а если утечка соответствует установленным критериям, - также компетентный орган по защите персональных данных.

254. Надзорным органам и финансовым учреждениям следует последовательно применять указанные выше меры защиты на всех этапах платежной цепочки. В частности, необходимо ограничивать использование персональных данных целями ПОД/ФТ/ФРОМУ, обеспечивать их конфиденциальность и безопасность при передаче и хранении, применять необходимые технические и организационные меры защиты, а также осуществлять хранение и трансграничную передачу персональных данных в соответствии с национальным законодательством и требованиями Рекомендации 11.

Вставка 17. –Примеры механизмов трансграничной передачи персональных данных и применяемых при этом мер защиты

Совместное соглашение между странами (решение о достаточности уровня защиты данных)⁶¹

США и Европейский союз сформировали механизм трансграничной передачи персональных данных в рамках программы **EU-US Data Privacy Framework**. Она предусматривает меры защиты персональных данных и механизмы защиты прав субъектов персональных данных при передаче персональных данных из Европейского союза участвующим в программе американским компаниям, а также государственным органам США, которые могут получать такие данные в целях правоохранительной деятельности или в интересах национальной безопасности.

Договорный механизм: Обязательные корпоративные правила ЕС (Binding Corporate Rules, BCR)⁶²

Обязательные корпоративные правила (BCR) устанавливают основные принципы защиты персональных данных и закрепляют права субъектов персональных данных, позволяющие поддерживать надлежащий уровень защиты при передаче данных внутри группы компаний. Компании Европейского союза обязаны представлять свои BCR на утверждение компетентному органу по защите персональных данных. Европейский союз ведет перечень утвержденных BCR. Использование таких договорных механизмов способствует реализации мер защиты при трансграничной передаче персональных данных.

Вставка 18. - Безопасность каналов обмена информацией

Платформа SWIFT применяет обязательные меры защиты информации в рамках Системы контроля безопасности клиентов (CSCF), основанной на международных стандартах NIST, ISO 27000 и PCI-DSS. К таким мерам относятся сквозное

⁶¹ [США и ЕС одобрили рамочную концепцию передачи персональных данных](#)

⁶² [Обязательные корпоративные правила ЕС](#)

шифрование данных и обязательная процедура подтверждения соответствия требованиям безопасности. Данный подход демонстрирует, какие меры защиты целесообразно применять при трансграничной передаче платежных сообщений, содержащих персональные данные.

Практика сопоставления требований различных стандартов информационной безопасности получает все более широкое распространение. Это позволяет организациям, внедрившим систему управления информационной безопасностью в соответствии с NIST Cybersecurity Framework 2.0 или ISO/IEC 27001:2022, использовать уже реализованные меры защиты для выполнения требований других стандартов информационной безопасности. Если организация уже внедрила международно признанный стандарт информационной безопасности, ей значительно проще пройти оценку на соответствие требованиям других организаций, чем при использовании стандартов, не получивших международного признания.

Предварительное проведение внутреннего аудита позволяет выявить и устранить возможные недостатки до прохождения сертификации и подтверждения соответствия требованиям указанных стандартов, что снижает риск получения замечаний по итогам внешнего аудита.

9.4 Требования к информационной безопасности и данным повышенного риска

255. Финансовые учреждения должны применять организационные, технические и физические меры защиты персональных данных. Такие меры защищают персональные данные и предотвращают их случайное или незаконное уничтожение, случайную утрату, несанкционированное раскрытие, изменение, неправомерный доступ и иные нарушения при обработке персональных данных.

256. Отдельные категории персональных данных, передача которых предусмотрена или допускается Рекомендацией 16, в случае их компрометации могут создавать повышенные риски для защиты неприкосновенности частной жизни и персональных данных, особенно при использовании в сочетании с другими сведениями. К таким данным, в частности, относятся уникальные государственные идентификаторы, номера счетов, адрес и дата рождения.

257. Надзорным органам и финансовым учреждениям при выборе мер защиты рекомендуется учитывать повышенную чувствительность отдельных категорий данных и риски их неправомерного использования. Для таких данных может потребоваться более высокий уровень защиты. При этом не рекомендуется устанавливать обязательные требования к применению конкретных технологий или технических решений. В качестве дополнительных мер защиты могут использоваться усиленный контроль доступа, более надежные средства шифрования и иные средства защиты при передаче и хранении данных, регистрация доступа к информации, а также установление сроков хранения данных в соответствии с принципом соразмерности и Рекомендацией 11.

258. При обработке персональных данных, собираемых или передаваемых в целях ПОД/ФТ/ФРОМУ, меры по их защите должны применяться всеми участниками платежной цепочки. Это требование распространяется также на организации, не являющиеся финансовыми учреждениями, но обрабатывающие сведения, предусмотренные Рекомендацией 16, по их поручению, включая технических поставщиков и поставщиков услуг в сфере информационно-коммуникационных технологий. Если финансовое учреждение передает обработку таких сведений третьим лицам, обязанность по их защите должна быть предусмотрена договором.

259. Финансовые учреждения могут использовать технологии повышения конфиденциальности (Privacy-Enhancing Technologies, PETs), если это соответствует требованиям Рекомендации 16 и позволяет повысить уровень защиты персональных данных без избыточного раскрытия информации. Применение таких технологий носит рекомендательный характер и не предполагает использования каких-либо конкретных технических решений.⁶³ Вместе с тем PETs являются лишь одним из инструментов защиты конфиденциальности информации и не заменяют иные меры по защите персональных данных и неприкосновенности частной жизни. Использование PETs должно быть частью комплексной системы защиты персональных данных.

260. Независимо от размера финансового учреждения процедуры реагирования на утечки данных необходимо регулярно актуализировать с учетом изменений законодательства, нормативных требований и рекомендаций. При разработке и совершенствовании таких процедур рекомендуется использовать актуальные методические материалы, в том числе NIST SP 800-61 Rev. 3.

261. Финансовым учреждениям также рекомендуется проверить, учитывают ли действующие процедуры реагирования на утечки данных риски, характерные для их деятельности, в том числе:

- утрату сообщений о подозрительных операциях;⁶⁴
- выявление нетипичного поведения клиентов или изменений в сведениях о клиентах;⁶⁵ и
- координацию между подразделениями (или процессами), осуществляющими реагирование на утечки данных и выявление мошенничества.

⁶³ См. ФАТФ. *Взаимодействие в борьбе с финансовыми преступлениями: защита данных, технологии и обмен информацией между организациями частного сектора*, 2022. <https://www.fatf-gafi.org/en/publications/Digitaltransformation/Partnering-in-the-fight-against-financial-crime.html>.

⁶⁴ ФАТФ. *Руководство по обмену информацией между организациями частного сектора*. 2017. <https://www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-information-sharing.html>

⁶⁵ AUSTRAC. *Утечки данных и вопросы ПОД/ФТ*. <https://www.austrac.gov.au/industry-and-business/obligations-and-guidance/additional-guidance/data-breaches-and-amlctf-considerations#mitigate-and-manage-ongoing-customer-risks>

9.5 Особенности применения Рекомендации 16 к карточным платежам и выдаче наличных денежных средств за рубежом

262. Обновленная Рекомендация 16 содержит специальные требования к карточным платежам и выдаче наличных денежных средств за рубежом (см. главы 6 и 7).

263. В соответствии с Рекомендацией 16 номер платежной карты относится к обязательной информации, передаваемой между финансовым учреждением-эмитентом карты и финансовым учреждением-эквайером. При оплате товаров и услуг платежными картами сведения о наименовании и местонахождении эмитента и эквайера должны предоставляться по запросу через справочные сервисы платежной системы. Включать эти сведения непосредственно в платежное сообщение не требуется. При выдаче наличных денежных средств за рубежом финансовое учреждение - эквайер вправе по запросу получить информацию об имени держателя карты.

264. Сведения о номерах платежных карт и именах их держателей могут использоваться злоумышленниками для совершения мошеннических платежей и переводов. В связи с этим при передаче, обработке и хранении таких сведений необходимо обеспечивать их безопасность и конфиденциальность.

265. При карточных операциях важно передавать данные по защищенным каналам связи, обеспечивающим разграничение доступа, конфиденциальность информации и возможность проведения аудита. В международной практике для защиты данных при карточных операциях применяется стандарт PCI DSS⁶⁶. Кроме того, используются и другие отраслевые стандарты информационной безопасности. Платежные системы уже располагают глобальной инфраструктурой защиты данных, которая обеспечивает безопасную передачу информации о карточных операциях между эмитентами и эквайерами, в том числе при трансграничных операциях. Благодаря этому обмен такими данными возможен даже между юрисдикциями, в которых действуют разные требования к защите персональных данных. Если Рекомендация 16 предусматривает трансграничную передачу данных платежной карты или ее держателя, важно использовать защищенные каналы связи и соблюдать требования законодательства в области защиты персональных данных. Соответствие принимающего финансового учреждения требованиям PCI DSS свидетельствует о достаточном уровне защиты данных.

266. Важную роль в защите данных при карточных операциях играют и компетентные органы. Они имеют возможность получать сведения о платежных картах и их держателях

⁶⁶ Стандарт PCI DSS разработан для повышения уровня защиты данных платежных карт. Он устанавливает единые требования к безопасности данных, применяемые во всем мире. PCI DSS определяет минимальный набор технических и организационных требований, направленных на защиту данных платежных карт, включая создание защищенной сетевой инфраструктуры и информационных систем, а также применение надежных механизмов разграничения доступа. В соответствии с PCI DSS к данным платежного счета относятся номер платежной карты (PAN), имя держателя карты, срок действия карты и сервисный код.

для целей ПОД/ФТ, главным образом при проведении расследований. Взаимодействие компетентных органов, ответственных за реализацию требований Рекомендации 16 к карточным операциям, с органами, ответственными за защиту неприкосновенности частной жизни и персональных данных, способствует единообразному толкованию и применению соответствующих требований.

267. Компетентные органы, запрашивающие у финансовых учреждений информацию о карточных операциях, должны учитывать требования национального законодательства, регулирующего обработку, использование и защиту таких сведений. Внутренние правила, регулирующие вопросы защиты неприкосновенности частной жизни и персональных данных, следует разрабатывать с учетом чувствительного характера такой информации и рисков ее утечки. При разработке таких правил, а также при работе с данными о карточных операциях компетентным органам необходимо руководствоваться отраслевыми стандартами защиты данных, в том числе PCI DSS.

9.6 Вопросы защиты персональных данных при использовании комплексных систем постоянного мониторинга

268. Системы комплексного мониторинга могут использовать более широкий состав данных, чем предусмотрено Рекомендацией 16, - в частности, поведенческие признаки, сведения о характере ранее совершённых операций, а в отдельных случаях и информацию в масштабе всей платёжной сети. Обработка таких данных может подпадать под действие законодательства, регулирующего применение искусственного интеллекта. Указанные подходы способны существенно повысить эффективность выявления мошенничества и иной противоправной деятельности, однако предполагают обработку значительных объёмов данных. В связи с этим их применение должно учитывать уровень риска, соответствовать поставленным целям, а также отвечать требованиям соразмерности и разумности. При необходимости принимаемые такими системами решения должны находиться под контролем человека.

269. Во многих странах законодательство в сфере защиты персональных данных ограничивает принятие решений, способных существенно затронуть права и законные интересы физических лиц, исключительно на основе автоматизированной обработки персональных данных без участия человека. Исключения возможны только в случаях, предусмотренных законодательством государства плательщика и государства получателя, при условии применения надлежащих мер защиты, включая возможность пересмотра такого решения с участием человека.

270. Как отмечалось в разделе 9.4, финансовые учреждения могут использовать технологии повышения конфиденциальности (PETs) для более эффективного мониторинга и ограничения избыточного раскрытия данных, если это соответствует требованиям Рекомендации 16.

271. Использование систем комплексного постоянного мониторинга предполагает наличие эффективной системы корпоративного управления, прозрачных правил обработки данных, разграничения доступа к информации, защищенной среды обработки данных и надлежащего контроля за функционированием таких систем.

Глава 10. Механизмы проверки соответствия данных

10.1 Обоснование проведения проверок соответствия данных

272. Цель Рекомендации 16 заключается в том, чтобы финансовые учреждения плательщика, финансовые учреждения-посредники и финансовые учреждения получателя располагали основной информацией о плательщике и получателе перевода сразу после проведения операции. Это необходимо, в частности, для выявления и сообщения о подозрительных операциях. Проверка соответствия данных, то есть проверка того, что получателем, указанным в платежном сообщении, является именно то лицо, которому плательщик намеревался перевести средства, позволяет предотвратить ошибки, выявить мошенничество и иную подозрительную деятельность, а также повысить качество информации, используемой финансовыми учреждениями получателя для целей ПОД/ФТ/ФРОМУ.

273. Платежи, направленные ненадлежащему получателю, могут быть следствием мошенничества, легализации (отмывания) преступных доходов или обычной ошибки. Доходы, полученные преступным путем, нередко переводятся через платежные системы с использованием недостоверных или подмененных сведений о получателе. Проверки соответствия данных позволяют своевременно выявлять такие случаи, способствуют противодействию мошенничеству и дополняют иные меры, применяемые финансовыми учреждениями получателя.

274. Вероятность возникновения ошибок при направлении платежей зависит от юрисдикции, сегмента платежного рынка, используемого платежного коридора, а также вида платежного продукта или услуги. Поэтому проверки соответствия данных должны проводиться с применением риск-ориентированного подхода, а их объем и порядок - соответствовать уровню выявленных рисков.

10.2 Обзор вариантов внедрения

275. Компетентные органы должны установить требование, согласно которому финансовые учреждения получателя при осуществлении трансграничных переводов, превышающих порог *de minimis*, принимают меры для снижения риска перечисления средств ненадлежащему получателю. Пояснительная записка к Рекомендации 16 предусматривает несколько вариантов выполнения этого требования путем проведения проверок соответствия данных. Выбор конкретного варианта зависит от особенностей способов осуществления платежей, применяемых бизнес-моделей и имеющихся технических возможностей. В соответствии с пунктом 30 Пояснительной записки к Рекомендации 16 положения настоящего раздела адресованы прежде всего финансовым учреждениям получателя.

276. В соответствии с Пояснительной запиской к Рекомендации 16 финансовые учреждения получателя должны применять по меньшей мере один из следующих механизмов проверки соответствия данных:

- a. При проведении каждой операции проверять, соответствуют ли имя получателя и номер его счета, указанные в платежном сообщении, сведениям, имеющимся в распоряжении финансового учреждения получателя; или
- b. Осуществлять комплексный постоянный мониторинг с применением риск-ориентированного подхода для выявления аномальных счетов, операций, иной подозрительной активности и случаев несоответствия сведений о получателе; либо
- c. Если финансовое учреждение плательщика и финансовое учреждение получателя являются участниками механизма предварительной проверки данных получателя (например, механизма подтверждения (верификации) получателя), финансовое учреждение получателя вправе использовать этот механизм вместо механизмов, предусмотренных подпунктами «а» или «б» настоящего пункта. При этом такой механизм должен обеспечивать проверку соответствия имени получателя и номера его счета, указанных в платежном сообщении, сведениям, имеющимся в распоряжении финансового учреждения получателя, до проведения каждой операции.

277. В следующих разделах рассматриваются основные принципы механизмов проверки соответствия данных и область их применения.

10.3 Понятие проверки соответствия данных

278. Проверка личности получателя и проверка соответствия данных, проводимая финансовым учреждением получателя, осуществляются на разных этапах и преследуют разные цели. Проверка личности получателя является одним из элементов надлежащей проверки клиента и проводится при установлении деловых отношений с клиентом, а также в процессе его дальнейшего обслуживания.

279. В отличие от проверки личности получателя, проверки соответствия данных проводятся применительно к каждому трансграничному переводу, превышающему порог *de minimis*. Их цель заключается не в повторной проверке личности получателя, а в том, чтобы установить, насколько сведения о получателе, содержащиеся в платежном сообщении, соответствуют информации, уже имеющейся у финансового учреждения получателя, прежде всего имени получателя и идентификатору его счета. Таким образом, проверки соответствия данных позволяют убедиться, что средства направляются именно тому клиенту, личность которого уже установлена, снизить риск ошибочных или мошеннических платежей, а также повысить качество и достоверность сведений о получателе, содержащихся в платежных сообщениях.

280. Проверка соответствия данных не требует полного совпадения сведений о получателе и номере его счета, указанных в платежном сообщении, с информацией, имеющейся у финансового учреждения получателя. Достаточно, чтобы они соответствовали друг другу в разумной степени. Поэтому при проведении проверки оценивается не только факт совпадения или несовпадения данных, но и степень их соответствия. Для этого финансовые учреждения могут использовать алгоритмы

нечеткого сопоставления (fuzzy matching) или иные методы, позволяющие определить, что сведения о получателе:

- соответствуют имеющейся информации;
- в целом соответствуют, несмотря на незначительные расхождения; или
- имеют существенные расхождения с имеющейся информацией.

281. Не всякое расхождение в сведениях о получателе следует рассматривать как их несоответствие. К допустимым расхождениям относятся, в частности, незначительные орфографические ошибки или опечатки, сокращения, обычно используемые в наименованиях юридических лиц (например, «Ltd» вместо «Limited»), использование фирменного или коммерческого наименования вместо официального, различия в порядке указания элементов имени, отсутствие отчества или инициалов, отсутствие диакритических знаков или специальных символов, различия, обусловленные транслитерацией, а также указание имени только одного из владельцев совместного счета. Подобные расхождения могут выявляться с помощью алгоритмов нечеткого сопоставления (fuzzy matching) или иных методов (например, допускающих определенный уровень расхождений, рассчитанный с использованием расстояния Левенштейна⁶⁷), а не путем посимвольного сравнения данных. При этом выбор таких методов должен осуществляться с учетом уровня риска и особенностей деятельности конкретного финансового учреждения.

282. При проведении проверки соответствия данных следует учитывать уровень риска и обстоятельства конкретной операции. При этом могут приниматься во внимание, в частности, профиль риска клиента, характер и цель платежа, сумма и периодичность операции (при наличии соответствующей информации), риски, связанные со страной или сектором экономики, а также используемый платежный канал. В отношении операций с повышенным уровнем риска или нетипичных операций может применяться более строгий подход к оценке соответствия данных, тогда как для операций с низким уровнем риска и стандартных платежей, как правило, достаточно более гибкого подхода.

283. Существенное несоответствие данных, как правило, имеет место, если имя получателя, указанное в платежном сообщении, полностью отличается от имени, связанного со счетом получателя, явно не соответствует виду счета (например, если для счета юридического лица указано имя физического лица) либо не относится ни к одному из клиентов, связанных с данным счетом, по информации, имеющейся у финансового учреждения получателя (например, в случае совместного счета). При оценке существенности такого несоответствия могут учитываться и дополнительные сведения, помимо предусмотренных пунктом 30 Пояснительной записки к Рекомендации 16 (например, адрес). Подобные случаи следует рассматривать как возможные признаки

⁶⁷ Расстояние Левенштейна - способ сравнения текстовых строк, который показывает, сколько символов необходимо изменить, удалить или добавить, чтобы одна запись совпала с другой. Благодаря этому можно учитывать незначительные ошибки в написании без признания записей разными. Прим. ред.

перечисления средств ненадлежащему получателю, ошибки, мошенничества или иной противоправной деятельности и принимать соответствующие меры с применением риск-ориентированного подхода.

10.4 Область применения проверок соответствия данных

284. Проверки соответствия данных должны проводиться как минимум в отношении имени получателя и идентификатора его счета при осуществлении трансграничных переводов, превышающих порог *de minimis*. Это позволяет убедиться, что средства направляются надлежащему получателю, а также снизить риск перечисления средств ненадлежащему получателю, ошибочных или мошеннических переводов.

285. Обязательная проверка соответствия данных распространяется только на те сведения, которые позволяют наиболее эффективно выявлять случаи перечисления средств ненадлежащему получателю. К ним относятся имя получателя и идентификатор его счета. Эти сведения постоянно доступны финансовым учреждениям и непосредственно связаны с риском ошибочного или мошеннического перевода средств. При проведении такой проверки финансовые учреждения не обязаны проверять правильность иных сведений о получателе по каждой операции или повторно проводить полную проверку информации о клиенте.

286. При проведении проверок соответствия данных в отношении юридических лиц финансовые учреждения могут использовать иные сведения, позволяющие однозначно идентифицировать получателя, если такая информация имеется в их распоряжении. К таким сведениям относятся, например, налоговый номер, идентификатор юридического лица (LEI или BIC) либо иной официальный идентификатор. Использование таких идентификаторов во многих случаях позволяет точнее оценить соответствие данных, чем сопоставление только по наименованию получателя.

10.5 Реализация механизмов проверки соответствия данных

10.5.1 *Переходный период и особенности практической реализации*

287. В переходный период наиболее сложной может оказаться реализация механизмов предварительной проверки данных, поскольку для их функционирования необходимо участие в единой системе как финансового учреждения плательщика, так и финансового учреждения получателя. Вместе с тем обязанность финансового учреждения получателя проводить проверки соответствия данных сохраняется независимо от того, участвует ли финансовое учреждение плательщика в соответствующей системе или механизме. Если механизм предварительной проверки использовать невозможно, финансовое учреждение получателя должно применять иной механизм проверки соответствия данных. Например, последующую проверку данных или комплексный постоянный мониторинг.

288. Надзорным органам следует установить четкие требования к тому, как финансовые учреждения должны выполнять обязанности по проведению проверок соответствия данных при осуществлении трансграничных операций с финансовыми учреждениями из юрисдикций, еще не внедривших требования Рекомендации 16. Это позволит обеспечить единообразный подход в переходный период.

289. Эффективность применения механизмов проверки соответствия данных во многом зависит от того, насколько они согласованы с механизмами, используемыми финансовыми учреждениями-контрагентами.

10.5.2 Последующая проверка данных (п. 30(а) Пояснительной записки к Рекомендации 16)

290. Последующая проверка данных применяется в случаях, когда финансовое учреждение получателя не использует механизмы предварительной проверки данных или комплексный постоянный мониторинг для проведения проверок соответствия данных. Такой механизм служит альтернативным способом выполнения указанных обязанностей и позволяет финансовым учреждениям получателя выявлять случаи перечисления средств ненадлежащему получателю, в том числе при осуществлении трансграничных операций или в юрисдикциях, где применение иных механизмов затруднено.

291. Если финансовое учреждение получателя использует последующую проверку данных, она должна проводиться в отношении каждого входящего трансграничного перевода, превышающего порог *de minimis*. По каждой такой операции финансовое учреждение получателя должно оценивать, соответствуют ли имя получателя и идентификатор его счета, указанные в платежном сообщении, информации, имеющейся в его распоряжении.

292. По общему правилу последующая проверка данных должна проводиться, насколько это возможно, до предоставления получателю доступа к средствам, то есть до их зачисления на его счет. Если этому препятствуют особенности работы платежной системы, требования законодательства или правила соответствующей платежной схемы (например, при осуществлении мгновенных платежей), финансовое учреждение получателя вправе, если это допускается законодательством и соответствует риск-ориентированному подходу, на непродолжительное время отложить зачисление средств для проведения последующей проверки данных и принятия необходимых мер по ее результатам. Такой подход должен быть разумным и соразмерным, обеспечивая баланс между снижением риска перечисления средств ненадлежащему получателю и недопущением необоснованных задержек при осуществлении трансграничных платежей. Последующая проверка данных может также использоваться совместно с другими механизмами проверки соответствия данных (например, комплексным постоянным мониторингом), если выявленные расхождения требуют дополнительного анализа.

293. Процессы и информационные системы, используемые при проведении последующей проверки данных, должны своевременно выявлять случаи существенного несоответствия данных и принимать необходимые меры в соответствии с внутренними документами финансового учреждения.

Вставка 19. Страновой пример применения механизмов последующей проверки данных

Гонконг, Китай

Денежно-кредитное управление Гонконга требует, чтобы банки проверяли, соответствует ли имя получателя, указанное в платежном сообщении, сведениям, которыми располагает финансовое учреждение получателя, при осуществлении переводов через Систему быстрых платежей (Faster Payment System - система мгновенных платежей Гонконга), а также через аналогичные системы внутрибанковских переводов. Если имя получателя, указанное в платежном сообщении, не соответствует сведениям финансового учреждения получателя, перевод отклоняется. При проведении такой проверки банки должны применять риск-ориентированный подход, в том числе при определении пороговой суммы, начиная с которой проводится проверка. При этом такая сумма не должна превышать 1 000 гонконгских долларов (около 130 долларов США).

10.5.3 Комплексный постоянный мониторинг

294. В качестве одного из способов выполнения обязанностей по проведению проверок соответствия данных компетентные органы могут предусмотреть использование финансовыми учреждениями получателя механизмов комплексного постоянного мониторинга, основанных на риск-ориентированном подходе. При оценке эффективности таких механизмов надзорным органам следует исходить из результатов работы системы в целом, а не оценивать каждый ее элемент изолированно. В целях выполнения требований Рекомендации 16 механизмы комплексного постоянного мониторинга основаны на постоянном анализе операций и поведенческих моделей по счету получателя для выявления аномальной активности. В частности, они позволяют выявлять случаи существенного несоответствия между именем получателя и идентификатором его счета, указанными в платежном сообщении, и сведениями, которыми располагает финансовое учреждение получателя, при осуществлении трансграничных переводов, превышающих порог *de minimis*.

295. Механизмы комплексного постоянного мониторинга могут анализировать как отдельные операции, так и поведение клиента или характер совершаемых им операций в целом, а также учитывать показатели риска, определяемые финансовым учреждением в рамках риск-ориентированного подхода. В отличие от проверки каждой операции по отдельности такие механизмы позволяют учитывать поведенческие и иные факторы риска, установленные финансовым учреждением. В платежных системах, осуществляющих трансграничные платежи, механизмы комплексного постоянного мониторинга должны функционировать с учетом скорости обработки операций и особенностей соответствующей платежной системы, а также характера платежа и уровня риска. По возможности проверка в рамках комплексного постоянного мониторинга должна проводиться до исполнения, клиринга, расчета или зачисления средств, чтобы снизить риск их быстрого вывода.

296. Для выполнения требований подпункта (b) пункта 30 Пояснительной записки к Рекомендации 16 механизмы комплексного постоянного мониторинга должны учитывать случаи несоответствия данных о получателе как один из значимых факторов

анализа, а не только как информацию для последующей оценки. На практике несоответствие имени получателя является лишь одним из признаков, используемых для выявления аномальных счетов, операций или мошеннических схем. К числу таких признаков могут относиться, в частности, неоднократные случаи несоответствия данных о получателе, переводы в пользу получателей, связанных с повышенным риском мошенничества, первые переводы между плательщиком и получателем, а также иные показатели риска, определенные финансовым учреждением. Механизмы комплексного постоянного мониторинга могут сочетать мониторинг в режиме реального времени, мониторинг с минимальной задержкой и последующий мониторинг, образуя единую систему контроля. Использование только периодических проверок соблюдения требований, выборочного контроля, внутреннего аудита или иных последующих контрольных процедур само по себе не является достаточным, особенно в системах, осуществляющих мгновенные или почти мгновенные платежи. Вместе с тем последующие контрольные процедуры могут использоваться как элемент комплексной системы мониторинга, если они дополняют мониторинг в режиме реального времени или мониторинг с минимальной задержкой и соответствуют уровню рисков ОД/ФТ, мошенничества или ошибок.

297. При оценке эффективности механизмов комплексного постоянного мониторинга могут учитываться, в частности, следующие факторы:

- Своевременность - проводится ли мониторинг с учетом скорости обработки операций, особенностей соответствующей системы, осуществляющей трансграничные платежи, а также уровня риска; выполняются ли проверки до или после исполнения, клиринга, расчета либо зачисления средств, если это возможно и оправдано с учетом уровня риска;
- Охват - включает ли механизм ключевые показатели, необходимые для проверки соответствия данных, в том числе случаи несоответствия имени получателя и идентификатора его счета, наряду с другими признаками аномальной активности; и
- Взаимодействие с другими механизмами проверки соответствия данных - каким образом комплексный постоянный мониторинг дополняет механизмы предварительной или последующей проверки данных, если они также применяются.

298. Механизмы комплексного постоянного мониторинга могут сочетать различные виды мониторинга, включая:

- анализ на уровне клиента, в том числе информации, полученной в рамках процедур надлежащей проверки клиента, оценку уровня риска клиента, а также анализ его ожидаемого поведения и характера совершаемых операций; и
- анализ на уровне операций, включая мониторинг операций, проверку по санкционным спискам, использование инструментов выявления мошенничества, анализ поведенческих особенностей и иных признаков, позволяющих выявлять нетипичную активность.

299. При проведении комплексного постоянного мониторинга несоответствие имени получателя может использоваться как один из признаков аномальной активности. При этом могут учитываться, в частности, регулярное возникновение несоответствий данных при переводах из определенных финансовых учреждений плательщика, от отдельных клиентов либо по отдельным платежным коридорам, а также признаки, характерные для мошенничества или деятельности «денежных мулов» (например, поступление большого количества переводов на один счет с последующим быстрым перечислением средств).

10.5.4 Предварительная проверка данных

300. Компетентные органы и финансовые учреждения могут выполнять обязанности по проведению проверок соответствия данных с помощью механизмов предварительной проверки, таких как Confirmation of Payee (CoP)⁶⁸ и Verification of Payee (VoP)⁶⁹. Такие механизмы позволяют финансовому учреждению плательщика до инициирования платежа или перевода направить запрос финансовому учреждению получателя и проверить, соответствуют ли имя получателя и идентификатор его счета, указанные в платежном сообщении, сведениям, которыми располагает финансовое учреждение получателя. Предварительная проверка может проводиться и по иным данным, позволяющим однозначно идентифицировать получателя, например по налоговому номеру, идентификаторам юридического лица (LEI или BIC) либо другим уникальным официальным идентификаторам, если такие данные доступны. Использование этих идентификаторов может повысить точность проверки соответствия данных по сравнению с сопоставлением только по имени получателя.

301. Поскольку такие механизмы предусматривают прямой обмен информацией между финансовым учреждением плательщика и финансовым учреждением получателя, их применение возможно только в случае участия обоих финансовых учреждений в одном механизме предварительной проверки либо если они используют общий набор правил и технических стандартов. Такое участие должно обеспечивать возможность проведения проверок CoP/VoP по каждой операции путем сопоставления имени получателя и идентификатора его счета, указанных в платежном сообщении, со сведениями, имеющимися у финансового учреждения получателя. Если финансовое учреждение плательщика предоставляет клиентам возможность заранее зарегистрировать получателей платежей, проверки CoP/VoP могут проводиться при регистрации получателя, а не при каждой отдельной операции. Исключения могут

⁶⁸ Система, используемая в Великобритании и некоторых других странах, которая позволяет отправителю платежа проверить, соответствует ли имя получателя указанным банковским реквизитам (счету и коду банка). Это помогает предотвратить переводы на неправильные счета и защищает от мошенничества, связанного с подменой данных получателя. Прим. пер.

⁶⁹ Широкий термин, охватывающий различные способы подтверждения получателя платежа. В зависимости от страны и платежной системы, VoP может включать механизмы проверки на основе идентификаторов клиентов, номеров телефонов, e-mail и других реквизитов. Направлена на повышение безопасности платежей и снижение случаев ошибочных или мошеннических переводов. Прим. пер.

предусматриваться в отдельных случаях, например при осуществлении пакетных платежей, переводов в пользу юридических лиц либо при отказе клиента от использования такого механизма, если это допускается правилами.

302. Механизмы предварительной проверки могут использоваться не только для сопоставления имени получателя и идентификатора его счета. В некоторых платежных системах они также позволяют до инициирования перевода подтвердить возможность его зачисления на счет получателя. Такая процедура проводится по единым правилам, установленным соответствующей платежной системой. В ходе предварительной проверки финансовое учреждение получателя подтверждает, что перевод может быть зачислен на счет получателя. В частности, проверяется, что счет является действующим, не превышены установленные лимиты операции и выполнены требования по надлежащей проверке клиента. Полученное подтверждение передается финансовому учреждению плательщика через платежную систему. Перевод осуществляется только после подтверждения операции финансовым учреждением плательщика и самим плательщиком. Если технические средства позволяют зафиксировать согласованные условия до исполнения перевода, это обеспечивает дополнительную гарантию того, что средства будут переведены именно предполагаемому получателю. Компетентным органам следует формировать нормативно-правовую базу таким образом, чтобы она не препятствовала внедрению новых механизмов предварительной проверки, если они позволяют достичь целей проверки соответствия данных, предусмотренных Рекомендацией 16.

Вставка 20. Механизмы CoP/VoP

Все больше стран внедряют механизмы CoP/VoP в рамках реализации мер, направленных на создание систем проверки платежей, позволяющих в режиме реального времени снижать риск мошенничества и ошибочного направления платежей.

Европейский союз

С октября 2025 года Регламент Европейского союза о мгновенных платежах (Instant Payments Regulation, Регламент (ЕС) 2024/886) обязывает финансовые учреждения, расположенные в странах еврозоны, финансовые учреждения, расположенные в странах еврозоны, обязаны предоставлять клиентам механизмы CoP/VoP при осуществлении всех внутренних переводов в евро в пределах Европейского союза.⁷⁰

- Указанное требование распространяется как на мгновенные, так и на обычные переводы в евро; и
- Данное требование не применяется к другим способам осуществления платежей, включая прямое дебетование и переводы виртуальных активов.

⁷⁰ С июля 2027 года данное требование будет применяться также к финансовым учреждениям, расположенным в государствах-членах Европейского союза, но не входящих в еврозону.

В соответствии с Регламентом финансовые учреждения обязаны внедрить механизм, позволяющий плательщику до подтверждения платежного поручения проверить, соответствует ли идентификатор счета получателя (например, IBAN) имени получателя, указанному при оформлении перевода. В Европейском союзе поставщики технических услуг оказывают финансовым учреждениям содействие во внедрении механизмов CoP/VoP.

Великобритания

В 2020 году в Великобритании был внедрен механизм проверки имени получателя CoP для внутренних платежей. Финансовые учреждения, ведущие счета клиентов, могут присоединиться к системе CoP либо разработав собственное техническое решение, либо воспользовавшись услугами специализированного поставщика.

С момента запуска механизма в 2020 году к системе CoP присоединилось более 300 организаций, а ежедневно выполняется свыше 2 миллионов проверок. В 2024 году Регулятор платежных систем Великобритании обязал участников рынка расширить применение механизмов CoP.

Гонконг, Китай

Для снижения риска ошибочного направления платежей в Системе быстрых платежей (FPS) плательщик может до подтверждения платежного поручения проверить имя получателя в сервисе адресации.

Если плательщик инициирует платеж или перевод, указывая прокси-идентификатор либо номер счета получателя, система FPS предоставляет для подтверждения частично скрытое имя получателя. Это позволяет существенно снизить риск мошенничества и ошибок при вводе реквизитов. Использование частично скрытого имени получателя также способствует защите конфиденциальности получателя.

Индия

Резервный банк Индии внедрил функцию проверки имени получателя в Системе валовых расчетов в режиме реального времени (Real Time Gross Settlement, RTGS) и Системе национальных электронных переводов (National Electronic Funds Transfer, NEFT). Аналогичная функция также используется в Едином платежном интерфейсе (Unified Payments Interface, UPI) и Системе мгновенных платежей (Immediate Payment Service, IMPS). Указанные системы позволяют плательщику до инициирования перевода проверить имя получателя.⁷¹

Сингапур

⁷¹ [Внедрение функции проверки имени получателя в Системе валовых расчетов в режиме реального времени \(RTGS\) и Национальной системе электронных переводов \(NEFT\)](#)

Nexus - инициатива⁷², по объединению систем мгновенных платежей нескольких юрисдикций - включает механизм трансграничной проверки CoP/VoP, позволяющий до исполнения платежа убедиться, что средства будут переведены получателю, которому они предназначены. При инициировании трансграничного платежа плательщик может указать прокси-идентификатор (например, номер мобильного телефона), используемый в стране получателя. Финансовое учреждение плательщика направляет через систему Nexus запрос на сопоставление прокси-идентификатора, который обрабатывается каталогом прокси-идентификаторов страны получателя.

Если прокси-идентификатор связан со счетом, каталог возвращает сведения о счете и имя получателя. После этого плательщику предлагается подтвердить, что указанное имя соответствует получателю, которому предназначен перевод. Только после этого платеж может быть исполнен. В зависимости от требований законодательства о защите данных имя получателя может отображаться полностью либо в частично скрытом виде.

303. С технической точки зрения механизмы CoP/VoP, как правило, используют автоматизированные интерфейсы (например, API) и структурированные платежные данные (например, в формате ISO 20022). При создании таких механизмов юрисдикциям также следует определить:

- единый технический стандарт сопоставления имени получателя и идентификатора счета;
- четкие правила участия финансовых учреждений, направляющих запросы и предоставляющих ответы;
- требования к срокам обработки и направления ответов;
- порядок обработки ошибок и повторного направления запросов;
- надежную правовую основу для обмена данными.

304. Действующие механизмы, такие как сервис CoP компании Pay.UK и система VoP Европейского союза, показывают важность наличия единых правил функционирования, минимальных требований к производительности, возможности проведения аудита и надлежащего надзора. При разработке механизмов CoP/VoP страны должны выработать сопоставимые стандарты, чтобы независимо от поставщика услуг механизмы предварительной проверки работали по единым правилам, были совместимы между собой и обеспечивали надежную проверку.

305. Механизм CoP/VoP, как правило, предусматривает автоматизированный обмен информацией между финансовыми учреждениями:

⁷² [Проект Nexus](#) был инициирован Инновационным центром Банка международных расчетов (BIS Innovation Hub, BISIH) с целью стандартизации взаимодействия между системами мгновенных платежей. В настоящее время центральные банки Индии, Индонезии, Филиппин, Таиланда и Сингапура объединили усилия для создания системы [Nexus Global Payments](#) и ее полномасштабного внедрения.

- (1) финансовое учреждение плательщика направляет финансовому учреждению получателя запрос на проверку;
- (2) финансовое учреждение получателя направляет ответ с результатом проверки (например, «совпадение», «частичное совпадение» или «несовпадение»); и
- (3) результат проверки доводится до сведения плательщика до подтверждения платежа. Если результатом проверки является «частичное совпадение» или «несовпадение», решение о проведении платежа принимает плательщик с учетом полученной информации и иных факторов риска. Объем информации, раскрываемой плательщику (например, полный или частично скрытый вариант имени владельца счета наряду с результатом проверки), определяется механизмами защиты данных.



www.epc-sep.eu

Вставка 21. Пример применения механизмов CoP/VoP

Европейский Союз

Европейский платежный совет разработал Свод правил для механизма VoP. Он устанавливает единые правила, стандарты и операционные процедуры, обеспечивающие совместимость между тысячами поставщиков платежных услуг в Европе, предоставляющих своим клиентам услуги VoP. Свод правил определяет:

- роли основных участников процесса;
- порядок предоставления услуги;
- сроки направления ответа и возможные результаты проверки;
- момент, к которому результат проверки должен быть доведен до сведения плательщика (например, до исполнения платежа).

Для взаимодействия участников механизма каждый из них должен располагать информацией, необходимой для связи с другими участниками (в частности, знать сетевой адрес другого участника) и обмена данными. С этой целью Европейский

платежный совет создал Сервис каталогов Европейского платежного совета (EPS Directory Service, EDS), который позволяет участникам взаимодействовать между собой.

10.5.5 Совместное применение различных подходов

306. Для выполнения требований к проверке соответствия данных финансовые учреждения получателя могут использовать одновременно несколько подходов, включая последующую проверку, комплексный непрерывный мониторинг и механизмы предварительной проверки. Их совместное применение позволяет более эффективно выявлять и устранять существенные несоответствия в информации о получателе.

307. На практике финансовые учреждения получателя могут использовать различные подходы, в том числе:

- использовать механизмы предварительной проверки, если они доступны, особенно в системах мгновенных или почти мгновенных платежей;
- применять комплексный непрерывный мониторинг в качестве основного механизма контроля для выявления аномальных операций, включая повторяющиеся или систематические несоответствия данных;
- использовать последующую проверку в качестве резервного или дополнительного механизма контроля, если механизмы предварительной проверки недоступны или не применяются, а также в случаях, когда комплексный непрерывный мониторинг выявил обстоятельства, требующие дополнительной проверки (например, в качестве последующей меры).

308. При совместном применении различных подходов финансовые учреждения получателя должны определить, какой подход и в каких случаях применяется, а также кто отвечает за выполнение соответствующих действий. Независимо от выбранного подхода все существенные несоответствия в информации о получателе должны выявляться и обрабатываться единообразно. Последующие меры должны соответствовать характеру и уровню выявленных рисков. Использование нескольких подходов одновременно не должно снижать общую эффективность проверки по сравнению с применением одного подхода или создавать дополнительные затруднения при проведении правомерных операций. При этом финансовые учреждения должны в полном объеме применять как минимум один из трех подходов, даже если одновременно используют отдельные элементы других.

Вставка 22. – Внедрение механизмов проверки соответствия данных в странах с менее развитой платежной инфраструктурой

Платежные системы и финансовые учреждения существенно различаются по уровню технического и операционного развития. Особенно остро эта проблема проявляется в странах с менее развитой платежной инфраструктурой, где пока недоступны механизмы предварительной проверки или отсутствуют достаточные объемы данных для комплексного непрерывного мониторинга.

Обновленная Рекомендация 16 учитывает эти особенности и предусматривает гибкий подход к выполнению финансовыми учреждениями получателя требований к проверке соответствия данных. В таких случаях государствам рекомендуется отказаться от универсального подхода и установить четкие, выполнимые и соразмерные требования к внедрению механизмов такой проверки. Например, допускать совместное применение различных подходов.

На практике это может включать:

- использование последующей проверки в качестве минимального механизма контроля при осуществлении трансграничных платежей или переводов, превышающих порог *de minimis*, если применение механизмов предварительной проверки или мониторинга в режиме реального времени технически невозможно;
- поэтапное внедрение более совершенных механизмов контроля, таких как расширенный мониторинг или механизмы предварительной проверки, по мере развития платежных систем и повышения качества данных;
- применение более оперативных или автоматизированных механизмов проверки соответствия данных в отношении тех направлений трансграничных переводов, видов операций и категорий клиентов, которые характеризуются повышенным уровнем риска, в соответствии с риск-ориентированным подходом;
- при совместном применении различных подходов - четкое распределение функций и обязанностей, исключающее случаи, когда существенные несоответствия данных остаются невыявленными или рассматриваются непоследовательно.

Стандарт ISO 20022 пока применяется не во всех юрисдикциях и не для всех способов осуществления платежей. В результате возможности использования более полных и структурированных данных при проверке соответствия данных остаются ограниченными. Для решения этой проблемы компетентным органам рекомендуется учитывать международные документы, посвященные развитию единых требований к данным при осуществлении трансграничных платежей и повышению совместимости платежных систем. В частности, речь идет о документе СРМІ «Гармонизированные требования к данным ISO 20022 для совершенствования трансграничных платежей» (Harmonised ISO 20022 Data Requirements for Enhancing Cross-border Payments). В нем подчеркивается важность единообразного использования уникальных идентификаторов счетов, четкой идентификации всех участников цепочки платежа и стандартизированного представления сведений о них.

С учетом этих ограничений компетентным органам рекомендуется подготовить практические разъяснения по вопросам выполнения финансовыми учреждениями получателя требований к проверке соответствия данных в условиях существующих

ограничений платежной инфраструктуры. Такие разъяснения должны охватывать все механизмы проверки соответствия данных, предусмотренные Рекомендацией 16, если их применение целесообразно. При этом они должны учитывать уровень риска и не создавать необоснованных препятствий для проведения правомерных операций.

10.6 Действия при выявлении несоответствий

309. Если финансовое учреждение получателя выявило существенное несоответствие информации о получателе, которое может привести к ошибочному зачислению средств, оно должно руководствоваться эффективными политиками и процедурами, основанными на риск-ориентированном подходе, при выборе дальнейших действий. В зависимости от обстоятельств перевод может быть исполнен, приостановлен, отозван или отклонен. При необходимости должны приниматься и иные корректирующие меры⁷³. Все принятые решения подлежат документированию. Финансовое учреждение получателя должно четко прописать во внутренних политиках порядок действий при выявлении существенных несоответствий информации о получателе, включая основания для применения каждой из возможных мер. Такие политики должны соответствовать требованиям законодательства и нормативных актов. Принятые меры должны фиксироваться. Во внутренних политиках финансовых учреждений-получателей необходимо закрепить перечень доступных мер и определить, в каких случаях применяется каждая из них, с учетом законодательства и нормативных требований.

310. В зависимости от уровня риска и обстоятельств финансовое учреждение получателя вправе:

- заморозить средства на период проверки выявленного несоответствия;
- при необходимости запросить разъяснения у клиента; или
- передать информацию для внутреннего рассмотрения (например, сотруднику, ответственному за соблюдение требований в сфере ПОД/ФТ, либо в подразделение, осуществляющее функции комплаенса или противодействия мошенничеству).

311. При выявлении признаков ОД/ФТ (в том числе мошенничества) финансовое учреждение получателя должно действовать в соответствии со своими внутренними процедурами. Если существенные несоответствия неоднократно выявляются при переводах, поступающих от одного и того же финансового учреждения плательщика либо в рамках одних и тех же трансграничных операций, это может свидетельствовать о системных недостатках. В таких случаях финансовому учреждению получателя следует рассмотреть вопрос о принятии дополнительных мер защиты, а также при необходимости организовать взаимодействие с соответствующими участниками. Если

⁷³ Включая мониторинг счета получателя на предмет выявления признаков мошенничества или использования счета в качестве счета дроппера.

это допускается законодательством и нормативными актами, финансовое учреждение получателя должно своевременно и в понятной форме информировать клиентов о приостановлении исполнения перевода или его отзыве.

312. Выявленное при предварительной проверке входящего платежа (например, с использованием CoP/VoP) несоответствие само по себе не свидетельствует о мошенничестве. Если плательщик был уведомлен о результатах проверки и подтвердил проведение платежа, финансовое учреждение получателя не должно приостанавливать исполнение или возвращать перевод только на основании такого несоответствия.

313. Выявление существенного несоответствия информации о получателе не должно быть единственным фактором, учитываемым финансовым учреждением получателя при принятии решения. Следует также учитывать особенности поведения клиента, историю операций по счету, характеристики операции и обстоятельства совершения платежа. Если с учетом всех обстоятельств возникают подозрения в ОД/ФТ/ФРОМУ, финансовому учреждению получателя следует направить сообщение о подозрительной операции в соответствии с требованиями национального законодательства. Если финансовое учреждение получателя неоднократно выявляет существенные несоответствия при переводах, поступающих от одного и того же финансового учреждения плательщика либо в рамках одних и тех же трансграничных операций, ему рекомендуется сообщить об этом компетентным органам. Такие случаи могут свидетельствовать о систематически ошибочном направлении платежей и требуют дополнительной проверки.

Приложение: Схемы платежных цепочек

1. В настоящем приложении приведены примеры наиболее распространенных платежных цепочек, встречающихся в практике. На их основе показано, в каких случаях платеж или перевод рассматривается как единая платежная цепочка, а в каких - как несколько отдельных платежных цепочек. Основное внимание уделено определению начальной и конечной точек. Схемы содержат только сведения, необходимые для иллюстрации рассматриваемых подходов. Они не являются исчерпывающими и не отражают все сопутствующие платежи и расчеты, которые могут осуществляться при оказании услуг по проведению платежей или переводов.

Принцип. «Платеж или перевод ценностей» рассматривается как единое целое.

Принцип. Новое распоряжение означает начало новой платежной цепочки.

Принцип. Распоряжение может быть передано финансовому учреждению непосредственно плательщиком либо через третье лицо.

Принцип. Способ исполнения платежа или перевода не влияет на существование платежной цепочки.

Принцип: «Платеж или перевод ценностей» рассматривается как единое целое.

Термин «платеж или перевод ценностей» охватывает любую операцию, при которой плательщик через финансовое учреждение с использованием электронных средств переводит денежные средства получателю, обслуживаемому другим финансовым учреждением. Хотя в исполнении такого платежа или перевода могут участвовать различные финансовые учреждения (например, банки, УПДЦ или ПУВА), все совершаемые операции образуют единую платежную цепочку.

Ниже приведен пример трансграничного Р2Р-перевода денежных средств между физическими лицами, который осуществляется через финансовые учреждения-посредники с последующей выплатой средств получателю через местный банк.

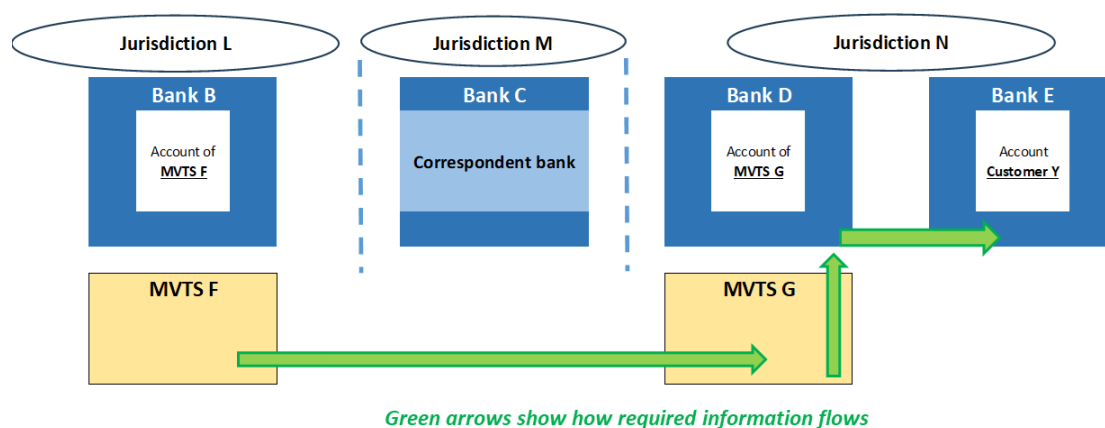
На практике небанковские финансовые учреждения все чаще самостоятельно исполняют распоряжения плательщиков. Вместе с тем участие в исполнении перевода банков, УПДЦ или инфраструктуры внутреннего платежного рынка (например, при зачислении средств на счет получателя) не означает, что возникает новая платежная цепочка. Независимо от того, сколько участников задействовано в переводе и каким образом он исполняется, информация о плательщике и получателе должна передаваться непрерывно от начала до конца платежной цепочки.

Распоряжение о платеже или переводе:

- Клиент X (плательщик) поручает УПДЦ F (финансовому учреждению плательщика) в юрисдикции L перевести денежные средства Клиенту Y (получателю) путем их зачисления на его счет, открытый в Банке E (финансовом учреждении получателя) в юрисдикции N.

Начальная и конечная точки платежной цепочки. Обязанности участников:

- Начальной точкой платежной цепочки является УПДЦ F. Именно это финансовое учреждение получает от Клиента X (плательщика) распоряжение о проведении трансграничного платежа или перевода и выступает финансовым учреждением плательщика.
- Конечной точкой платежной цепочки является Банк E. В нем открыт счет Клиента Y (получателя). Банк E выступает финансовым учреждением получателя.
- Информация о плательщике и получателе, предусмотренная Рекомендацией 16, должна передаваться по всей платежной цепочке: УПДЦ F → УПДЦ G → Банк D → Банк E. УПДЦ G, выступающий финансовым учреждением-посредником, информирует Банк D о том, что перевод является трансграничным платежом или переводом.
- УПДЦ F включает в платежное сообщение всю необходимую информацию. УПДЦ G и Банк D, выступающие финансовыми учреждениями-посредниками, сохраняют эту информацию при ее передаче по платежной цепочке. Даже если УПДЦ F и УПДЦ G входят в одну группу УПДЦ, вся необходимая информация должна передаваться в полном объеме. УПДЦ F передает полный комплект необходимых сведений УПДЦ G, который направляет их Банку D. Банк D, в свою очередь, передает эти сведения Банку E.



Принцип. Новое распоряжение означает начало новой платежной цепочки.

В рамках исполнения одного распоряжения может возникнуть несколько самостоятельных платежных цепочек. Получение финансовым учреждением плательщика нового распоряжения означает начало новой платежной цепочки. Это свидетельствует о том, что предыдущее распоряжение уже исполнено, а для проведения следующего платежа или перевода требуется новое распоряжение.

Ниже приведен пример, в котором плательщик дает распоряжение предоставить денежные средства получателю одним из следующих способов: (1) путем их зачисления на счет или цифровой кошелек получателя, открытый в УПДЦ (в том числе с использованием механизмов, отличных от традиционных банковских счетов), либо (2) путем выплаты получателю наличных денежных средств через УПДЦ.

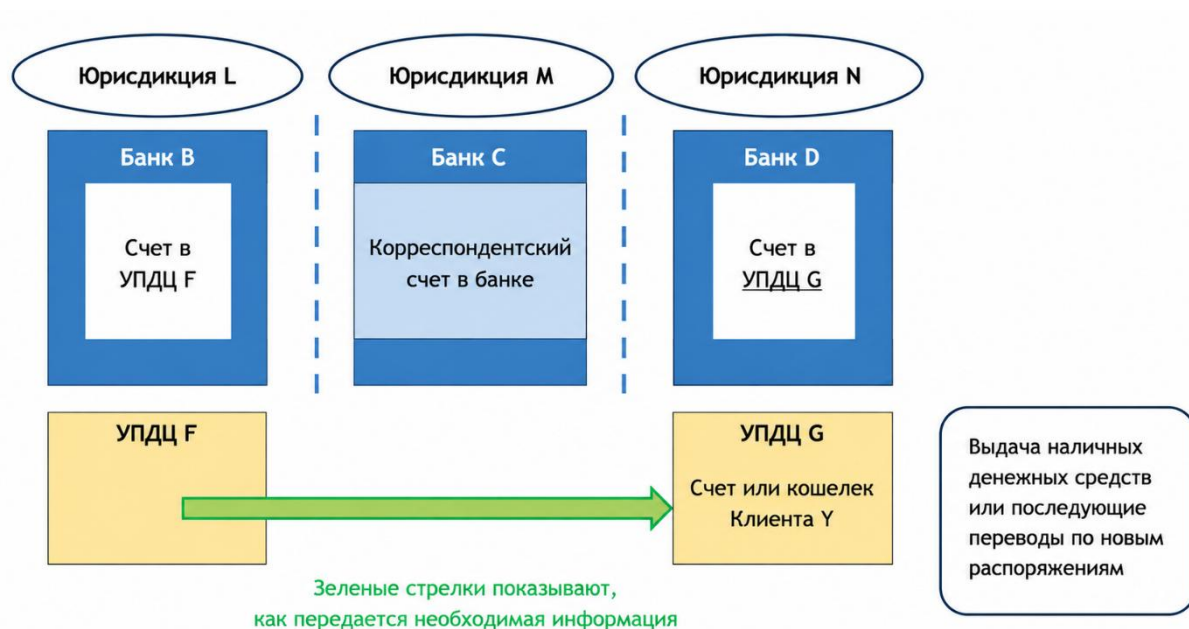
Распоряжение о платеже или переводе

- Клиент X (плательщик) поручает УПДЦ F (финансовому учреждению плательщика), расположенному в юрисдикции L, перевести денежные средства Клиенту Y (получателю), обслуживаемому УПДЦ G (финансовым учреждением получателя) в юрисдикции N.
- В отличие от предыдущего примера распоряжение Клиента X не предусматривает дальнейший перевод денежных средств в другое финансовое учреждение, например банк.
- После зачисления денежных средств Клиент Y может дать УПДЦ G новое распоряжение - о выдаче наличных денежных средств либо о переводе средств на банковский счет в юрисдикции N. В этом случае возникает новая самостоятельная платежная цепочка.

Начальная и конечная точки платежной цепочки. Обязанности участников

- Начальной точкой платежной цепочки является УПДЦ F. УПДЦ F получает распоряжение плательщика и выступает финансовым учреждением плательщика. Конечной точкой платежной цепочки является УПДЦ G, который выступает финансовым учреждением получателя.
- УПДЦ F собирает информацию о плательщике и получателе, предусмотренную Рекомендацией 16, проверяет информацию о плательщике и передает всю необходимую информацию УПДЦ G вместе с переводом. Даже если УПДЦ F и УПДЦ G входят в одну группу УПДЦ, вся необходимая информация должна передаваться в полном объеме.

- После зачисления денежных средств на счет или цифровой кошелек, открытый в УПДЦ G, Клиент Y может дать распоряжение о выдаче наличных денежных средств или переводе средств на другой счет. Такое распоряжение означает начало новой самостоятельной платежной цепочки.



Принцип. Распоряжение может быть передано финансовому учреждению непосредственно плательщиком либо через третье лицо.

Когда третье лицо, в частности финансовое учреждение получателя, передает финансовому учреждению плательщика распоряжение плательщика, такой механизм иногда называют «платежом по запросу получателя». Передача распоряжения через третье лицо не меняет его природы: оно по-прежнему считается распоряжением плательщика, адресованным финансовому учреждению плательщика. Без соответствующего распоряжения или согласия плательщика получатель не вправе самостоятельно инициировать платеж или перевод ценностей через финансовое учреждение плательщика.

К таким случаям относятся:

- Платежи по прямому дебетованию (direct debit), при которых плательщик предоставляет финансовому учреждению получателя право направить в финансовое учреждение плательщика запрос на списание денежных средств. Независимо от того, что такое распоряжение передается через финансовое учреждение получателя, оно считается распоряжением плательщика, адресованным финансовому учреждению плательщика. При этом договорные механизмы, на основании которых осуществляются операции прямого дебетования, могут различаться;
- Операции с использованием кредитных, дебетовых и предоплаченных платежных карт, при которых распоряжение плательщика формируется через платежный терминал торгового-сервисного предприятия. Финансовое учреждение получателя (эквайер) передает его финансовому учреждению плательщика (эмитенту), которое принимает решение об исполнении платежа или перевода. Следует учитывать, что в соответствии с Рекомендацией 16 при оплате товаров и услуг вместе с переводом должен передаваться только номер платежной карты, который также получает эквайер.

Для целей Рекомендации 16 платежная цепочка начинается с финансового учреждения, которое получает распоряжение плательщика и приступает к его исполнению, то есть с финансового учреждения плательщика. При этом не имеет значения, какое финансовое учреждение передало это распоряжение (например, в рамках ранее выданного согласия на регулярное списание денежных средств или в соответствии с правилами платежной системы).

Принцип. Способ исполнения платежа или перевода не влияет на существование платежной цепочки.

При исполнении платежа или перевода могут использоваться различные платежные инструменты и технологии, в том числе предусматривающие конвертацию средств из одной формы в другую. Это не означает начала новой платежной цепочки.

К таким случаям относятся:

- Финансовые учреждения-посредники могут конвертировать средства из одной валюты в другую (например, в рамках корреспондентских отношений)
- УПДЦ может использовать виртуальные активы при осуществлении трансграничного перевода с последующей выплатой получателю средств в фиатной валюте. Это следует отличать от использования виртуальных активов для расчетов между УПДЦ.