

FATF



РУКОВОДСТВО ПО ПРИМЕНЕНИЮ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА

ПРЕДОПЛАЧЕННЫЕ КАРТЫ,
МОБИЛЬНЫЕ ПЛАТЕЖИ И
ОНЛАЙН ПЛАТЕЖИ

Июнь 2013



ГРУППА РАЗРАБОТКИ ФИНАНСОВЫХ МЕР ПО БОРЬБЕ С
ОТМЫВАНИЕМ ДЕНЕГ (ФАТФ)

Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) – это независимая межправительственная организация, разрабатывающая и популяризирующая свои принципы для защиты всемирной финансовой системы от угроз отмывания денег, финансирования терроризма и финансирования распространения оружия массового уничтожения. Рекомендации ФАТФ являются общепризнанными международными стандартами по противодействию отмыванию денег (ПОД) и финансированию терроризма (ПФТ).

Подробная информация о ФАТФ размещена на сайте:

www.fatf-gafi.org

© FATF/OECD. All rights reserved, 2013

© ФАТФ/ОЭСР. Все права защищены, 2013

© АНО «МУМЦФМ». Все права защищены, 2013

Перевод подготовлен Международным учебно-методическим центром по
финансовому мониторингу

Копирование и перевод настоящего отчета осуществляются только по предварительному письменному разрешению ФАТФ. Заявки на получение разрешения для всего документа или его отдельных частей направляются в Секретариат ФАТФ: 75775 Париж, ул. Андре Паскаля (факс: +33 1 44 30 61 37, e-mail: contact@fatf-gafi.org).

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	4
I. ВВЕДЕНИЕ	5
А. Сфера применения и потенциальные пользователи	5
В. Задачи Руководства	6
II. РОЛЬ ОРАГАНИЗАЦИЙ, ПРЕДОСТАВЛЯЮЩИХ НПМУ	7
А. Предоплаченные карты	7
В. Мобильные платежи	8
С. Платежи через Интернет	11
III. ОРГАНИЗАЦИИ, ПОДПАДАЮЩИЕ ПОД РЕКОМЕНДАЦИИ ФАТФ	12
А. Определение «финансового учреждения», используемого ФАТФ	13
В. Исключения при применении мер по ПОД/ФТ, на основании риск-ориентированного подхода	14
IV. ОЦЕНКА РИСКОВ И УПРАВЛЕНИЕ РИСКАМИ В СФЕРЕ НПМУ	14
А. Факторы риска	15
В. Меры по снижению рисков	21
V. ВЛИЯНИЕ РЕГУЛИРОВАНИЯ НА РЫНОК НПМУ	26
А. Руководство ФАТФ по доступности финансовых услуг	26
В. Принципы «двадцатки» по доступности инновационных финансовых услуг	26
VI. РЕГУЛИРОВАНИЕ, НАДЗОР И РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД	27
А. Риск-ориентированный подход, меры по ПОД/ФТ и надзор	27
В. Надлежащая проверка клиентов	28

С. Лицензирование/регистрация	30
Д. Электронные денежные переводы	31
Е. Подход надзорных органов и определение компетенции	32
VII. НАДЛЕЖАЩЕЕ РЕГУЛИРОВАНИЕ В СФЕРЕ ПОД/ФТ, КОТОРОЕ ПОЗВОЛЯЕТ СНИЖАТЬ РИСКИ	33
А. Уровень мер по ПОД/ФТ, который бы соответствовал уровню риска	33
В. Факторы, которые необходимо учитывать, при применении мер по ПОД/ФТ в отношении провайдеров НПМУ	34
ПРИЛОЖЕНИЕ 1 – ПОДХОДЫ РЕГУЛЯТОРОВ К НПМУ	38
СПИСОК ЛИТЕРАТУРЫ	45

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

G2P	<i>Government to person</i> - Переводы от правительства физическому лицу
IP	Интернет-протокол
P2B	<i>Person to business</i> - Переводы от физического лица в адрес юридического лица
P2P	<i>Person to person</i> - Переводы от одного физического лица в адрес другого физического лица
ББС	Ближняя бесконтактная связь
ЗСК	Знай своего клиента
НДСД	Неструктурированные дополнительные сервисные данные
НПК	Надлежащая проверка клиента
НПМ	Новые платежные методы
НМПУ	Новые платежные методы и услуги
ОД	Отмывание денег
ОСС	Оператор сотовой связи
ПОД/ФТ	Противодействие отмыванию денег и финансированию терроризма
СИМ	Модуль идентификации абонента
УПДЦ	Услуги перевода денег или ценностей
ФТ	Финансирование терроризма

РУКОВОДСТВО ПО ПРИМЕНЕНИЮ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА ДЛЯ ПРЕДОПЛАЧЕННЫХ КАРТ И ОНЛАЙН ПЛАТЕЖЕЙ

I. ВВЕДЕНИЕ

1. Быстрое развитие, высокая функциональность и значительный рост использования новых платежных методов и услуг (НПМУ) по всему миру создает определенные трудности для стран и организаций частного сектора в обеспечении того, чтобы эти продукты и услуги не использовались для отмывания денег (ОД) и финансирования терроризма (ФТ). Это привлекло внимание органов, которые занимаются вопросами противодействия отмыванию денег и финансированию терроризма, так как они стараются разработать руководства для развития и применения мер по ПОД/ФТ для НПМУ. Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) подготовила отчеты по типологиям¹ в 2006 г., в 2008 г. и в 2010 г. относительно новых платежных методов (НПМ), в которых особое внимание уделялось тому, как НПМ могут быть использованы преступниками, выявлению факторов риска, которые могут варьироваться от одного нового платежного продукта или услуги к другому, в зависимости от функциональности, а также факторы снижения риска, применяемые к конкретному платежному продукту или услуге, чтобы снизить их специфический профиль риска. ФАТФ признает инновационное использование появляющихся технологий в данной сфере, включая децентрализованные цифровые валюты. Обсуждения в рамках ФАТФ отражают эти проблемы и будут рассматривать риски и меры, необходимые для снижения рисков в ПОД/ФТ.

A. СФЕРА ПРИМЕНЕНИЯ И ПОТЕНЦИАЛЬНЫЕ ПОЛЬЗОВАТЕЛИ

2. Этот документ является руководством о применении риск-ориентированного подхода для мер по ПОД/ФТ и о регулировании ряда аспектов, связанных с НПМУ, а именно prepaid карт, мобильных платежей и онлайн платежей в соответствии с *Рекомендациями ФАТФ*. Руководство не носит обязательного характера и не отменяет компетенцию национальных властей. Цель – это, основываясь на типологических исследованиях ФАТФ и используя существующие руководства ФАТФ о разработке и реализации риск-ориентированного подхода для ПОД/ФТ, включая, в частности, *Руководство ФАТФ по оценке рисков ОД/ФТ*² указать на то, что НПМУ играют важную роль при обеспечении доступности финансовых услуг. Настоящее руководство соответствует положениям *Руководства ФАТФ «О борьбе с отмыванием денег и финансированием терроризма и обеспечением доступности финансовых услуг»*, которое должно помочь странам и финансовым учреждениям разработать такие меры по ПОД/ФТ, которые отвечали бы национальным задачам обеспечения доступности финансовых услуг, не нанося ущерба существующим мерам по борьбе с преступностью³. В этом отношении, ФАТФ признает, что применение сверхосторожного подхода для обеспечения мер по ПОД/ФТ может привести к нежелательным последствиям, например, вытеснению законной деятельности и потребителей из финансовой системы, заставляя их, таким образом, пользоваться услугами, регулирование и надзор за которыми не осуществляется. Контроль в сфере ПОД/ФТ не должен препятствовать доступу к официальным финансовым операциям для лиц, которые не имеют доступа к финансовым или банковским услугам. ФАТФ признает, что отсутствие доступа к финансовым услугам может снизить эффективность режима ПОД/ФТ, расширение доступа к финансовым услугам и эффективное функционирование системы ПОД/ФТ необходимо рассматривать как задачи, служащие одной цели.

3. В контексте данного Руководства считается, что НПМУ – это новые и инновационные платежные продукты и сервисы, являющиеся альтернативными по отношению к традиционным

¹ См. ФАТФ(2006), ФАТФ (2008) и ФАТФ(2010)

² См. ФАТФ (2013а). Этот документ содержит основные принципы, которые могут служить основой для оценки рисков ОД/ФТ на национальном уровне. Однако, эти принципы могут быть использованы при проведении целевой оценки. Руководство не содержит описание того, как надзорные органы должны оценивать риски с учетом риск-ориентированного надзора.

³ См. ФАТФ (2013b)

финансовым услугам. НПМУ включают в себя широкий спектр продуктов и услуг, которые помогают осуществить платежи через традиционные розничные системы электронных платежей, а также продукты, не зависящие от традиционных система перевода денежных средств и ценностей между юридическими и физическими лицами. Учитывая быстрое развитие и изменение природы таких продуктов и услуг, любая попытка дать какое-либо точное определение того, что такое НПМУ скорее всего приведет к ограничению применения настоящего Руководства. В этой связи необходимо признать, что не смотря на то, что данное Руководство описывает существующие НПМУ, но оно также может применяться и к новым и зарождающимся НПМУ, которые не рассматриваются в данном Руководстве. Для того чтобы обеспечить применимость и практичность данного Руководства, оно детально сконцентрировано на трех категориях НПМУ (1) предоплаченные карты, (2) мобильные платежи и (3) платежи через Интернет. Важно отметить, что все категории НПМУ взаимосвязаны, больше всего между собой и с традиционными платежными методами.

4. Традиционные финансовые услуги, такие как банковские услуги, все чаще оказываются за счет использования новых и инновационных методов, включая использование Интернета и технологий, связанных с мобильными телефонами. При этом если страны и финансовые учреждения должны выявлять и оценивать риски ОД/ФТ могут возникать в отношении новых методов донесения традиционных финансовых услуг⁴, то они не подпадают под сферу действия данного Руководства. Основное внимание настоящего Руководства уделяется инновационным платежным методам и мерам по снижению риска ОД/ФТ, которые они несут.

5. Руководство изначально предназначено для органов власти, регулирующих деятельность, связанную с НПМУ (надзорные органы и органы, вырабатывающую политику в установленной сфере), а также для организаций частного сектора, которые задействованы в разработке, развитии и продвижении НПМУ. Это включает в себя финансовые учреждения, выпускающие и управляющие НПМУ, которые уже реализуют меры по НПМУ, а также предпринимают иные шаги для снижения риска отмывания денег и финансирования терроризма.

В. ЗАДАЧИ РУКОВОДСТВА

6. Цель Руководства это:

(a) разъяснить как функционируют новые платежные системы, какие организации занимаются НПМУ, их роль и деятельность (Раздел II);

(b) понять, какие учреждения, участвующие в реализации НРР, уже охвачены *Рекомендациями ФАТФ* (то есть в силу того, что они уже подпадают под определение ФАТФ «*финансовое учреждение*») (Раздел III);

(c) установить риски, возникающие при распространении НПМУ, в том числе путем рассмотрения любых соответствующих факторов риска и мер по снижению рисков (Раздел IV);

(d) проанализировать влияние регулирования на рынок НПМУ, включая то, как такое регулирование повлияет на доступность финансовых услуг, а также на перемещение денежных вкладов в регулируемые финансовые учреждения (Раздел V);

(e) понять как регулировать и осуществлять надзор за учреждениями, занимающимися НПМУ, а также как такое регулирование или надзор способствуют реализации мер по ПОД/ФТ (Раздел VI);
и

⁴ См. Рекомендацию 15

(f) обсудить факторы (которые необходимо учитывать при регулировании ПОД/ФТ и НПМУ), снижающие риски, признавая, что существуют большое количество регулируемых учреждений, основываясь на результатах, описанных в Разделах III, IV, V и VI (Раздел VII).

II. РОЛЬ УЧРЕЖДЕНИЙ, ПРЕДОСТАВЛЯЮЩИХ НПМУ

7. Данный раздел описывает то, как функционируют новые платежные системы, какие организации занимаются НПМУ, их роль и деятельность. Структура, характеристики и модели НПМУ отличаются друг от друга значительно, многие из них служат для разрешения рисков ОД/ФТ.

A. ПРЕДОПЛАЧЕННЫЕ КАРТЫ

8. Предоплаченные карты появились на рынке платежей в конце 1990-х как альтернатива кредитным картам (в отношении которых существовало требование о том, что эмитент карт оценивал минимальную платежеспособность держателя карты) и дебетовым картам (что приводило к необходимости открывать расчетный счет в банке или финансовом учреждении). Предоплаченные карты изначально считались инструментом оплаты услуг и товаров, который не требовал от эмитента анализа платежеспособности держателя или затрат на открытие и ведение расчетного счета. Многие предоплаченные карты используются в настоящее время для получения наличных из банкомата во всем мире. Кроме того, многие из них сейчас предусматривают возможность перевода от лица к лицу.

9. Динамичный и быстро развивающийся характер рынка предоплаченных карт создает определенные трудности регулирования в сфере ПОД/ФТ в части обеспечения его своевременности. В настоящее время функционал предоплаченных карт очень сильно изменился: они прошли путь от подарочных сертификатов и инструментов с ограниченным применением/и применением в рамках одной/замкнутой системы до инструмента, наделенного всеми функциями платежного инструмента, привязанного к банковскому счету. На одном конце спектра находятся подарочные карты, которые могут быть использованы для оплаты покупок в одном или ограниченной сети магазинов (их обычно называют предоплаченные карты одноэмитентной (закрытой) системы). Такие карты не дают доступа к банкоматам во всем мире и не предусматривают возврат наличных через торговые сети (известное как «cash back»). Учитывая их низко рисковые характеристики, эта категория предоплаченных карт, особенно если они не предусматривают возможность внесения или снятия денежных средств, не подпадает под настоящее Руководство и на них не распространяются меры по ПОД/ФТ, описанные ниже⁵. На другом конце спектра платежные карты фирменных сетей, которые позволяют совершать операции с любой торговой точкой или поставщиком услуг, входящих в сеть (предоплаченные карты многоэмитентной (открытой) системы). Большинство предоплаченных карт данной категории открывают клиентам доступ к средствам, хранящимся на привязанном расчетном счете. Не смотря на то, что средства «можно хранить» на чипе предоплаченной карты, количество предоплаченных карт с чипами снижается. Некоторые предоплаченные карты можно пополнять, используя наличные и иные электронные платежные инструменты; некоторые из них дают возможности, что и расчетный счет и связанные с ним инструменты, например, перевод средств, использование банкоматов по всему миру, а в некоторых случаях переводы от лица лицу. Между этими двумя крайностями располагается целая линейка продуктов, некоторые из которых наделены чертами счета, но которые также содержат и ограничения (например, лимиты по пополнению или по расходованию средств), что значительно снижает риски.

10. Многие учреждения могут выпускать предоплаченные карты. Роль этих учреждений может меняться в зависимости от бизнес-модели продуктов предоплаченных карт. Это учреждение или его агенты могут выполнять различный функционал. Это создает определенные трудности в

⁵ ФАТФ не думает, что для предоплаченных карт одноэмитентной (закрытой) системы существует низкие риски ОД/ФТ, однако их уровень снижен в результате ограниченного применения таких карт

части того, на кого возложить ответственность по контролю ПОД/ФТ. В Разделе VII настоящего Руководства содержится описание для стран, какое из учреждений считать ответственной стороной (сторонами) и, как следствие, кто подпадает под регулирование о ПОД/ФТ с учетом модели. Учреждения, занимающиеся prepaid картами, могут включать следующее:

(a) *Эквайер* – учреждение, у которого есть отношения с ритейлером, предоставляющее инфраструктуру, необходимую для получения карточного платежа (например, доступ к кассовому терминалу или платежным сервисам, поддерживаемым сайт с электронной коммерцией), а также обслуживающее счета, на которые поступают доходы от продаж;

(b) *Дистрибьютор (включая ритейлера)* – учреждение, которое продает, распространяет prepaid карты среди клиентов от имени эмитента. Дистрибьюторы могут также предлагать и ряд других услуг своим клиентам;

(c) *Оператор платежной системы* – учреждение, которое предоставляет техническую платформу для осуществления операции;

(d) *Эмитент* – учреждение, выпускающее prepaid карту, и к которому клиент обращает свое требование о пополнении или снятии наличных;

(e) *Менеджер программы* – учреждение, которое несет ответственность за установление и работу программы для prepaid карт совместно с банком или институтом электронных денег. Менеджер программы обычно продвигает prepaid карту на рынке и устанавливает отношения с банками и дистрибьюторами или клиентами, а также во многих случаях предоставляют возможность для обработки данных. Некоторые эмитенты prepaid карт сами управляют своими программами, то есть без менеджеров программы;

(f) *Агент* – для целей настоящего Руководства, это физическое или юридическое лицо, оказывающее услуги, связанные с prepaid картами от имени другого учреждения, предоставляющего prepaid карты в соответствии с контрактом или по указанию последнего. Учреждения на рынке prepaid карт очень часто выступают от имени других учреждений, в зависимости от выбранной модели для программы prepaid карт.

В. МОБИЛЬНЫЕ ПЛАТЕЖИ

11. Мобильные платежи и то, что они представляют сегодня, являются результатом эволюционного процесса, который начался вместе с распространением мобильных телефонов в конце 1990-х. Первая стадия этого эволюционного процесса связана с неотъемлемой возможностью передавать данные – свойством, характерным для всех мобильных телефонов, которое привлекло внимание банков, побуждая их запустить программу запросов, например, запрос баланса. Затем перечень услуг расширился вплоть до перевода денежных средств. Этот комплекс услуг начали называть «мобильным банкинг». Этот этап характеризуется тем, что банки стали основными поставщиками мобильных платежных услуг. Как было отмечено выше, «мобильный банкинг» и иные традиционные финансовые услуги, оказываемые через инновационные каналы не являются предметом настоящего Руководства. Такие мобильные банковские услуги отличаются от банковских централизованных мобильных платежных моделей, которые предоставляют новые продукты и услуги новым клиентам, как это описано ниже.

12. Второй этап совпадает с дальнейшим распространением мобильной телефонии и использованием электронных денег, что мотивировало различные учреждения проводить с ними различные эксперименты для проведения операций при помощи мобильных телефонов, а также расширения сети ритейлеров, которые работали по prepaid модели. На этом этапе с учетом того, что мобильные денежные продукты связаны зачастую с prepaid счетами, небанковские учреждения также вели очень активную деятельность. На самом деле поставщики

услуг связи преуспели в эмиссии мобильных денег. На этом этапе некоторые юрисдикции столкнулись с этим явлением; часть из них позволила этому явлению существовать без всякого регулирования, другая – начала регулировать, предъявляя специальные требования к лицензированию или регистрации, а третьи - вовсе запретили их деятельность. Однако в странах с зарождающимися рынками объем мобильных денег, включая мобильные платежи, растет, обеспечивая доступность финансовых услуг, предоставляя доступ людям к их широкому спектру.

13. В настоящее время финансовые учреждения, которые осуществляют мобильные платежи, включая от физического лица юридическому лицу (P2B), от физического лица физическому лицу (P2P), от правительства физическому лицу (G2P) могут являться как традиционными поставщиками платежных услуг (банк или кредитное учреждение), так и небанковскими поставщиками платежных сервисов, которые определены в Глоссарии ФАТФ как учреждения, оказывающие услуги по переводу денежных средств и ценностей (НПМУ). В зависимости от бизнес-модели и используемой технологии, многие из провайдеров являются важными партнерами для финансовых учреждений, оказывающих услуги мобильных платежей. Такие партнеры включают в себя операторов сотовой связи (ОСС), а также могут включать производителей мобильных телефонов, представителей групп, разрабатывающих телекоммуникационные стандарты, платежные системы и разработчиков программного обеспечения. Что касается технологий, то в моделях используются разные подходы для проведения мобильных платежей, включая текстовые сообщения, доступ в Интернет при помощи мобильного телефона, ближняя бесконтактная связь (ББС), модуль идентификации абонента (СИМ) и неструктурированные дополнительные сервисные данные (НДСД).

14. Характер и проведение мобильных платежей очень сильно варьируются в зависимости от бизнес-модели и от используемых новых технологий, а также связей с другими НПМУ, что несет трудности в выработке эффективного регулирования в сфере ПОД/ФТ. Бизнес-модели могут меняться в зависимости от того какой поставщик услуг играет главную роль, является ли сервис предоплаченным или оплата производится по факту, когда клиент платит после того, как услуга оказана, и какая техническая платформа используется. Описание видов мобильных платежей, изложенное ниже, не является исчерпывающим и не является описанием конкретной схем. Наоборот, оно обобщает характеристики мобильных платежных сервисов с тем, чтобы помочь выработать меры по ПОД/ФТ и регулирование в данной сфере, а также активно его применять.

15. Клиенты системы мобильных платежей, в которой *центральное место отведено банку*, владеют счётом в банке, предоставляющем услуги платежей. Эта услуга отличается от предоставляемых традиционных банковских услуг с помощью мобильного телефона, так как банк также развивает новые виды услуг с использованием мобильного телефона для того, чтобы поддерживать уже существующие банковские услуги: связанные с ограниченными операциями по счетам, или, наоборот, является поставщиком электронных денег, не привязанных к платёжным счетам. Банк сотрудничает с разработчиками программного обеспечения и операторами по приёму платежей (платёжные системы), что позволяет клиентам банка получать и отправлять платёжные уведомления через оплату доступа к мобильному телефону, а также через внутренние сети автоматизированной клиринговой палаты или сеть платёжных карт. Средства снимаются или вносятся на хранение на банковский счёт клиента, привязанный к платёжной карте. Роль ОСС в данном случае сводится к предоставлению телекоммуникационной сети, которая позволяет передавать платёжные сообщения, и ОСС не управляет и не хранит денежные средства клиента. Следовательно, ОСС не требуется лицензия на оказание финансовых услуг, так как поставщиком платёжных услуг является банк.

16. Если брать модель, где *центральную роль играет ОСС*, то ОСС предлагают платежные услуги в дополнение к своим основным телекоммуникационным услугам. Обычно средства клиента хранятся на предоплаченном счете самим ОСС или его дочерней организацией. Даже если ОСС является собственником бизнеса (учреждение, которое принимает на себя большую часть финансовых рисков и операционную ответственность за оказание услуг), то банк-партнер все равно формально является держателем лицензии. Если средства поступают по факту оказанной услуги, то ОСС могут предоставлять кредиты на короткий срок или платежные услуги своим

клиентам как при реализации трехсторонних схем с платежными карточками⁶. При таком раскладе предоплаченные счета снижают кредитные риски ОСС в том случае, если у клиента с постоплаченным счетом есть и кредитные отношения с ОСС. ОСС часто являются международными компаниями, которые могут оказывать свои услуги и за рубежом. Это также может относиться и к платежным сервисам, если для этого не существует правовых или технических препятствий.

17. Между этими двумя моделями лежит широкий спектр мобильных платежных сервисов, предлагаемых и финансовыми учреждениями, и ОСС, которые становятся партнерами для создания агентской сети с тем, чтобы заполучить новых клиентов из тех географических регионов, не охваченных банковской системой. В таком случае ОСС открывают розничные точки или привлекают ритейлеров, предлагающих аналогичные услуги, характерные для банковских филиалов, но с ограниченным функционалом, привлекая новых клиентов, принимая денежные средства или выплачивая наличные для проведения расчетов по мобильным платежам. Платежные сервисы могут оказываться под именем ОСС или под именем банка.

18. Мобильные платежи тесно связаны с иными платежными сервисами. ОСС вступают в партнерские отношения с электронными платежными системами, чтобы обеспечить клиентам внутри страны доступ к банкоматам для снятия наличных путем введения кода, а не «прокачивая» карту. Чтобы обеспечить своим клиентам международный доступ к наличными денежным средствам ОСС развивают партнерские отношения с эмитентами платежных карт с тем, чтобы предлагать предоплаченные карты многоэмитентной (открытой) системы.

19. Мобильные сервисы, которые предлагаются одним или ограниченным числом предпринимателей, стоимость продуктов которых ограничена при использовании мобильных телефонов (например, приложения или мелодии для мобильных телефонов) не рассматриваются в настоящем Руководстве. Операции в данном случае сравнимы с предоплаченными картами одноэмитентной (закрытой) системы и меры по ПОД/ФТ, содержащиеся в данном Руководстве, к ним не применимы. Чтобы внести ясность хотелось бы отметить, что цель настоящего Руководства не является рассмотрение создания, продажи или потребления пре- или постоплаченного баланса клиента ОСС. Однако настоящее Руководство может применяться в том случае, когда «эфирные» средства могут быть переведены или приняты в качестве платежа или альтернативной валюты.

20. Большое количество компаний может быть вовлечено в предоставление услуг мобильных платежей. Роль этих учреждений может варьироваться в зависимости от бизнес-модели сервиса мобильных платежей и различные функции могут выполняться либо одним учреждением, либо через агентов⁷. Это может создавать нормативные трудности в определении того, на кого возложить надлежащую ответственность за исполнение контроля по ПОД/ФТ. В данном документе приводится руководство (Раздел VII) для стран какие из сторон подпадают под регулирование в сфере ПОД/ФТ. Учреждения, осуществляющие мобильные платежи могут подразделяться на следующие группы:

(а) ОСС – учреждение, предоставляющее техническую платформу, которая обеспечивает доступ к средствам при помощи мобильного телефона;

⁶ При такой модели эмитент (имеющий отношения с владельцем карточки) и эквайер (имеющий отношения с торговой точкой) является одним и тем же лицом. Это означает, что необходимость в комиссии между эмитентом и эквайером отпадает. Поскольку создается франшиза, то существует только один франшизополучатель, который и является стимулирующим фактором в этой модели. Внутри брэнда нет конкуренции как это бывает, когда объединяются несколько брэндов.

⁷ Учреждения, выполняющие мобильные платежи на рынке, могут действовать в качестве агентов для других учреждений, в зависимости от бизнес-модели, выбранной для сервиса мобильных платежей

(b) *Дистрибьютор (включая ритейлера)* – учреждение, которое продает или выдает деньги клиенту от имени эмитента, если такие денежные средства могут быть использованы для платежа. Дистрибьютор может также предлагать и иные услуги своим клиентам, например, техническую поддержку;

(c) *Эмитент электронных денег* – учреждение, выпускающее электронные деньги. Для целей настоящего Руководства электронные деньги – это запись о деньгах или ценностях, доступных клиенту, которые хранятся на платежном средстве, например, чипе prepaid-карты, мобильном телефоне или в компьютерной системе на счете⁸ в нетрадиционном его понимании банковского или небанковского учреждения⁹.

С. ПЛАТЕЖИ ЧЕРЕЗ ИНТЕРНЕТ

21. Интернет открыл мир электронной торговли и привел к развитию платежных систем, зародившихся в конце 1990-х гг. для осуществления переводов между продавцами и покупателями (P2B) и физическими лицами (P2P). В течение последнего десятилетия финансовые учреждения и ритейлеры продолжали развивать инструменты электронных платежей, в основе которых лежит использование Интернета и доступ к широкому кругу потребителей¹⁰.

22. Платежные системы в Интернете предоставляют клиентам доступ при помощи Интернета к prepaid-счетам, которые могут быть использованы для перевода денежных электронных денег и ценностей, хранящихся на этих счетах, другим лицам или предприятиям, у которых также открыты счета у того же провайдера. Получатель затем возвращает средства от эмитента путем внесения платежа или снятия средств. Снятие осуществляется путем перевода на обычный банковский счет, prepaid-карту или иную систему перевода денежных средств и ценностей. Если клиенты держат средства на prepaid-счетах, то у них нет необходимости этого делать. Если счет нужно пополнить, то это можно сделать путем debetования банковского счета или счета платежной карты или через иной финансовый источник, в случае необходимости.

23. Многие Интернет-платежные системы используют различные бизнес-модели. Эти сервисы называют «цифровые кошельки», «цифровые валюты», «виртуальные валюты» или «электронные деньги». Интернет-платежные системы могут значительно различаться, исходя из функционала, структуры и процедур. Сервисы могут позволить осуществлять переводы от физического лица физическому или юридическому лицу, обслуживающихся в этих системах, или операции могут быть ограничены конкретной торговой точкой или онлайн средой. Платежные онлайн-системы могут быть также связаны с иными платежными методами, например, prepaid-картами.

24. Поставщики электронных денег могут позволить третьим лицам брать на себя обмен национальных валют на электронные деньги или ценности. При такой бизнес-модели электронные деньги могут быть выпущены и возвращены через таких агентов. Такие агенты могут быть как связаны, так и не связаны с поставщиком услуг, действуя, таким образом, как виртуальный обменный пункт. Поставщики, которые используют эту модель, взимают деньги за перевод со счета на счет. Обменщики продают цифровую валюту со своих счетов, переводя ценности со своего счета на счет клиента. Направление в обратную сторону происходит тогда, когда получатель платежа хочет обналечить денежные средства. Покупая или продавая

⁸ Использование слова «счет» в настоящем определении не решает для стран вопрос о том, были ли установлены деловые отношения (см.сноску 38)

⁹ Это определение «электронных денег» взято из отчета Всемирного банка «*Инновации в розничной системе платежей во всем мире: краткая характеристика*» (июль 2012). Определение «электронных денег» должно оставаться гибким и может также отличаться от «сетевых денег», «М-денег», «электронного кошелька».

¹⁰ См. Всемирный банк (2012)

цифровые валюты за наличные или иные цифровые валюты, обменщики действуют в качестве виртуальных обменных пунктов.

25. Еще один распространенный вид Интернет-платежных услуг это продавцы цифрового выражения ценных металлов онлайн. Такие поставщики услуг продают виртуальное золото или серебро по рыночной цене, утверждая, что хранят драгоценные металлы от имени своего клиента. Посредники или обменщики, как их часто называют, покупают и продают электронные драгоценные металлы через собственные счета в сделках с клиентами. Такие обменщики самостоятельно определяют, какой вид платежа они обменивают на цифровую валюту.

26. Предоплаченные счета, которые используются клиентами для платежей на виртуальных аукционах, являются наиболее распространенными среди таких платежных систем. Получатель может как зарегистрироваться, а может и не регистрироваться как поставщик электронных услуг для получения денежного перевода. Клиент может авансировать свой платежный Интернет – счет при помощи обычного банковского счета. Средства на этом платежный Интернет – счете могут быть использованы для перевода их другому лицу – клиенту того же провайдера или возврата на обычный банковский счет клиента.

27. Платежные онлайн – системы также могут быть связаны с виртуальными играми или мирами, где могут быть использованы только собственные валюты для осуществления операции. Участники хранят на счете прокси-валюты, используя средства для операций с собственником, другими участниками или торговцами закрытой онлайн-среды. Получатели собственной валюты могут обменять ее на национальную валюту после выхода из среды.

28. Интернет-платежные сервисы, предусматривающие эмиссию электронных денег только для покупки товаров и услуг у эмитента электронных денег или в ограниченном количестве торговых точек, чей ассортимент товаров и услуг ограничен, не подпадают под настоящее Руководство, так как их можно сравнить с предоплаченными картами одноэмитентной (закрытой) системы. Как отмечалось ранее, регулирование и меры по ПОД/ФТ, предусмотренные настоящим Руководством, не применяются к таким услугам.

29. Развитие альтернативных цифровых валют является предметом внимания как органов, разрабатывающих политику в сфере ПОД/ФТ, так и частного сектора. Не смотря на то, что некоторые валюты «выпадают» из настоящего Руководства, однако ряд его положений все-таки может применяться. Лица, вырабатывающие политику, должны знать о существующих или зарождающихся электронных продуктах, услугах, формах валют и отслеживать их развитие на рынке для того, чтобы понимать, какие потенциальные риски они повлекут за собой и разрабатывать соответствующую политику. Учитывая степень развития альтернативных онлайн валют, ФАТФ может рассмотреть возможность продолжить работу в данном направлении в будущем.

30. Как было описано выше оплата услуг через Интернет может осуществляться как финансовыми, так и нефинансовыми учреждениями. В Разделе VII настоящего Руководства содержится описание для стран, какое из учреждений считать ответственной стороной (сторонами) в Интернет-платежных сервисах и, как следствие, кто подпадает под регулирование о ПОД/ФТ.

III. ОРГАНИЗАЦИИ, ПОДПАДАЮЩИЕ ПОД РЕКОМЕНДАЦИИ ФАТФ

31. В данном Разделе содержится указание на то, какие учреждения, занимающихся предоставлением НПМУ, подпадают под *Рекомендации ФАТФ* (то есть какие из них охвачены определением «*финансовых учреждений*», согласно Глоссарию ФАТФ).

32. В соответствии с *Рекомендациями ФАТФ* страны должны обеспечить, чтобы финансовый сектор и иные установленные секторы применяли превентивные меры. Если провайдеры НПМУ предоставляют товары и услуги, которые подпадают под положения *Рекомендаций ФАТФ*, то порой трудно определить, какое учреждение ответственно за реализацию превентивных мер по ПОД/ФТ из-за широкого круга учреждений, вовлеченных в оказание НПМУ. Соответственно, настоящий документ является руководством для стран о применении мер по ПОД/ФТ в отношении поставщиков НПМУ.

А. ОПРЕДЕЛЕНИЕ «ФИНАНСОВОГО УЧРЕЖДЕНИЯ», ИСПОЛЬЗУЕМОГО ФАТФ

33. Применяя превентивные меры по ПОД/ФТ к НПМУ, страны должны определить, какие учреждения подпадают под положения *Рекомендаций ФАТФ*. Определяя «*финансовые учреждения*» ФАТФ приводит перечень финансовой деятельности или операций, изложенных в Глоссарии и которые должны быть охвачены для целей ПОД/ФТ.

Таблица 1. Финансовые учреждения – определение ФАТФ

Термин «*финансовое учреждение*» означает любое физическое или юридическое лицо, которое в качестве деятельности осуществляет одно или более из перечисленных далее видов деятельности или операций (сделок) для клиента или от его имени:

1. Принятие депозитов и иных средств на возвратной основе от населения.¹¹
2. Кредитование¹²
3. Финансовый лизинг¹³
4. Услуги перевода денег или ценностей
5. Выпуск и управление средствами платежа (например, кредитные и дебетовые карточки, чеки, дорожные чеки, платежные поручения и банковские переводные векселя, электронные деньги).
6. Финансовые гарантии и обязательства.
7. Операции с:
 - (a) инструментами денежного рынка (чеки, векселя, депозитные сертификаты, производные ценные бумаги и т.д.);
 - (b) обменом иностранной валюты;
 - (c) инструментами, привязанными к обменному курсу, процентным ставкам и индексам;
 - (d) переводными ценными бумагами;
 - (e) биржевой торговлей по срочным товарным сделкам.
8. Участие в выпусках ценных бумаг и предоставление финансовых услуг, относящихся к таким выпускам.
9. Управление индивидуальными и коллективными портфелями.
10. Хранение и распоряжение наличными денежными средствами или ликвидными ценными бумагами от имени других лиц.

¹¹ Это охватывает также частные банки.

¹² Это включает среди прочего: потребительские кредиты, ипотечные кредиты, факторинг с правом или без права регресса, а также финансирование коммерческих сделок (включая учет векселей без права регресса).

¹³ Это не распространяется на схемы финансового лизинга, относящиеся к потребительским товарам.

11. Иное инвестирование, распоряжение или управление активами или денежными средствами от имени других лиц.

12. Андеррайтинг и размещение полисов страхования жизни и иных страховых полисов, связанных с инвестициями¹⁴.

13. Обмен денежных средств и наличных.

34. Провайдеры НПМУ подпадают под определение «*финансового учреждения*», предоставляя услуги по переводу денежных средств или ценностей или выпуская/управляя средствами платежа. Таким образом, они должны принимать превентивные меры по ПОД/ФТ, как это установлено *Рекомендациями ФАТФ*, включая надлежащую проверку клиентов, хранение данных и направление сообщений о подозрительных операциях. Однако может все-таки возникнуть трудность в определении того учреждения (или учреждений), предоставляющего НПМУ, которое ответственно за имплементацию превентивных мер и применение таких мер на национальном уровне. В Разделе VII настоящего Руководства содержится описание для стран, какого из поставщиков НПМУ считать ответственной стороной (сторонами) и, как следствие, кто подпадает под регулирование о ПОД/ФТ.

В. КОГДА ВОЗМОЖНО НЕ ПРИМЕНЯТЬ МЕРЫ ПОД/ФТ НА ОСНОВАНИИ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА

35. Страны при наступлении определенных обстоятельств могут принять решение о неприменении соответствующих превентивных мер, предусмотренных *Рекомендациями ФАТФ*, к видам деятельности, перечисленным в определении «*финансового учреждения*». Пояснительная записка к Рекомендации 1 говорит о том, что существует две ситуации, когда страны могут принять решение не применять некоторые из Рекомендаций ФАТФ, требующих от финансовых учреждений принимать соответствующие меры:

(a) имеется доказанный низкий риск отмывания денег и финансирования терроризма, это происходит в строго ограниченных и оправданных обстоятельствах; и это относится к конкретному типу финансового учреждения или деятельности, или УНФПП; или

(b) финансовая деятельность (кроме перевода денег и ценностей) осуществляется физическим или юридическим лицом на разовой или очень ограниченной основе (с учетом количественных и абсолютных критериев) таким образом, что имеется низкий риск отмывания денег и финансирования терроризма¹⁵.

36. Страны должны учитывать, что Пояснительная записка к Рекомендации 1 также содержит положение о том, что хотя собранная информация может различаться в зависимости от уровня риска, требования Рекомендации 11 хранить информацию должны применяться ко всей собранной информации. Говоря о НПМУ, которые являются НПМУ, то их деятельность не может подпадать под исключения ввиду того что осуществляется она разово или ограничено¹⁶.

IV. ОЦЕНКА РИСКОВ И УПРАВЛЕНИЕ РИСКАМИ В СФЕРЕ НПМУ

37. Для реализации риск-ориентированного подхода для ПОД/ФТ и НПМУ очень важно, чтобы страны и честный сектор выявляли и оценивали риски ОД/ФТ, которые несут НПМУ при

¹⁴ Это относится как к страховым организациям, так и к страховым посредникам (агентам и брокерам).

¹⁵ См. Пояснительную записку к Рекомендации 1 параграф 6 (FATF(2012))

¹⁶ В Рекомендации 10 сказано, что финансовые учреждения должны принимать меры по надлежащей проверке клиентов при совершении разовых операций, которые являются электронными переводами

разработке регулирования в сфере ПОД/ФТ для НПМУ и создании НПМУ. В соответствии с Рекомендацией 1 страны должны выявлять, оценивать и понимать риски ОД/ФТ¹⁷ и должны обеспечить, чтобы финансовые учреждения выявляли и оценивали риски ОД/ФТ¹⁸. Также определенное значение для НПМУ имеет и Рекомендация 15, которая требует от стран и финансовых учреждений выявлять и оценивать риски ОД/ФТ, которые могут возникнуть при развитии новых продуктов и деловых практик и использовании новых или развивающихся технологий. Кроме того, положения Рекомендации 15 предусматривают, что страны должны требовать от финансовых учреждений выявлять и оценивать риски, которые несут с собой новые продукты, деловые практики или использование новых технологий до того, как они будут запущены¹⁹.

38. В этом Разделе описаны некоторые факторы риска, а также меры по их снижению с тем, чтобы помочь и странам, и частному сектору в оценке рисков, которые несут НПМУ. При оценке рисков, которые несут НПМУ, страны должны принимать во внимание положения *Руководства ФАТФ «Об оценке рисков ОД/ФТ»*²⁰. Кроме того, страны и финансовые учреждения также должны учитывать и иные факторы риска, указанные в Пояснительной записке к Рекомендации 10 о надлежащей проверке клиентов. И хотя эти примеры являются необязательными элементами рекомендации ФАТФ, они в то же время являются полезными примерами факторов риска, которые более детально изложены ниже в связи с рисками ОД/ФТ, которые несут НПМУ.

А. ФАКТОРЫ РИСКА

39. Данный раздел документа описывает различные факторы риска, которые помогают выявлять риски ОД/ФТ, связанные с НПМУ. Многие НПМУ обладают характеристиками, которые снижают риски ОД/ФТ, и это должно считаться частью комплексного подхода при оценке рисков, связанных с конкретным НПМУ. Уровень риска ОД/ФТ, который несет в себе конкретный НПМУ, будет зависеть от учета всех факторов риска, факторов снижения риска и его функциональности.

і. Отношения без присутствия сторон и анонимность

40. Как и большинство банковских методов НПМУ предполагают возможность отношений без личного присутствия. В зависимости от своих характеристик НПМУ могут быть использованы для быстрого перевода средств по всему земному шару, покупок товаров и доступа к наличным средствам (прямо или косвенно) при помощи банкоматов. Отношения без личного присутствия могут рассматриваться как высоко рисковая ситуация с точки зрения ОД/ФТ. Если меры по надлежащей идентификации и верификации не снижают в должной мере риски, связанные с отношениями без личного присутствия, например, выдача себя за другого, то риски ОД/ФТ возрастают, поскольку возникают трудности с отслеживанием средств.

41. Если механизмы мониторинга и направления сообщений еще можно применять для выявления подозрительной деятельности, то отсутствие НПК делает невозможным для поставщика услуг выполнить эти требования. Например, это влияет на возможности поставщика услуг выявить тех клиентов, владеющих одновременно несколькими счетами.

42. Для предоплаченных карт риски, которые несет анонимность (то есть отсутствие идентификации клиента), могут иметь место, когда карта уже куплена, зарегистрирована,

¹⁷ Любое упоминание «страны» или «стран» применяется к территориям и юрисдикциям

¹⁸ См. Рекомендацию 1 и Пояснительную записку к ней.

¹⁹ См. Рекомендацию 15: «Странам и финансовым учреждениям необходимо определять и оценивать риски отмывания денег или финансирования терроризма, которые могут возникнуть в связи с (а) разработкой новых продуктов и новой деловой практики, включая новые механизмы передачи, и (б) использованием новых или развивающихся технологий как для новых, так и для уже существующих продуктов. В случае финансовых учреждений такая оценка риска должна проводиться до запуска новых продуктов, деловой практики или использования новых или развивающихся технологий. Им также следует принимать соответствующие меры для контроля и снижения этих рисков».

²⁰ См. FATF (2013a)

пополнена или используется клиентом. Уровень риска, который несет анонимность, связаны с функционалом карты, наличием мер по снижению рисков ОД/ФТ, например, лимиты на пополнение или покупку, доступ к наличным, а также возможностью использования за рубежом страны-эмитента. Предоплаченные карты могут быть пополнены различными способами при соблюдении различных степеней НПК, то есть через банки, Интернет, небольшие магазины розничной торговли, а также банкоматы. Хотя пополнение через банковский счет или Интернет начинается со счета или платежного инструмента, владелец которого был проидентифицирован, внесение наличных денежных средств или пополнение через другие НПМУ возможно и могут быть полностью анонимным. Кроме того, предоплаченные карты могут быть с легкостью переданы третьим лицам, неизвестным для эмитента, включая, но не ограничиваясь, «двойные карты», которые специально предназначены для переводов третьим лицам и для которых анонимность – эта характеристика продукта. Это вызывает озабоченность, если провайдеры этих продуктов находятся в стране, где регулирование и надзор в сфере ПОД/ФТ за провайдерами предоплаченных карт осуществляется на низком уровне, а продукты продаются и за рубежом²¹.

43. Мобильные платежные системы могут устанавливать свои клиентские отношения через агентов, онлайн или с использованием возможностей самой платежной системы. Те же каналы используются и для внесения денежных средств на мобильный счет. Риск, который несет анонимность возникает, когда мобильная платежная система используется или пополняется и имеет отношение к функционалу мобильных платежных услуг и наличию мер по снижению рисков ОД/ФТ, например НПК или пороговых значений для пополнения.

44. Для Интернет платежей характерны контакты без личного присутствия клиента. Это увеличивает возможность мошенничества с персональными данными или риск того, что клиент предоставит неточную информацию намеренно для того, чтобы скрыть незаконную деятельность, если эффективные меры для снижения этих рисков не применяются. Однако этот недостаток личного контакта обычно сводится на нет путем принятия альтернативных идентификационных механизмов, которые содержат в себе меры по снижению рисков. Риск, связанный с анонимностью Интернет – платежей или отсутствием идентификации клиента при использовании интернетовских платежных систем, имеет отношение к функционалу услуги, механизмам пополнения (если средства переводятся с обычного счета, то уровень риска значительно снижается) и наличию мер по ПОД/ФТ.

ii. Географический охват

45. Степень, в которой НПМУ используется по всему миру для осуществления платежей или перевода денежных средств, является важным фактором, который должен учитываться при определении уровня риска.

46. Предоплаченные карты многоэмитентной (открытой) системы часто позволяют клиентам осуществлять платежи на внутренних и международных пунктах продажи через глобальную платежную сеть. Такие карты принимаются как средства платежа там, где принимаются дебетовые или кредитные карты того же брэнда. Провайдеры предоплаченных карт могут находиться в одной стране, но продавать свои продукты за рубежом или через Интернет. Таким образом, эти карты могут быть использованы повсеместно для покупки товаров и услуг и доступа к наличным. Более того, некоторые программы для предоплаченных карт предусматривают для владельцев карт возможность перевода от лица к лицу. Такой международный охват некоторых видов предоплаченных карт в части осуществления платежей, доступа к наличным денежным средствам и перевода их делает эту категорию продуктов очень привлекательной для целей ОД/ФТ. Небольшой размер предоплаченной карты также делает их потенциально уязвимыми для злоупотребления преступниками, которые используют их вместо наличности, при перемещении через границу ценностей. Предоплаченные карты, предоставляющие доступ к услугам по всему

²¹ Опыт описан в Руководстве ФАТФ (2010), в Разделе 3 «Оценка рисков НПМ»

миру, особенно уязвимы в связи логистическими выгодами перемещения небольшого количества prepaid карт, привязанных к счетам, на которые внесены средства на большую сумму, которые невозможно установить, просто взглянув на карты, а не огромных сумм наличных денежных средств с использованием курьеров. Страны также должны изучить возможность применения Рекомендации 32 к определенным категориям prepaid продуктов, которые будут считаться оборотными инструментами на предъявителя.

47. Мобильные платежные системы и онлайн платежные системы, которые могут быть использованы для перевода средств по всему миру или географический охват которых высок при большом количестве контрагентов, являются более привлекательными для преступников с точки зрения ОД/ФТ, чем исключительно национальные модели. Кроме того, провайдеры НПМУ, находящиеся в одной юрисдикции могут предлагать свои услуги клиентам из других юрисдикций, где применяются иные меры по ПОД/ФТ и иные формы надзора. Это особенно вызывает озабоченность в тех случаях, когда поставщик НПМУ находится на территории юрисдикции со слабым режимом ПОД/ФТ.

iii. Методы пополнения.

48. Методы пополнения НПМУ влияют на уровень риска ОД/ФТ. Анонимные методы пополнения скрывают происхождение денежных средств, создавая высокие риски ОД/ФТ. Наличные денежные средства несут самый высокий возможный риск в силу своей анонимности и невозможности отследить цепочку операций. Однако если НПМУ предоставляют платформу для мониторинга операций, то пополнение продукта НПМУ через иные платежные сервисы, которые не предусматривают проверку личности клиента, также могут создать условия для механизма анонимного пополнения. Также, использование НПМУ prepaid модели, подразумевающей отсутствие риска при предоставлении кредита для провайдера, может снизить осуществление полной НПМ, при этом усилить риск ОД/ФТ.

49. Риски ОД/ФТ, которые несут с собой prepaid карты, увеличивается, если предусмотрено пополнение наличными средствами, в некоторых редких случаях, пополняемость без каких-либо ограничений карточного счета или низкий уровень соблюдения требований по НПМ. Это делает prepaid карты уязвимыми для использования преступниками, которые могут использовать их, например, как средство отмывания доходов от преступной деятельности путем размещения этих средств в финансовой системе или использования prepaid карт как альтернативы физическому трансграничному перемещению наличных денежных средств.

50. Мобильные платежные сервисы позволяют производить пополнение счетов и проводить транзакции разными путями. Многие платформы, независимо от модели, предусматривают, что средства могут списываться с банковского счета или счета платежной карточки, иные осуществляют пополнение через своих агентов. Если предыдущий метод пополнения ограничивал риски ОД/ФТ, а также ограничивал возможный доступ, то сейчас услуги оплаты наличными и не через банки открыли доступ для платежных систем, но это приводит к сокрытию источника происхождения средств, повышая риски ОД/ФТ. Мобильные платежные сервисы, которые позволяют осуществлять переводы со счета на счет, также предусматривают пополнение через третьи лица, что увеличивает риски ОД/ФТ, если владелец пополняемого счета не был должным образом проидентифицирован.

51. Онлайн-платежные системы, которые позволяют производить пополнение через третьих лиц из анонимных источников, также могут столкнуться с повышенными рисками ОД/ФТ. Особняком стоит пополнение через третьих лиц с использованием обменников и виртуальных обменников. Такие обменники/обменщики могут обойти запрет онлайн-платежной системы об определенных методах пополнения (например, «запрет на пополнение наличными») если они используют запрещенные платежные методы, перепродавая уже выпущенные цифровые валюты или электронно-денежные средства. Более того, провайдер при осуществлении мониторинга

увидит только имя обменщика, но никогда не увидит, кто конкретно отдавал указания на пополнение счета.

iv. Доступ к наличным денежным средствам

52. Доступ к наличным денежным средствам через международную сеть банкоматов повышает уровень риска ОД/ФТ. Такой доступ к наличным денежным средствам может быть прямым, например, как в случае с prepaid картами, когда пополнение идет в одной стране, а снятие – в другой. При этом мобильные и он-лайн платежные системы становятся все более связанными с иными НПМУ, например, prepaid картами, которые косвенно предоставляют возможность снимать наличные.

v. Сегментация рынка

53. Оказание НПМУ обычно требует сложной инфраструктуры, с привлечением нескольких участников для осуществления платежей. В деятельность, связанную с prepaid картами, обычно вовлечено несколько сторон, включая программного менеджера, эмитента, эквайера, платежную сеть, дистрибьютора и агента. При этом поставщики мобильных платежных услуг должны взаимодействовать с несвязанными между собой поставщиками услуг, а также международными партнерами для осуществления трансграничных операций.

54. Большое количество участников вовлечено в предоставление НПМУ, особенно если охватываются несколько стран, что повышает риск ОД/ФТ продукта в результате возможной сегментации и потери информации о клиенте или операции. Это особенно вызывает озабоченность в тех случаях, когда нет возможности точно и определенно установить, какое из учреждений подпадает под требования по ПОД/ФТ, какое должно их выполнять, а также какая из стран, участвующая в проведении операции обязана осуществлять регулирование и надзор за соблюдением требований о ПОД/ФТ.

55. Использование агентов и полагание на третьих неаффилированных лиц при установлении деловых отношений с клиентом и пополнении способствует возникновению рисков ОД/ФТ, особенно если собираемая информация не передается в учреждения, которые должны выполнять обязательства по ПОД/ФТ. Поставщик услуг может взять на себя ответственность за все стороны взаимоотношений с клиентом (то есть регистрация, внесение наличных денежных средств/их снятие и проведение операций) и это снижает уровень риска. Также имеет значение организационная структура и процессы, которые имеют место для обучения, управления и контроля сети агентов.

56. Кроме того, учреждения, занимающиеся НПМУ часто выходят из таких секторов, например как ОСС, которые незнакомы с требованиями о ПОД/ФТ. И как следствие идет ограничение по сравнению с традиционным банковским сектором и меры по НПК зачастую ограничены анализом информации о необычных операциях и обратной связью от дистрибьюторов. При этом цепочка информации не дает возможность установить перемещение средств. Например, цепь информации по одной финансовой операции может охватить нескольких участников, некоторые из которых находятся на территории других государств. Это может привести к замедлению процесса следствия, которое и так затруднено из-за высокой скорости денежных потоков. При этом возникают трудности и при аресте и замораживании преступных активов, которые могут быть быстро переведены или перевезены в другое государство с использованием НПМУ.

57. Провайдеры НПМУ обеспечивают функционирование банковских счетов и используют банковскую систему для периодических расчетов с агентами и партнерами по НПМУ. Однако даже если оптовая сделка для банковских расчетов между провайдером НПМУ предусматривает обязательства по НПК в отношении провайдера НПМУ, то практически отсутствует или

ограничена возможность увидеть операции клиента провайдера НПМУ, равно как и осуществлять надзор операции между провайдером НПМУ и клиентами.

58. Онлайн-овые платежные системы, которые сами стараются «держать в своих руках» все аспекты взаимоотношений с клиентами (например, регистрацию, операции по пополнению/снятию), и подпадают под требования о ПОД/ФТ, могут нести более низкие риски ОД/ФТ, чем децентрализованные системы. Провайдеры, полагающиеся на неаффилированных третьих лиц для выпуска или возврата электронных валют, тем самым ведут систему к сегментации услуг и увеличивает риски ОД/ФТ. Сегментация онлайн-овых платежных систем особенно вызывает озабоченность, учитывая их транснациональный характер, когда провайдер может находиться на территории юрисдикции с ненадлежащим регулированием и надзором в сфере с ПОД/ФТ.

vi. Матрица рисков

59. Матрица рисков, приведенная ниже²², содержит описание некоторых факторов риска, перечень которых не является исчерпывающим и которые помогают выявлять риски, связанные с конкретным видом НПМУ, включая предоплаченные карты, мобильные и онлайн-овые платежные системы. Очень важно использовать единый подход при оценке рисков, связанных с определенным НПМУ, а не рассматривая факторы риска, содержащиеся в матрице один за одним: риски, факторы их снижающие, и функционал определенного НПМУ должны рассматриваться все вместе, чтобы понять несет или данный продукт высокие или низкие риски ОД/ФТ. Факторы риска, приведенные ниже, носят описательный характер, и некоторые НПМУ могут содержать как высоко, так и низко рисковые факторы, которые должны учитываться и сочетаться с иными факторами риска для определения общего уровня риска.

60. И хотя матрица рисков в полном объеме применяется для НПМУ, природа и функциональность НПМУ могут варьироваться в значительной степени при сравнении с иными платежными инструментами (например, с дебетовыми и кредитными картами) и продукт может быть создан различными способами, исходя из целей использования. По этой причине, оценка рисков для НПМУ должна проводиться с учетом индивидуальных характеристик каждого отдельно взятого продукта. Поступая так, необходимо учитывать следующие риски, связанные с НПМУ.

Таблица 1 Факторы рисков методов платежей (1)

Критерии		Наличные денежные средства (2)	НПМ с высоким риском	НПМ с низким риском
НПК	Идентификация	Анонимная	Анонимные	Личность клиента устанавливается
	Верификация	Анонимная	Личность клиента (если установлена) не проверяется с использованием надежных, полученных из независимых источников документов, данных или информации	Личность клиента проверяется с использованием надежных, полученных из независимых источников документов, данных или информации (Рек.10)

²² Впервые матрица рисков была опубликована в типологическом исследовании ФАТФ «Новые способы отмывания денег с использованием новых платежных методов» (2010). Это обновленная версия матрицы рисков, которая изначально была опубликована в типологическом исследовании ФАТФ «О новых платежных методах» (2006)

	Мониторинг	Отсутствует	Отсутствует	Проводится постоянный мониторинг деловых отношений
Хранение данных		Данные получены для органов через систему декларирования о трансграничном перемещении (Р.32)	Записи об электронных операциях ведутся, но не хранятся и не предоставляются по запросу правоохранительных органов	Записи об электронных операциях хранятся и предоставляются по требованию правоохранительных органов
Лимиты сумм	Макс. сумма, хранящаяся на счету/счетах из расчета на одно лицо	Данные получены для органов через систему декларирования о трансграничном перемещении (Р.32)	Без ограничения	Ограничения по сумме
	Макс. сумма операции (включая пополнение/снятие средств)	Без ограничения	Без ограничения	Ограничения по сумме
	Макс. частота операций	Без ограничения	Без ограничения	Ограничения по количеству операций
Методы пополнения		Не доступно	Анонимные источники вложения средств (например, наличные деньги, денежные переводы, анонимные НПМ); также множественные источники вложения средств, например, третьи лица	Вложение средств через счета, открытые в регулируемом финансовом или кредитном учреждении, или из иных установленных источников, на которые распространяются обязательства и надзор в сфере ПОД/ФТ
Географические ограничения		Некоторые виды валют принимаются более широко, нежели другие; валюту можно обменять через посредников	Перевод средств за рубеж или снятие средств за рубежом	Перевод и снятие средств только внутри одного государства
Ограничение использования	Возможность приема к оплате (прием продавцами)	В целом принимаются	Большое количество принимающих продавцов/торговых точек (например, при использовании «VISA»)	Небольшое количество принимающих продавцов/торговых точек

			или «MasterCard»)	
	Возможность осуществления различных операций	Платежи: физическое лицо - компания, компания - физическое лицо - физическое лицо. Использование через Интернет невозможно	Платежи: физическое лицо - компания, компания - компания, физическое лицо - физическое лицо. Использование через Интернет возможно	Платежи: физическое лицо - компания, компания - компания, но не физическое лицо - физическое лицо. Использование через Интернет возможно
	Снятие денег	Не доступно	Анонимное и неограниченное снятие денег (например, снятие наличных через банкоматы)	Ограниченные возможности снятия (например, перевод только на ссучные счета); ограничения по снимаемым суммам и частоте снятия (например, не более определенной установленной суммы в течение календарного года)
Сегментация услуг	Взаимодействие провайдеров услуг	Не доступно	Несколько независимых провайдеров услуг выполняют отдельные этапы операции без эффективного надзора и координации	Вся операция проводится одним провайдером услуг
	Аутсорсинг	Не доступно	Аутсорсинг нескольких отдельных этапов; аутсорсинг в юрисдикции, где нет соответствующих мер контроля; отсутствие надзора и четкого разграничения ответственности	Все процессы осуществляются в одной компании в соответствии с высокими стандартами

Примечание к таблице

(1) Матрица рисков взята из типологического исследования 2010 г. и уделяет особое внимание факторам риска, было пересмотрено заглавие только двух колонок «высокий/низкий риск» на «высоко рисковые факторы/низко рисковые факторы». Это согласуется с *Рекомендациями ФАТФ*, которые также ссылаются на низко /высоко рисковые сценарии развития событий.

(2) Колонка наличные денежные средства приводится для сравнения факторов риска, которые несут НПМ и наличные денежные средства, отражая высокий/низкий уровень риска ОД/ФТ. Контроль за наличными денежными средствами может осуществляться, исходя из перемещения наличных денежных средств с использованием системы декларирования или раскрытия в соответствии с требованиями Рекомендации 32. Положения Рекомендации 32 также применимы к определенным продуктам, если они отнесены к оборотным инструментам на предъявителя.

В. МЕРЫ ПО СНИЖЕНИЮ РИСКОВ

61. Общий уровень риска конкретного НПМУ (в данном контексте) является совокупностью каждого из факторов риска, описанного выше. Более того, процедуры по снижению рисков должны быть пропорциональны уровню риска конкретного продукта или услуги. Принятие пропорционального подхода позволяет свести на нет риски от НПМУ, при этом поддерживая функциональность, нацеленную на удобство и простоту его использования клиентом. На фоне таких выводов, учитывая национальные и применяемые нормативные основы, учреждения частного сектора должны учитывать риски ОД/ФТ конкретного продукта или услуги на стадии его разработки/проектирования, чтобы свести все его уязвимости к минимуму. Данный Раздел Руководства содержит описание некоторых мер по снижению уровня рисков, которые частный сектор должен принимать во внимание в процессе создания продукта.

62. Финансовые учреждения должны выявлять, оценивать и понимать риски, связанные с НПМУ, которые они предоставляют, до того, как будут выработаны процессы и процедуры по НПК. В частности, финансовым учреждениям необходимо проводить оценку риска ОД/ФТ, которые могут возникнуть в связи с разработкой новых продуктов и новой деловой практики, включая новые механизмы передачи. Финансовые учреждения должны проводить такую оценку риска до запуска новых продуктов. Это очень важный шаг, который позволяет финансовым учреждениям разработать риск-ориентированный комплекс мер по ПОД/ФТ пропорционально выявленному уровню риска.

i. Надлежащая проверка клиентов

63. НПК – это эффективная мера для снижения рисков ОД/ФТ, в соответствии с концепцией риск-ориентированного подхода, меры, принимаемые НПМУ, включая меры по идентификации и верификации личности их клиентов могут варьироваться в зависимости от уровня риска, который представляет конкретный продукт в соответствии с положениями *Рекомендаций ФАТФ* и законодательства, действующего на территории того или иного государства.

64. Если уровень риска ОД/ФТ невысок, то финансовым учреждениям может быть разрешено проводить упрощенные меры по НПК, которые должны учитывать природу низкого уровня риска. Упрощенные меры по НПК не означает неприменение или отсутствие мер по НПК. Для провайдеров НПМУ, которые устанавливают деловые отношения²³, упрощенные меры по НПК могут быть базовыми и минимальными, но они должны учитывать все четыре составляющих НПК, указанных в Разделе VI. В соответствии с концепцией риск-ориентированного подхода необходимо иметь информацию о виде и величина клиента и операции, а также мерах по выполнению этих минимальных стандартов, которые будут варьироваться в зависимости от уровня риска. При наличии низкого риска требования о выполнении мер по НПК в части идентификации, верификации и мониторинга, предусмотренные Рекомендацией 10, могут быть, например, менее интенсивными и формализованными в части сбора информации, мониторинга и полагания на разумное предположение о возможном использовании основных продуктов. Кроме того, он может быть менее детализированным и не таким частым. *Рекомендации ФАТФ* содержат примеры обстоятельств, когда риски ОД/ФТ могут считаться потенциально низкими в отношении определенной категории клиентов, стран, географических регионов или товаров, услуг, операций или каналами поставки²⁴. В случае НПМУ примером низкого риска может служить «четко определенные и ограниченные по объему финансовые продукты и услуги, предоставляемые определенной категории клиентов для облегчения доступа к этим продуктам и услугам». Провайдеры НПМУ должны также учитывать обстоятельства, при которых клиент

²³ Рекомендации ФАТФ не определяют этот момент. Решение о том, установлены отношения или нет, принимают сами страны

²⁴ См. Пояснительную записку к Рекомендации 10 параграф 17

НПМУ может рассматриваться как высоко рисковый, и иметь процедуры для применения усиленных мер по НПК, если выявлены высокие риски ОД/ФТ²⁵.

65. Стоит отметить, что Рекомендации ФАТФ позволяют при осуществлении деятельности без личного присутствия сторон провести проверку личности клиента после установления деловых отношений (а не до или вовремя их установления), если важно не нарушить обычное осуществления деятельности при условии, если управление рисками ОД/ФТ осуществляется эффективно²⁶.

66. Рост функциональности НПМУ может потребовать усиленных мер по НПК. Проверка личности клиента без личного присутствия зачастую требует подтверждения данных, полученных от клиента с информацией из баз данных, которые ведут третьи лица, или иных надежных источников, а также, возможно, выявления адреса Интернет – протокола клиента²⁷ или поиска информации во всемирной паутине принимая во внимание тот факт, что сбор информации должен осуществляться в соответствии с национальным законодательством о неприкосновенности частной жизни. Возможно было бы целесообразно использовать несколько методов для эффективной проверки личности клиента. В ситуации когда уровень риска ОД/ФТ высок должны применяться усиленные меры по НПК, пропорциональные существующему риску.

67. Во всех этих случаях особую роль играет мониторинг операций и направление сообщений о подозрительных операциях. Важность этих процедур возрастает, если получение достоверной информации о клиенте затруднено. Это может иметь место в тех странах, у которых отсутствует надежная система удостоверения личности или альтернативные формы для проведения идентификации.

68. Предоплаченные карты и мобильные платежные услуги распространяются обычно с использованием разветвленной сети агентов или дистрибьюторов, которых поставщик услуг может использовать для проведения идентификации, когда лицо лично присутствует. В таких случаях дистрибьюторы и агенты выполняют обязательства по НПК от имени провайдера; программный менеджер или эмитент должны включать дистрибьюторов и агентов в свои программы по ПОД/ФТ и отслеживать их соответствие принимаемым мерам по НПК.

69. Использование агентов дает учреждениям возможность проводить НПК, когда клиент лично присутствует. При использовании Интернета поставщик мобильных платежных услуг будет вынужден полагаться на идентификацию и верификацию, проведенные без личного присутствия.

70. Онлайн-платежные системы как правило устанавливают свои отношения с клиентом посредством Интернета; тот же канал используется для пополнения счетов, доступ к которым осуществляется в онлайн режиме. Поставщик онлайн-платежных сервисов в такой ситуации будет вынужден полагаться на идентификацию и верификацию, проведенные без личного присутствия.

ii. Лимиты сумм, пополнения и географические ограничения

71. Установление лимитов для НПМУ может оказаться хорошим механизмом для снижения рисков ОД/ФТ, так долго, сколько это сочетается с иными мерами по ПОД/ФТ, например мониторинг счета и операций и направление сообщений о подозрительных операциях. Введение географических ограничений или лимитов на пополнение также снижает риски того, что НПМУ будет использована в целях ОД/ФТ. Ограничение функционала НПМУ определенным

²⁵ См. Пояснительную записку к Рекомендации 10 параграфы 15 и 20.

²⁶ См. Пояснительную записку к Рекомендации 10 параграф 11

²⁷ Каждый раз, когда лицо входит в Интернет провайдер Интернет услуг на динамичной основе присваивает ему уникальный идентификационный номер, похожий на телефонный номер – адрес Интернет-протокола, который в ходе процесса регистрации аккаунта получает информацию о географическом местонахождении, временных рамках, которые могут быть сравнены с физическим адресом лица. Примечание: Рекомендации ФАТФ не требуют получения такой информации.

географическим регионом или конкретными товарами или услугами, которые могут быть приобретены, снижает их привлекательность для лиц, отмывающих деньги и финансирующих терроризм. При этом следует отметить, что такие ограничения снижают привлекательность продукта в целом; финансовые учреждения и страны должны учитывать негативный эффект от любых ограничений, устанавливаемых для законной деятельности клиентов. Эти меры должны быть рассмотрены и реализованы на стадии разработки проекта.

72. Учитывая тот факт, что риск ОД/ФТ возрастает с увеличением функционала НПМУ, финансовые учреждения могут рассмотреть вопрос о целесообразности установления индивидуального подхода к услугам, оказываемым клиентам. Это должно быть сделано в индивидуальном порядке на стадии создания продукта; таким образом, финансовые учреждения могут рассмотреть вопрос о применении различных ограничений, например пороговых значений, для НПМУ с целью обеспечить низкий уровень риска с тем, чтобы затем разрешить применять им упрощенные меры по НПК. При таком сценарии, объем НПК и других мер ПОД/ПФТ должен возрастать пропорционально функционалу и, следовательно, повышению уровня риска.

73. Многие программы prepaid карт уже предусматривают ограничения по пополнению и длительности с тем, чтобы обеспечить низкие риски ОД/ФТ для оставшихся на prepaid карте средств иные общие меры могут включать в себя ограничения по сумме, которая является prepaid, доступность к средствам при помощи карты, а также ограничения возможности пополнения prepaid карты. Ограничения по срокам и суммам пополнения, как и ограничения на снятие наличных могут сделать prepaid карты менее привлекательными для преступников. Пороговые значения – это эффективные меры для установления того максимума, который может быть внесен на prepaid карту и храниться на одной карте одновременно или в течение определенного промежутка времени. Предел таких пороговых значений должен быть определен с учетом риск-ориентированного подхода и может варьироваться в зависимости от наличия иных мер по ПОД/ФТ. Однако должное внимание должно быть уделено защите клиентов с тем, чтобы обеспечить доступ последних к их средствам, если это необходимо. Также должна быть обеспечена защита прав в том случае, если клиенту было отказано в доступе к средствам, хранящимся на prepaid карте.

74. Кроме того, существует возможность того, что некоторые программы по prepaid картам позволяют переводить денежные средства напрямую от лица к лицу, что может представлять высокий риск злоупотреблений в системе ОД/ФТ. Особенно в тех случаях, когда предполагается, что переводы денег напрямую от лица к лицу могут быть сделаны через карту prepaid – ограничения, налагаемые на такие возможные переводы, могут послужить эффективной мерой для смягчения рисков ОД/ФТ, особенно, применительно к обороту наличных денежных средств. Этот эффект можно усилить за счёт совмещения ограничений по переводам с ограничениями пополнения счетов или снятия со счетов денежных средств. При применении риск-ориентированного подхода максимальная сумма, которая может быть переведена от лица к лицу с использованием карт prepaid может варьироваться в зависимости от наличия иных мер ПОД/ФТ, например таких, как географические (территориальные) ограничения.

75. Для сектора мобильных платежей могут быть предусмотрены ограничения по максимальной сумме, которая может находиться на мобильном платежном счете, или максимальной сумме, допускаемой при разовой сделке, включая снятие наличных, а также по частоте или суммарному значению операций и снятию наличных, разрешенных в день/неделю/месяц/год или сочетание всего вышеперечисленного. Установление географических ограничений или ограничений на покупки также снижает риски использования мобильных платежных сервисов для целей ОД/ФТ.

76. Онлайн-платежные системы обычно представляют собой многоуровневую структуру для клиентов и должны рассматриваться каждая по отдельности. Некоторые цифровые валюты изначально были созданы для осуществления переводов от лица к лицу в онлайн-среде, например, игровой, что снижало риски ОД/ФТ, так как оборот их осуществляется в замкнутой

системе. Однако уровень рисков может возрасти, если цифровая валюта может быть обменена через третьи лица на национальную валюту.

iii. Источники пополнения

77. При оценке рисков ОД/ФТ провайдеры НПМУ должны учитывать источник пополнения и могут ограничить источники пополнения для конкретного продукта. Анонимные источники пополнения, например, наличные денежные средства или иные анонимные НПМУ повышают уровень риска ОД/ФТ. Провайдерам НПМУ следует принять всеобъемлющий подход по снижению рисков ОД/ФТ, реализовывая эти меры; ограничения могут быть сочетаться с иными лимитами, описанными выше.

78. Если наличные денежные средства используются физическим лицом, для того, чтобы пополнить один или несколько НПМУ, в отношении которых существуют определенные ограничения, то провайдер НПМУ может потребовать у лица проведение идентификации, если сумма наличных денежных средств превышает определенный лимит на пополнение наличными как индивидуального счета, так и на проведение одной или нескольких операций в день.

iv. Хранение данных, мониторинг операций и направление СПО.

79. Данные об операциях и НПК являются одной из основ системы ПОД/ФТ и проведения правоохранительными органами расследований. Как минимум информация должна содержать следующие данные: о платеже или переводе средств, включая идентификационные данные сторон по операции, номер счета, и вид и дату проведения операции, а также переведенную сумму. Относительный размер операции не равен автоматически сумме операции, информация о которой была передана в правоохранительные органы. Таким образом, данные должны храниться обо всех операциях, независимо от суммы. Данные, которые хранятся, должны быть достаточно для того, чтобы отследить средства, путем восстановления всей цепочки.

80. Электронная природа НПМУ в принципе закладывает хорошую основу для эффективного учета данных и мониторинга операций. Провайдеры НПМУ должны хранить все данные, имеющие отношение к операциям и НПК, минимум пять лет, как того требуют положения Рекомендации 11 или больше, в соответствии с требованиями законов, применяемых в государстве.

81. Уникальными для мобильных платежей являются номера мобильных телефонов отправителя и получателя, а также данные о сим-карте получателя и потенциального получателя. Также это может быть информация, полученная от ОСС, касаемо точного местонахождения телефонов отправителя и получателя на момент проведения операции. В зависимости от характера и суммы операции, информация о местонахождении может быть полезной для базы данных о записи транзакций. Поскольку сбор такой информации не предусмотрен Рекомендациями ФАТФ, то провайдеры могут рассмотреть этот вопрос, принимая во внимание, что сбор информации должен осуществляться в соответствии с положениями национального законодательства о неприкосновенности частной жизни, поскольку она может быть полезна для мониторинга деятельности клиента.

82. Провайдеры НПМУ должны предусмотреть возможность создания системы мониторинга операций, которая поможет выявить подозрительную деятельность, основываясь на типологиях и индикаторах отмыывания денег и финансирования терроризма. Такие системы мониторинга должны учитывать клиентские, страновые или географические риски, а также риски, связанные с продуктами, услугами и каналами поставки. Система мониторинга операций может использоваться для выявления множественных счетов или продуктов, которые есть у физического лица или группы, например множественные предоплаченные карты.

83. Провайдеры НПМУ должны анализировать хранящуюся информацию и данные с тем, чтобы выявлять необычные проявления или деятельность. Когда провайдер НПМУ выявляет операцию, в отношении которой у него возникли подозрения или основания подозревать, что привлечены средства являющиеся доходами от преступной деятельности или связаны с финансированием терроризма, то он должен сообщить о своих подозрениях в соответствующее подразделение финансовой разведки в соответствии с положениями *Рекомендаций ФАТФ*, а также национального законодательства.

84. Провайдеры НПМУ должны относиться очень внимательно к тем операциям или деятельности, у которой нет явного юридического или экономического смысла. В частности, провайдеры должны принимать во внимание ситуации, когда НПМУ используются как замена банковского счета без очевидного правового смысла. Так, prepaid карта используется необычным способом (например, операции на большую сумму), что может считаться необычным в некоторых обстоятельствах с учетом того, что prepaid карта не обеспечивает должный уровень защиты (то есть ограничения по страхованию вкладов) или некоторые выгоды (например, проценты), которые имеют место во многих юрисдикциях для банковских счетов. Провайдеры должны учитывать не только смысл использования prepaid карты, но и так же те обстоятельства, которые существуют в той юрисдикции, где они осуществляют свою деятельность. Дополнительное руководство относительно разработки и развития эффективной системы мониторинга операций, особенно в части выявления подозрительных транзакций, может быть найдено в типологическом исследовании ФАТФ о НПМ.

V. ВЛИЯНИЕ РЕГУЛИРОВАНИЯ НА РЫНОК НПМУ

85. Разрабатывая регуляторный режим по ПОД/ФТ для НПМУ страны также должны учитывать влияние регулирования на рынок НПМУ. В частности, страны обеспечивают, чтобы меры регулирования в сфере ПОД/ФТ были пропорциональны рискам ОД/ФТ, связанным с НПМУ, а существующие меры регулирования не имели бы негативного влияния на функционирование существующих продуктов и не препятствовали бы разработке новых. В настоящем Разделе будет рассмотрен вопрос влияния регулирования на рынок НПМУ, включая влияние на обеспечение доступности финансовых услуг.

A. РУКОВОДСТВО ФАТФ ПО ДОСТУПНОСТИ ФИНАНСОВЫХ УСЛУГ

86. В июне 2011 г. после обращения «Двадцатки» ко всем организациям, вырабатывающим стандарты, помочь странам в применении их стандартов таким образом, чтобы был обеспечен доступ к финансовым услугам, ФАТФ опубликовала Руководство «*Меры по противодействию отмыванию денег и финансированию терроризма и доступность финансовых услуг*»²⁸. Не уделяя особого внимания платежным методам, настоящее Руководство относит prepaid карты и мобильные переводы к платежным инструментам, которые обеспечивают доступ к финансовым услугам. Следует также отметить, что некоторые правительства обеспечивают доступ к финансовым услугам используя НПМУ, например, prepaid карты для выплаты государственных субсидий; этот подход примем для получателей субсидий. Руководство ФАТФ по доступности финансовых услуг обеспечивает поддержку странам и их финансовым учреждениям в разработке новых мер по ПОД/ФТ, которые бы отвечали бы главной цели – обеспечение доступности финансовых услуг, не подрывая те меры, которые направлены на борьбу с преступностью.

V. ПРИНЦИПЫ «ДВАДЦАТКИ» ПО ДОСТУПНОСТИ ИННОВАЦИОННЫХ ФИНАНСОВЫХ УСЛУГ

²⁸ См. ФАТФ (2013b)

87. Принципы «Двадцатки» по доступности инновационных финансовых услуг²⁹ были приняты в 2010 г. и поддерживают применение принципа пропорциональности в качестве баланса между рисками и выгодами путем приведения в соответствие регулирования, направленного на снижение риска продукта без наложения чрезмерного бремени, которое может сдерживать развитие инноваций³⁰. Если говорить в общих чертах, то принцип пропорциональности уже заложен в *Рекомендациях ФАТФ*. Принцип пропорциональности позволяет странам применять риск-ориентированный подход, предусматривая помимо всего прочего применение упрощенных мер по надлежащей проверке клиентов (НПК) для низко рискованных продуктов, а в некоторых случаях отказаться от применения мер по НПК³¹. Принципы «Двадцатки» также признают особую роль предоплаченных карт, как возможного инструмента обеспечения доступности к финансовым услугам рекомендуют установить специальный режим, отвечающий рискам, возникающим в отношении конкретной категории оказываемой услуги³². Пропорциональный подход позволяет обеспечить доступ на рынок и увеличить число участвующих поставщиков услуг и тех, кто не имеет доступа к обычным банковским услугам. Такой подход позволяет увеличить объемы использования законных каналов таким образом снижая риски ОД/ФТ, связанные с финансовыми запретами.

VI. РЕГУЛИРОВАНИЕ, НАДЗОР И РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД

88. Этот Раздел документа содержит руководство для стран с тем, чтобы помочь им в разрешении конкретных вопросов, связанных с применением *Рекомендаций ФАТФ* в части НПК. Он разъясняет, как осуществлять регулирование надзора за организациями, занимающимися НПК и какое влияние такого регулирования и надзора на эффективную реализацию мер по ПОД/ФТ.

A. РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД, МЕРЫ ПО ПОД/ФТ И НАДЗОР

89. *Рекомендации ФАТФ* поддерживают развитие и реализацию риск-ориентированного подхода в сфере ПОД/ФТ. Этот подход позволяет странам, соблюдая требования ФАТФ, применять более гибкий комплекс мер для более эффективного распределения своих ресурсов и применения превентивных мер, которые соотносятся с природой риска, а также прилагать усилия наиболее эффективно. Самым важным первым шагом для риск-ориентированного подхода является то, что страны должны сначала выявить, оценить и понять существующие риски отмывания денег и финансирования терроризма, с которыми они встречаются, как того требует Рекомендация 1. Это одно из основных требований, которое применяется ко всем мерам по ПОД/ФТ в соответствии с *Рекомендациями ФАТФ*. Также особое значение в настоящем контексте играет и Рекомендация 15, которая содержит требование для стран и финансовых учреждений определять и оценивать риски отмывания денег или финансирования терроризма, которые могут возникнуть в связи с разработкой новых продуктов и новой деловой практики, включая новые механизмы передачи, и использованием новых или развивающихся технологий как для новых, так и для уже существующих продуктов. Страны должны принимать соответствующие и пропорциональные меры для снижения рисков, которые были выявлены в отношении НПК.

²⁹ См. Принципы и Отчет о доступности инновационных финансовых услуг (2010)

³⁰ См. Принцип 8 «Пропорциональность»: «Выстройте политику и создайте правовую базу, пропорциональную рискам и выгодам, которые имеют место для инновационных продуктов и сервисов и основана на понимании пробелов и барьеров в существующем регулировании»

³¹ Пояснительная записка к Рекомендации 1 в параграфе 6 предусматривает следующее: «Исключения — страны могут решить не применять некоторые из Рекомендаций ФАТФ, устанавливающих требования для финансовых учреждений или УНФПП, при условии, что: имеется доказанный низкий риск отмывания денег и финансирования терроризма, это происходит в строго ограниченных и оправданных обстоятельствах; и это относится к конкретному типу финансового учреждения или деятельности, или УНФПП». Полный текст Пояснительной записки к Рекомендации 1 доступен для просмотра на сайте www.fatf-gafi.org.

³² Пропорциональный правовой режим может включать в себя, например, сочетание максимально возможного оборота операций, пороги, ликвидность и требования относительно банкротства)

90. Основной принцип риск-ориентированного подхода сводится к тому, что если уровень риска высокий, то страны должны требовать от финансовых учреждений применять усиленные меры для управления рисками и их снижения и, соответственно, когда уровень риска низкий (и нет подозрений в отмывании денег или финансирование терроризма) можно принимать упрощенные меры. Это означает, что страны могут и должны отойти от принципа «один подход подходит всем» и должны изменить свои режимы ПОД/ФТ, исходя из национальных рисков. В соответствии с концепцией риск-ориентированного подхода интенсивность мер по ПОД/ФТ зависит от уровня и природы выявленных рисков. Риск-ориентированный подход *требует* от стран усилить меры в сферах, где уровень риска высок и *разрешает* принимать упрощенные меры, если уровень риска низкий и предусматривает исключения в части применения ряда требований, если доказано, что уровень риска низкий и остальные требования соблюдены³³. Это позволяет странам с учетом требований ФАТФ применять гибкий подход к мерам с тем, чтобы распределять свои ресурсы эффективно и предпринимать превентивные меры, соразмерные природе риска, для того, чтобы наиболее эффективно сосредоточить свои усилия. Кроме того, риск-ориентированный подход позволяет НПМУ повысить уровень доступности к финансовым услугам, что снизит риски ОД/ФТ и поможет в достижении эффективного применения положений *Рекомендаций ФАТФ*.

91. Как было отмечено выше, задача настоящего Руководства о риск-ориентированном подходе, применяемого в отношении НПМУ это создать новое и дополнить существующие Руководства ФАТФ, связанные с развитием и применением риск-ориентированного подхода в сфере ПОД/ФТ, в частности Руководства ФАТФ «Об оценке рисков ОД/ФТ» и Руководстве ФАТФ «О мерах по противодействию отмыванию денег и финансированию терроризма и обеспечению доступности финансовых услуг».

В. НАДЛЕЖАЩАЯ ПРОВЕРКА КЛИЕНТОВ

92. В соответствии с положениями Рекомендации 10 страны должны требовать от финансовых учреждений проводить НПК с тем, чтобы идентифицировать своих клиентов и выяснять всю необходимую информацию для ведения дел с ними. Требования по НПК направлены на то, чтобы финансовые учреждения могли эффективно идентифицировать, проверять своих клиентов и осуществлять мониторинг в отношении них, а также отслеживать операции, которые проводят последние в части выявления рисков отмывания денег и финансирования терроризма.

93. В соответствии с положениями Рекомендации 10 страны должны обеспечить, что финансовые учреждения проводили НПК, включая идентификацию и проверку личности своих клиентов при:

- (i) установлении деловых отношений;
- (ii) совершении разовых операций (сделок): (i) на сумму, превышающую установленное пороговое значение (15 000 долларов США/евро); или которые являются электронными переводами при обстоятельствах, подпадающих под действие положений Пояснительной записки к Рекомендации 16³⁴;
- (iii) наличии подозрений в отмывании денег или финансировании терроризма; или
- (iv) наличии у финансового учреждения сомнений в достоверности или достаточности полученных ранее данных о личности клиента.

³³ Ситуации, описанные как «низко рисковые» могут квалифицироваться как исключения в части применения ряда требования *Рекомендаций ФАТФ*, при этом упрощенный режим ПОД/ФТ имеет место, если уровень риска ниже.

³⁴ Рекомендации ФАТФ не определяют этот моменте. Решения о том установлены ли отношения или нет, принимают страны.

94. Важный вопрос для стран, который они должны разрешить, это участвуют ли НПМУ в установлении деловых отношений непосредственно. Обычно НПМУ функционируют как обычные счета, предусмотренные Рекомендацией 10. Открытие и ведение счетов от имени клиента предполагает установление деловых отношений, что в соответствии с положениями Рекомендацией 10 в свою очередь требует осуществления мер по НПК. В частности, предоплаченные карты многоэмитентной (открытой) системы все больше и больше используются как счета, так как их функционал возрастает. Онлайн-платежные сервисы также управляют средствами от имени клиента. При этом провайдеры мобильных платежей как предоплаченных, так и пост-оплаченных обычно устанавливают деловые отношения с клиентом, как предусмотрено Рекомендацией 10.

95. В соответствии с положениями Рекомендации 10 страны должны обеспечить, чтобы финансовые учреждения предпринимали следующие шаги для НПК: (i) идентификация клиента и подтверждение личности клиента, (ii) определение бенефициарного собственника, (iii) понимание целей деловых отношений (iv) проведение на постоянной основе надлежащего мониторинга деловых отношений. Страны должны требовать от финансовых учреждений применения каждой из мер по НПК, но им следует выбирать степень применения этих мер с помощью риск-ориентированного подхода. Также необходимо учитывать, что если НПМУ выступает в качестве счета, то в соответствии с требованиями Рекомендации 10 страны должны запретить финансовым учреждениям вести анонимные счета или счета, открытые на явно вымышленные имена. При реализации мер по ПОД/ФТ с учетом риск-ориентированного подхода страны могут разрешить применение упрощенных мер по НПК, если новый платежный продукт является низко рисковым.

96. Для НПК и НПМУ очень важен вопрос применения пороговых значений. Пороговые значения могут быть использованы в качестве эффективного фактора, снижающего риски, и как, следствие, может привести к реализации упрощенных мер по НПК. Пороговые значения могут варьироваться от страны к стране, в зависимости от того, какие риски несут НПМУ; такое пороговое значение должно определяться после проведения оценки рисков.

97. Если НПМУ были признаны низко рисковыми и к ним применяются низкие лимиты по использованию и пополнению, то страны все равно должны требовать от финансовых учреждений уделять достаточное внимание с тем, чтобы своевременно выявлять этапы смешения и структурирования преступных доходов, направленных на то, чтобы обойти пороговые значения и требования по направлению сообщений о подозрительных операциях. Например, страны могут рассмотреть возможность применения пороговых значений, чтобы помочь финансовым учреждениям осуществить первые три меры по НПК, полагаясь на информацию, полученную от клиента. В этом случае страну могут предусмотреть возможность применения, так называемого «прогрессивного» или «многоуровневого» подхода к KYS/НПК, при котором операция/платеж/остаток баланса на небольшую сумму сокращает риски ОД/ФТ. Чем жестче ограничения, используемые для определенной категории продуктов, тем очевиднее, что риски ОД/ФТ будут ниже и такой продукт/услуга могут считаться низко рисковыми. И в таком случае можно рассмотреть возможность применения упрощенных мер по НПК.

98. Кроме того, при наличии строго определенных и оправданных обстоятельств, подтверждающих, что риск ОД/ФТ сравнительно низок, страны могут рассмотреть возможность отказа от применения ряда мер по НПК в отношении некоторых НПМУ³⁵. При таких обстоятельствах наличие порогового значения может являться дополнительной мерой предосторожности.

³⁵ В параграфе 6 Пояснительной записки к Рекомендации 1 содержится следующее положение: «*Исъятия — страны могут решить не применять некоторые из Рекомендаций ФАТФ, устанавливающих требования для финансовых учреждений или УНФПП, при условии, что имеется доказанный низкий риск отмывания денег и финансирования терроризма, это происходит в строго ограниченных и оправданных обстоятельствах; и это относится к конкретному типу финансового учреждения или деятельности...*» Полный текст Пояснительной записки к Рекомендации 1 приведен на сайте www.fatf-gafi.org

99. Страны должны обеспечить, чтобы провайдеры НПМУ подпадали под требования о проведении НПК и мониторинга как части постоянной НПК с целью выявления подозрительной деятельности. В частности, провайдеры НПМУ, чей функционал похож на функционал счета, должны проводить постоянную НПК. Чем меньше схожесть prepaid карты и ее функционала со счетом, тем выше возможность применения упрощенных мер по НПК. Также в этой связи может помочь установление лимитов на пополнение.

100. Страны должны учитывать, что в соответствии с Рекомендациями ФАТФ они могут, в качестве исключения, позволить финансовым учреждениям при осуществлении деятельности без личного присутствия провести проверку личности клиента после установления деловых отношений (а не до или входе их установления), когда самое главное не нарушить обычное течение дел при условии, что управление рисками, связанными с отмытием денег, имеет место³⁶. Страны могут учесть это и примеры, приведенные в Пояснительной записке к Рекомендации 10³⁷, по проверке личности клиента после установления деловых отношений при определении того момента, когда необходимо проводить НПК.

101. Применение лимитов на пополнение и осуществление операций может снизить риски, возникающие в результате использования розничных магазинов (аутлетов) и Интернета для распространения prepaid карт и услуг мобильных платежей. Если НПК не проводится, то может возникнуть ситуация приобретения через Интернет множества prepaid карт одним и тем же лицом под разными именами. Страны должны предусмотреть меры для снижения рисков, связанных с приобретением большого количества НПМУ, таких как prepaid карты с лимитами для одной сделки или для множественных пунктов продаж. При этом в такой ситуации должно соблюдаться требование о направлении сообщений о подозрительных операциях. Кроме того, страны должны рассмотреть возможность установить лимиты в части количества карт, которые могут быть приобретены за раз, при этом ФАТФ осознает трудности, связанные с практической реализацией такого ограничения. Если prepaid карты и мобильные платежные услуги распространяются через розничные магазины, и при этом последние должны реализовывать меры по НПК, то неточная идентификация клиента представляет собой риск, если персонал такого розничного магазина не обучен должным образом. Если НПК реализуется при помощи электронной верификации, то провайдеры должны обеспечить, чтобы информация, на которую они полагаются, является точной и полученной из надежных источников.

102. Во многих случаях клиентом провайдера НПМУ является лицо, подписавшееся на услугу или приобретшее НПМУ. Учитывая ограниченный личный контакт с клиентами НПМУ или вообще его отсутствие, то существует высокий риск, что НПМУ будет передано, использовано третьими лицами, не идентифицированными провайдерами. Уровень риска может быть снижен путем применения риск-ориентированного подхода, то есть усиленных мер, а именно постоянная НПК и мониторинг операций. В качестве альтернативы страны могут определять другие точки применения НПК, например пункт пополнения.

103. Роль банков и других кредитных учреждений, предоставляющих счета провайдерам новых платежных методов и услуг (НПМУ), требует повышенного внимания стран. Согласно требованиям Рекомендации 10, страны должны обеспечить выполнение надлежащей проверки клиентов финансовых учреждений, держащих денежные средства по поручению провайдеров НПМУ, в отношении НПМУ пропорционально рискам, которые несет за собой провайдер НПМУ.

³⁶ Параграф 11 Пояснительной записки к Рекомендации 10 устанавливает, что примеры могут включать деятельность без личного присутствия и операции с ценными бумагами. Следует также отметить, что финансовые учреждения должны разработать процедуры управления рисками с учетом условий, согласно которым клиент может начать деловые отношения до верификации.

³⁷ См. Пояснительную записку к Рекомендации 10, параграф 21

С. ЛИЦЕНЗИРОВАНИЕ/РЕГИСТРАЦИЯ

104. Если НПМУ подпадает под определение НПМУ, предусмотренное Глоссарием к Рекомендациям ФАТФ, то такой провайдер должен получить лицензию или зарегистрироваться, в отношении него должен осуществляться надзор и он должен подпадать под меры по ПОД/ФТ. Рекомендация 14 предусматривает для стран две опции в части регистрации и лицензирования агентов³⁸. Страны также должны установить требование о лицензировании или регистрации агентов или возможен иной вариант, когда провайдер НПМУ ведет перечень своих агентов, который доступен компетентным органам.

105. Система услуг по переводу денежных средств и ценностей (УПДЦ) в Интернете должна соответствовать требованиям Рекомендации 14. В частности, так как проводящиеся в Интернете УПДЦ не имеют территориальных границ, очень важно, чтобы страны прояснили и в законе, и в руководящих документах критерии лицензирования и/или регистрации, применимые как для традиционных УПДЦ, так и для УПДЦ в Интернете, даже если поставщик услуг находится за рубежом. Данный вопрос детально разобран ниже.

Д. ЭЛЕКТРОННЫЕ ДЕНЕЖНЫЕ ПЕРЕВОДЫ

106. Рекомендация 16 устанавливает требования для стран в отношении электронных денежных переводов. Страны должны обеспечить, чтобы финансовые учреждения включали информацию, относящуюся к отправителю и получателю, в электронный денежный перевод и эта информация должна сопровождать перевод на всех его этапах, как предусмотрено положениями Пояснительной записки к Рекомендации 16³⁹. Кроме того, НПК должна проводиться в отношении клиентов, отправляющих и получающих электронный перевод. Однако стоит отметить, что страны могут установить минимальное пороговое значение для трансграничных электронных переводов. Если перевод осуществляется не меньшую сумму, то информация о проверке личности клиента, выгодоприобретателя не нужна, если только не имеется подозрение в совершении ОД/ФТ⁴⁰. При совершении разовых трансграничных электронных переводов на сумму, ниже 1000 долларов/евро также применяются требования, изложенные в Пояснительной записке к Рекомендации 16, то есть потребуются имя отправителя и получателя, а также номер счета каждого или уникальный номер ссылки на операцию, однако такая информация не проверяется.

107. Рекомендация 16 применяется к трансграничным и внутренним электронным переводам⁴¹ и страны должны определить, распространяются ли данные требования на НПМУ. Преоплаченные карты, предназначенные в большинстве своем для переводов от лица к лицу, имеют функционал, схожий с электронными переводами и, таким образом, на них должны распространяться положения Рекомендации 16. Рекомендация 16 не охватывает переводы с преоплаченных карт на покупку товаров и услуг. Однако под положения Рекомендации 16 подпадают операции с преоплаченными картами, когда последние используются в качестве платежной системы для

³⁸ В соответствии с параграфом 22 Пояснительной записки к Рекомендации 16 предусматривает, что «провайдеры услуг перевода денег и ценностей (НПМУ) должны соблюдать все соответствующие требования Рекомендации 16 в странах, в которых они действуют, прямо или через своих агентов. В случае провайдера НПМУ, который контролирует как отправляющую, так и получающую стороны электронного перевода, провайдер НПМУ: (а) должен принять во внимание всю информацию как от отправляющей стороны, так и от получающей стороны, чтобы решить, нужно ли направлять СПО и (б) должен направить СПО в любой стране, затронутой подозрительным электронным переводом, и предоставить соответствующую информацию об электронном переводе в подразделение финансовой разведки.

³⁹ Для того, чтобы обеспечить наличие информации об отправителе при международном переводе, надзорные органы должны предусмотреть, что финансовые учреждения используют фильтры, которые специально предназначены для международных переводов, (а не внутренние фильтры для внутренних переводов)

⁴⁰ См. Пояснительную записку к Рекомендации 16, параграф 5.

⁴¹ См. Пояснительную записку к Рекомендации 16, параграф 3.

электронного перевода средств между лицами⁴². Страны должны обеспечить, чтобы учреждения, выпускающие prepaid карты, используемые для осуществления перевода от лица к лицу, получали и хранили точную информацию об отправителе; также должна быть представлена информация о получателе в соответствии с требованиями Рекомендации 16. Кроме того, под требования Рекомендации 16 подпадают мобильные и онлайн-платежные системы, которые также являются поставщиками услуг по УПДЦ⁴³.

Е. ПОДХОД НАДЗОРНЫХ ОРГАНОВ И ОПРЕДЕЛЕНИЕ КОМПЕТЕНЦИИ

108. Страны должны обеспечить, чтобы в отношении провайдеров НПМУ осуществлялось регулирование и надзор в соответствии с требованиями Рекомендации 26. Надзорные органы должны применять риск-ориентированный подход, где в качестве минимально меры установлено, что провайдеры НПМУ, являющиеся провайдерами УПДЦ должны быть зарегистрированы или получить лицензию и стать субъектами системы эффективного мониторинга⁴⁴.

109. Что касается НПМУ, распространяемых через агентов, то страны должны обеспечить, что учреждение, полагающееся на агента в части реализации мер по ПОД/ФТ, должно включить последних таких агентов (всех без исключения) в свои программы по ПОД/ФТ, а также проверять их на предмет соответствия. Страны должны обеспечить, чтобы их правовая система работала таким образом, чтобы провайдеры НПМУ подпадали под требования о ПОД/ФТ и несли ответственность за действия своих агентов.

110. При создании надзорной системы страны должны четко определить надзорный орган, ответственный за надзор за НПМУ в части ПОД/ФТ. Кроме того, надзорные органы должны обладать соответствующими полномочиями на осуществления надзора или мониторинга и обеспечить соответствие провайдеров НПМУ требованиям в сфере ПОД/ФТ, предусмотренным Рекомендацией 27. Страны должны предусмотреть наличие публичного органа, который лучше всего расположен в системе органов и будет наиболее эффективно осуществлять свои полномочия в части регулирования деятельности провайдеров НПМУ и надзора за ними, учитывая, что для участников сектора нужны единые правила игры и последовательный подход в части надзора за учреждениями, предлагающими схожие услуги, не смотря на секторальные различия, которые могут быть у таких учреждений (например, банки, телекоммуникационные компании). Ситуация с компетентным органом может быть ясна, например, когда в стране существует единый надзорный орган в сфере ПОД/ФТ. С другой стороны, а именно когда в стране существует ряд различных органов, осуществляющих надзор за соблюдением требований по ПОД/ФТ для разных провайдеров НПМУ, то должен существовать эффективный механизм сотрудничества между ними.

111. Что касается мобильных платежных услуг (это особенно важно для модели, где центром является ОСС), то за ними обычно государственными органами, ответственными за соблюдение

⁴² В параграфе 4 Пояснительной записке к Рекомендации 16 предусмотрено следующее: «Рекомендация 16 не нацелена на охват следующих типов платежей:(а) любой перевод, который связан с операцией (сделкой) с использованием кредитной, дебетовой или prepaid карты для покупки товаров или оплаты услуг, если номер кредитной, дебетовой или prepaid карты сопровождает все переводы, связанные с этой операцией (сделкой). Однако, когда кредитные, дебетовые или prepaid карты используются в качестве платежной системы для осуществления электронных переводов между людьми, эта операция (сделка) охватывается Рекомендацией 16, и необходимая информация должна быть включена в сообщение.». Полный текст Пояснительной записки к Рекомендации 16 доступен на сайте www.fatf-gafi.org

⁴³ Параграф 22 Пояснительной записке к Рекомендации 10 «Провайдеры услуг перевода денег и ценностей (УПДЦ) должны быть обязаны соблюдать все соответствующие требования Рекомендации 16 в странах, в которых они действуют, прямо или через своих агентов. Полный текст Пояснительной записки к Рекомендации 16 доступен на сайте www.fatf-gafi.org

⁴⁴ См. Рекомендацию 14

обязательств по ПОД/ФТ надзор не осуществляется. Страны, например, могут рассмотреть возможность надления органа в сфере телекоммуникаций надзорными полномочиями в сфере ПОД/ФТ, особенно если количество мобильных платежных услуг, предлагаемых ОСС, велико. Однако, если компетентный орган в сфере телекоммуникаций понимает ситуацию, складывающуюся в секторе мобильных услуг, и уже осуществляет надзор за ОСС, то опыта, которым обладают органы, осуществляющие надзор в сфере ПОД/ФТ, может и не доставать. Если же государств все-таки примет решение о надления органа в сфере телекоммуникаций надзорными полномочиями, то последние должны пройти обучение для наработки соответствующего опыта. Кроме того, особую роль играет сотрудничество между финансовыми и органами, надзорными в сфере ПОД/ФТ с тем, чтобы обеспечить последовательный подход в отношении финансовых услуг. И наоборот орган, надзорный в сфере ПОД/ФТ, может осуществлять надзор за провайдерами в сфере мобильных платежей, так как у него есть существенный опыт в сфере ПОД/ФТ. Власти должны принимать решение о надзорном органе в сфере мобильных платежей в сфере ПОД/ФТ, учитывая обстоятельства и существующую структуру надзора и опыт каждой страны.

112. Онлайнновые платежные услуги несут с собой трудности для государств в части их регулирования в сфере ПОД/ФТ, поскольку в силу своего транснационального характера, поставщики могут находиться в иной стране, нежели клиенты. Платежи могут быть отправлен из любой точки земного шара посредством Интернета; правоохранительным и надзорным органам трудно установить, где находится провайдер и осуществляет ли свою деятельность в данном государстве. Это вызывает особую озабоченность, так как провайдеры могут находиться в стране, которая в недостаточной мере регулирует этот сектор и не осуществляет надзор за ним. Страны должны обеспечить, чтобы провайдеры, которые предлагают онлайнновые платежные услуги подпадали внутри страны под регулирование в сфере ПОД/ФТ и надзор, независимо от того, где территориально находится провайдер. В соответствии с положениями Рекомендации 14 странам следует предпринять меры для обеспечения того, чтобы физические или юридические лица, предоставляющие услугу перевода денег или ценностей (УПДЦ), имели лицензию или были зарегистрированы, и они должны принимать меры по выявлению физических и юридических лиц, которые осуществляют услуги по УПДЦ без такой лицензии и регистрации.

С тем, чтобы определить какие услуги предлагаются в конкретной стране, а последние должны учитывать какой язык используется, получать описание услуг с официальных сайтов, которые в некоторых покупках могут помочь установить ту категорию клиентов, на которую нацелены провайдеры услуг. Чтобы помочь в осуществлении надзорных полномочий за представленными в их юрисдикции продуктами страны должны рассмотреть возможность, соответствующую их правовой системе⁴⁵, запрещая онлайнновым платежным системам распространять рекламу своих услуг, где они физические не присутствуют. Для этого можно использовать местное представительство или агентство.

VII. НАДЛЕЖАЩЕЕ РЕГУЛИРОВАНИЕ В СФЕРЕ ПОД/ФТ, КОТОРОЕ ПОЗВОЛЯЕТ СНИЖАТЬ РИСКИ

113. Настоящий раздел представляет собой Руководство странам об определении того учреждения, которое и будет нести обязательства в сфере ПОД/ФТ, особенно в части предоплаченных карт, мобильных и онлайнновых платежных систем.

A. УРОВЕНЬ МЕР ПО ПОД/ФТ, КОТОРЫЙ БЫ СООТВЕТСТВОВАЛ УРОВНЮ РИСКА.

114. Объем применяемых мер в сфере ПОД/ФТ должен соответствовать рискам, которые несут НПМУ. Например, если функционал НПМУ близок к функционалу банковского счета, то должно применяться аналогичное регулирование, включая применение всех мер по НПК. В частности,

⁴⁵ Примеры правовых баз см. в Приложении 1 (Раздел онлайнновых платежных услуг)

если функционал НПМУ становится похожим на постоянные отношения депозитарного характера, то должны применяться соответствующие обязательства в сфере ПОД/ФТ⁴⁶.

115. Что делает функционал НПМУ похожим на функционал банковского счета так это наличие одного или нескольких нижеперечисленных факторов:

- (a) НПМУ может быть пополнено бесчисленное количество раз;
- (b) предусмотрено отсутствие или очень жесткие лимиты в части пополнения и расходования;
- (c) есть возможность осуществлять трансграничные переводы и внутри той страны, где продукт был выпущен;
- (d) НПМУ могут быть пополнены наличными денежными средствами, которые затем можно снять через банкомат;
- (e) возможность вносить средства на счет при помощи наличных или их эквивалента напрямую или через иных поставщиков или посредников.

116. Эти факторы должны учитываться при применении риск-ориентированного подхода в части регулирования сферы ПОД/ФТ. Подходы, используемые национальными регуляторами в отношении НПМУ отличаются, некоторые конкретные примеры приведены в Приложении 1. Страны могут счесть эти примеры полезными при выборе режима ПОД/ФТ для НПМУ, однако это ответственность страны обеспечить, чтобы режим по ПОД/ФТ соответствовал Рекомендациям ФАТФ, учитывая при этом обстоятельства и профиль рисков.

В. ФАКТОРЫ, КОТОРЫЕ НУЖНО УЧИТЫВАТЬ, ПРИ ПРИМЕНЕНИИ МЕР ПО ПОД/ФТ В ОТНОШЕНИИ ПРОВАЙДЕРОВ НПМУ

117. Учитывая круг учреждений, которые могут быть вовлечены в предоставление НПМУ, страны должны обеспечить, чтобы их правовые системы содержали прямое указание на то, кто является ответственным за контроль и надзор за соответствующими учреждениями, подпадающими под требования о ПОД/ФТ (здесь и далее именуемые «провайдеры НПМУ»). Кроме того, страны также должны обеспечить, чтобы в отношении таких провайдеров НПМУ осуществлялись регулирование и надзор в соответствии с положениями Рекомендации 26. Кроме того, провайдеры НПМУ, которые охватываются определением УПДЦ, должны быть зарегистрированными или получить лицензию. Также, в отношении них должна осуществляться эффективная система мониторинга, как того требует Рекомендация 14⁴⁷.

118. Как уже отмечалось выше в соответствии с Рекомендациями ФАТФ учреждения – провайдеры УПДЦ, которые являются НПМУ или средством платежа должны подпадать под

⁴⁶ Следует отметить, что пропорциональный подход был одобрен частным сектором в *Руководстве Вольфсбергской Группы «О предоплаченных картах и картах с заложенным лимитом средств»*, которое было выпущено в октябре 2011 г. В нем говорится, что чем ближе по своему характеру предоплаченная карта к банковскому счету (например, может быть пополнена, не обременена ограничениями в части внесения или снятия и позволяет осуществлять переводы денежных средств), то должно применяться соразмерное регулирование.

⁴⁷ Глоссарий к *Рекомендациям ФАТФ* гласит, что «УПДЦ относятся к финансовым услугам, которые предусматривают прием наличных денег, чеков, других денежных инструментов или других средств сбережения, а также выплату соответствующей суммы наличными или в другой форме получателю посредством коммуникации, послания, перевода или через клиринговую сеть, к которой принадлежит этот провайдер УПДЦ. В сделках, совершенных с помощью таких услуг, могут участвовать один или более посредников, и окончательный платеж может производиться третьей стороной с возможным использованием новых методов платежей. Иногда эти услуги имеют связь с конкретными географическими регионами и поэтому описываются рядом специальных терминов, в том числе хавала, хунди и фэй-тсиен».

обязательства о ПОД/ФТ. Если в предоставлении услуги или продукта вовлечены несколько учреждений и остается неясным, кто из всей этой группы лиц является поставщиком, то страны должны учесть следующие факторы для определения «своего» провайдера(ов) НПМУ:

- (a) учреждение, которое реально существует (дословно «видимы») и осуществляют управление НПМУ;
- (b) учреждение, которое поддерживает отношения с клиентом;
- (c) учреждение, которое принимает средства от клиента; и
- (d) учреждение, в отношении которого у клиента есть право требовать эти средства.

119. В зависимости от бизнес-модели (особенно в случае сильной сегментации услуг) также может быть не одно учреждение, ответственное за предоставление НПМУ, и, как следствия, субъектов, на которые распространяются требования по ПОД/ФТ. Ниже приведено руководство для prepaid карт мобильных и онлайн-платежных систем. В частности, это руководство основано на операциях и роли учреждений, участвующих в предоставлении НПМУ, указанных в Разделе I.

i. Провайдеры prepaid карт

120. В некоторых моделях программа prepaid карт эффективно работает под руководством программного менеджера, который оказывает платежные услуги в соответствии с положениями контракта, заключенного с эмитентом. Эмитент в свою очередь несет ответственность за средства клиента. Если отношения с клиентом поддерживаются, то менеджер программ по prepaid картам должен быть субъектом регулирования в сфере ПОД/ФТ, так как является учреждением, которое управляет процессом предоставления prepaid карт или косвенно подпадает под регулирование в сфере ПОД/ФТ, как агент эмитента. В других случаях эмитент карточки может выступать в роли программного менеджера и поддерживать отношения с клиентами, а также отслеживать использование этих карточек. В других случаях эмитент подпадает под регулирование в сфере ПОД/ФТ.

121. На практике поставщики платежных карт обычно используют своих дистрибьюторов и агентов для осуществления соответствующих мер по ПОД/ФТ. В таких обстоятельствах поставщик prepaid карт несет ответственность за соблюдением всех мер по ПОД/ФТ. При таком раскладе дистрибьютор prepaid карт осуществляет деятельность от имени провайдера НПМУ и будет считаться агентом поставщика prepaid карт, независимо от того, предусматривает ли prepaid карта УПДЦ. В этом случае поставщик prepaid карт несет ответственность за несоблюдение требований по ПОД/ФТ своими дистрибьюторами и агентами.

122. В некоторых случаях страны могут принять решение о наложении требования по ПОД/ФТ не только на провайдера НПМУ, но и на агента и дистрибьютора. В соответствии с этим подходом дистрибьюторы и агенты несут ответственность и в отношении них должен осуществляться надзор соответствующим надзорным органом. Этот подход может быть выигрышным в ситуациях, когда договорные отношения отсутствуют между дистрибьютором и провайдером НПМУ, или если учреждение находится на территории иного государства, что создает трудности с точки зрения эффективности надзора. Такая ситуация возможна, когда эмитент использует оптовых дистрибьюторов, а те в свою очередь – дистрибьюторов помельче и агентов.

ii. Провайдеры мобильных платежных услуг

123. Провайдеры мобильных платежных услуг подпадают под определение «финансового учреждения» и как УПДЦ и как учреждение, выпускающее средства платежа и управляющее ими в

зависимости от характера услуги. Мобильные платежные системы, позволяющие осуществлять переводы от лица к лицу, являются УПДЦ. Страны должны обеспечить, чтобы и они были охвачены мерами по ПОД/ФТ, включая и требования относительно регистрации и лицензирования в соответствии с положениями Рекомендации 14.

124. С другой стороны мобильные платежные системы, позволяющие осуществлять переводы от физического лица юридическому лицу, подпадают под *Рекомендации ФАТФ*, как провайдеры, которые осуществили выпуск платежных средств и управляют ими. Меры по ПОД/ФТ должны распространяться на таких провайдеров. Однако, если выполняются требования о лицензировании или регистрации, то положения Рекомендации 14 не применяются.

125. Выбор учреждения, которое будет нести ответственность за неисполнение обязательств по ПОД/ФТ, будет зависеть от модели и структуры мобильной платежной системы. *Если используется модель, где центральная роль отведена банку*, то банк управляет средствами и отношениями с клиентом и отвечает за применение мер по НПК.

126. Если *центральное место занимает ОСС*, то ОСС или его дочерние организации считаются финансовыми учреждениями в соответствии с *Рекомендациями ФАТФ*. Если используется эта модель, то ОСС и его дочерние организации оказывают услуги, поддерживают отношения с клиентом, хранят средства клиентов, а клиент может выступить с правом требования средств.

127. Как и в случае с prepaid картами, провайдер мобильных платежных услуг может использовать обширную сеть дистрибьюторов в качестве агентов, у которого прямой контакт с клиентом в момент продажи и который должен принимать меры по ПОД/ФТ, (например, НПК) от имени провайдера, например, в случае внесения prepaid средств на prepaid счет или эмиссии мобильных денежных средств. При таком развитии событий дистрибьюторы осуществляют деятельность от имени провайдера мобильных платежных услуг и будет, таким образом, считаться агентом, независимо от того, является ли провайдер УПДЦ.

iii. Провайдеры онлайнных платежных систем.

128. Провайдеры онлайнных платежных систем подпадают под определение «*финансового учреждения*» и как УПДЦ, и как учреждение, выпускающее средства платежа и управляющее ими в зависимости от характера услуги. Онлайнные платежные системы, позволяющие осуществлять переводы от лица к лицу, являются УПДЦ. Страны должны обеспечить, чтобы и они были охвачены мерами по ПОД/ФТ, включая и требования относительно регистрации и лицензирования в соответствии с положениями Рекомендации 14.

129. Однако, некоторые онлайнные платежные системы, которые выпускают электронные деньги, как средство платежа за товары и услуги и не осуществляют переводы от физического лица физическому лицу, подпадают под *Рекомендации ФАТФ*, так как они выпускают средство платежа и управляют им. Меры по ПОД/ФТ должны распространяться на таких провайдеров. Однако, если выполняются требования о лицензировании или регистрации, то положения Рекомендации 14 не применяются.

130. Провайдер онлайнных платежных систем – это учреждение, которое принимает средства, валюты и иные ценности от клиента и:

(a) переводит, организует перевод средств, валюты и иных ценностей в иные места, используя Интернет для передачи платежного сообщения, или

(b) выпускает электронные валюты, которые могут быть использованы для переводов и платежей.

131. Не смотря на то, что для онлайн-платежных систем обычно существует много моделей, то учреждение, которое оказывает услуги, также взаимодействует с клиентами. В таком случае у клиента есть право требовать средства у провайдера. Страны должны обеспечить, чтобы такие учреждения несли ответственность за неисполнение обязательств в сфере ПОД/ФТ и подлежали надзору.

ПРИЛОЖЕНИЕ 1 – НОРМАТИВНО-ПРАВОВЫЕ ПОДХОДЫ К НПК

Это приложение содержит примеры подходов регуляторов, которые применяют государства-члены ФАТФ в отношении НПК. Эти подходы не оценивались на соответствие *Рекомендациям ФАТФ*, принятым в феврале 2012 г. и их включение в настоящее Руководство не означает соответствие *Рекомендациям ФАТФ*. Их описание не означает одобрение ФАТФ. Страны могут посчитать эти примеры полезными при рассмотрении подходов по ПОД/ФТ в отношении НПК. Однако на странах лежит ответственность по обеспечению того, чтобы национальные режимы ПОД/ФТ полностью соответствовали Рекомендациям ФАТФ с учетом их собственного профиля риска.

ПРЕДОПЛАЧЕННЫЕ КАРТЫ

Аргентина

В 2011 г. Аргентина выработала меры и процедуры в сфере ПОД/ФТ для эмитентов prepaid карт (пополняемых и не пополняемых). Это регулирование в Аргентине устанавливает меры по НПК, которые компании должны реализовывать в отношении клиентов. Среди других обязательств, по которым компании отчитываются в ПФР ежемесячно, появилось обязательство сообщать о выпуске непополняемых карт на сумму выше 4000 аргентинских песо (приблизительно 700 евро).

Европейский Союз

Европейский опыт особенно интересен в отношении prepaid карт, которые подпадают под более широкое определение электронных денег, поскольку законодательная база, которая рассматривала изначально электронные деньги близко к депозиту, стала более понятной. Это было достигнуто за счет введения упрощенного режима по НПК для электронных денег, предусмотренного третьей антиотмывочной директивой в 2005 г., а также пересмотра пруденциального режима, применяемого к учреждениями, которые могут выпускать электронные деньги, которые значительно облегчили пруденциальные требования, но не сняли основные требования по ПОД/ФТ. Как показывают данные Европейского Центрального банка комбинация этих двух регуляторных нововведений, направленных на стимулирование развития сектора электронных денег на европейском рынке, привела к значительному прогрессу. В Еврозоне количество операций, осуществляемых при помощи электронных денег, увеличилось с 386 миллиардов в 2006 г. до 1024,56 миллиардов в 2010 г.⁴⁸ Однако, необходимо отметить, prepaid карты одноэмитентной (закрытой) системы (когда их прием ограничен эмитентом, например, в случае подарочных карт отдельного брэнда) не подпадают под определение электронных денег, предусмотренного Европейской Директивой. Prepaid карты одноэмитентной (закрытой) системы до сих пор составляют большую часть prepaid карт.

Хотелось бы отметить, что введение при помощи антиотмывочной Директивы возможности для государства-члена ЕС применять упрощенные меры по НПК для электронных денег произошло только после консультаций с операторами рынка, которые заявили, что применение полного объема мер по НПК к электронным деньгам является непропорциональным и это одна из причин медленного роста рынка электронных денег. Помимо требований рынка возникла и правовая необходимость для сифта и дешевых

⁴⁸ См. Европейский Центральный банк (пс)

платежных инструментов, чтобы обеспечить доступ к платежным услугам людей, у которых нет возможности или которые не заинтересованы в открытии банковского счета для получения доступа к платежной системе (например, несовершеннолетние и мигранты). В 2004 г. также возрос интерес и обязательства правительств в целом по улучшению качества и снижению стоимости денежных переводов. Продукты, связанные с электронными деньгами, включая prepaid карты, имеют потенциал для этого. Европейский регулятор учел требования операторов и позволил каждому отдельному государству-члену ЕС применять упрощенные меры по НПК для электронных денег при соблюдении следующих пороговых значений: если устройство не может быть пополнено и максимальная сумма не превышает 150 евро или если устройство может быть пополнено, но максимальный годовой лимит операций не превышает 2500 евро. Вторая Директива, посвященная электронным деньгам и выпущенная в 2009 г., увеличила пороговое значение до 250 евро для устройств, которые не могут быть пополнены.

Примечание: ФАТФ сообщат, что в настоящее время идет разработка 4 антиотмывочной Директивы Евросоюза и просит читателей отслеживать все этапы разработки и реализации этой Директивы.

Германия

Следует отметить, что некоторые государства-члены Евросоюза не используют возможности, предусмотренные третьей антиотмывочной Директивой ЕС, в части применения упрощенных мер по НПК, но вместо этого они разрабатывают свои более жесткие режимы для упрощенной надлежащей проверки, связанной с электронными деньгами. Например, в Германии в декабре 2011 г. появилось новое законодательство, которое позволяет не проводить НПК в отношении prepaid карт, если соблюдены следующие условия:

1. Продукт содержит пороговое значение – не более 100 евро (что значительно ниже, чем в Директиве ЕС);
2. Продукт не позволяет клиенту осуществлять операции от лица к лицу;
3. Продукт не может быть пополнен иными электронно-денежными продуктами и не может быть использован для пополнения иных продуктов, связанных с электронными деньгами; и
4. Продукт не позволяет снять наличными более 20 евро.

Prepaid карты, которые не отвечают этим условиям, также могут подпадать под упрощенные меры по НПК или даже освобождены от применения мер по НПК. Однако это требует официального обращения в компетентный орган, который оценит уровень риска, соответствующий prepaid продукту, и определит какие меры по НПК должны применяться. Такая оценка риска основана не только на пороговом значении, но принимает в расчет все соответствующие факторы риска. С другой стороны, если компетентный орган принимает решение, что prepaid карта несет высокие риски ОД/ФТ, то он может выпустить предписание и предпринять дополнительные меры в отношении эмитентов и дистрибьютеров, включая запрет продукта. Это также применяется к prepaid картам, выпущенным за границей.

Южная Африка

В Южной Африке карточные ассоциации выпускают зарплатные prepaid карты для некоторых своих рабочих для перечисления на них зарплаты. Prepaid карты могут

быть использованы для снятия наличных в банкомате и оплате товаров в торговых точках. На такие предоплаченные карты ни владелец карты, ни третьи лица не могут вносить денежные средства. Кроме того, никакие дебетовые поручения не могут быть выданы в отношении таких карт или баланса работодателя на счете в банке. Работодатель может подать заявку на участие в зарплатном проекте. После одобрения работодатель подпадает под требования Закона «О Центре финансовой разведки» (FICA) в части реализации мер по НПК и ведению учета личности и адреса проживания каждого держателя карты. Затем открывается внутренний банковский счет для работодателя, который используется для расчетов и в любое время отражает среднее кредитовое сальдо по предоплаченным картам. Перед днем зарплаты работодатель переводит общую сумму заработной платы на банковский счет для предоплаченных карт и уведомляет /инструктирует банк о тех предоплаченных картах, на которые необходимо перевести средства.

Индия

Предоплаченные платежные инструменты (PPIs), выпускаемые банками и небанковскими учреждениями набирают популярность как средство платежа в Индии. Предоплаченные платежные инструменты, которые могут быть выпущены внутри страны, подразделяются на три категории: (i) замкнутая система платежных инструментов, (ii) полузамкнутая система платежных инструментов, (iii) открытая система платежных инструментов. И банки и небанковские учреждения могут выпускать PPIs, однако, только банки могут выпускать открытые PPIs, то есть те, которые позволяют снимать наличные денежные средства в банкомате.

Предложение по выпуску PPI банком одобряется после получения соответствующих документов от RBI. Все остальные лица, которые хотят войти в платежную систему, связанную с выпуском PPIs, должны получить разрешение Резервного банка Индии (RBI) в соответствии с Законом «О платежно-расчетной системе» 2007 г. Все остальные лица должны иметь оплаченный капитал в размере 10 миллионов индийских рупий (приблизительно 1.8 миллионов долларов США), а также положительный баланс собственных денежных средств.

Максимальный порог для любых PPIs составляет 50 000 индийских рупий (приблизительно 900 долларов США). Допустимые PPIs могут быть пополнены при помощи наличных денежных средств и/или путем дебетования банковского счета или кредитной карты в филиале банка/ а также через банкоматы/уполномоченные магазины/через банковских и небанковских агентов. Надлежащая проверка агентов, уполномоченных на продажу/пополнение PPIs, является обязательным условием.

Банки, которым RBI разрешил использовать мобильный банкинг для проведения операций, вправе запускать любые мобильные PPIs (мобильные счета и мобильные кошельки). Другим лицам разрешено выпускать полузамкнутые PPIs с лимитом в 5000 индийских рупий (приблизительно 90 долларов США) и без возможности переводов ценностей от лица к лицу.

Банкам также разрешено выпускать PPIs для кредитования трансграничных входящих переводов в соответствии со Схемой по предоставлению услуг по переводу денег (MTSS) RBI, при этом банки подпадают по требованию «знай своего клиента», а также иные требования. Использование PPIs для трансграничных переводов также подпадает под требования законодательства о валютном регулировании. Риск-ориентированный подход применяется для требования «Знай своего клиента» для PPIs в той степени как варьируется надлежащая проверка клиентов в зависимости от денежных лимитов и характера инструмента. Могут быть выпущены следующие три вида полузамкнутых PPIs:

1. Полузамкнутая система prepaid платежных инструментов, которая может быть выпущена на сумму до 10000 индийских рупий при предоставлении незначительного количества деталей при условии, что сумма остатка неисполненных обязательств в любое время не превышает 10000 индийских рупий и общая сумма пополнений в течение месяца не превышает 10000 индийских рупий. Выпускается только в электронной форме;

2. Полузамкнутая система prepaid платежных инструментов, которая может быть выпущена на сумму от 10001 до 50000 индийских рупий при получении «официального действительного документа», как это определено в Правиле 2(d) Закона «О противодействии отмыванию денег». Такие PPIs могут быть выпущены в электронной форме и по своей природе не являются пополняемыми;

3. Полузамкнутые системы prepaid платежных инструментов могут быть выпущены на сумму до 50000 индийских рупий при проведении всех мер KYC и могут пополняться.

Перевод средств на карты, выпущенные тем же эмитентом, или на банковский счет допускается для всех трех категорий карт. Небанковские учреждения могут выпускать мобильные полузамкнутые PPIs, в отношении которых действует лимит 50000 индийских рупий (приблизительно 900 долларов США). Такие карты могут выпускаться только для операций внутри страны.

Субъекты, выпускающие PPIs, согласно Акту о Предупреждении отмывания денег от 2002 г., подлежат учету и требованию об обязательном предоставлении отчетности.

МОБИЛЬНЫЕ ПЛАТЕЖИ

Европейский Союз

Любое из государств-членов Европейского Союза может применять упрощенные меры по НПК сервисов, связанных с электронными деньгами, в отношении которых осуществляется регулирование, при соблюдении пороговых значений: 250 евро, если отсутствует пополнение и 2500 евро ежегодный оборот, если предусмотрено пополнение. Настоящие положения применяются к мобильным платежам, когда средства prepaid (в этом случае они считаются электронными деньгами), а не когда средства уплачиваются после совершения операции.

«Прямой расчет» исключен из платежных услуг, если купленный продукт или услуга подпадает под соответствующее исключение, предусмотренное Директивой о платежных услугах и Второй Директивой об электронных деньгах. Одним из исключения является то, что продукт или услуга приобретается посредством мобильного телефона и поставляется/используется через телекоммуникационные средства, цифровые и IT устройства (например, мелодии мобильного звонка, музыка и новостные рассылки) при условии, что ОСС не действует в качестве посредника между клиентом и поставщиком продукта или услуги.

Соединенные Штаты Америки

Модель регулирования вопросов ПОД/ФТ в отношении электронных денег, используемая в США, интерпретирует все новые платежные технологии, не делая различия между платежами, совершенными при помощи prepaid карт, мобильного телефона или

Интернета⁴⁹. США требует, чтобы все поставщики по УПДЦ были зарегистрированы в США или получили там лицензию, если поставщик УПДЦ предлагает услуги на территории США.

Индия

Индийская модель, где ведущая роль отведена банкам, построена таким образом, чтобы обеспечить доступ клиент к различным банковским услугам, а не только к услугам перевода. Только банки, которые получили лицензию и в отношении которых, осуществляется надзор со стороны Резервного Банка Индии (RBI) и имеющие физическое присутствие на территории Индии, могут предлагать мобильные банковские услуги. Услуги оказываются только клиентам банка или держателям дебетовых/кредитных карт. Клиенты должны подключаться к мобильному банкингу только в своем банке. Банки используют систему регистрации на основании полученных документов при обязательном личном присутствии клиента, до того, как начнут оказывать услуги мобильного банкинга.

Система быстрых платежей (IMPS) разработана и управляется Национальной платежной корпорацией Индии (NCPI) и позволяет осуществлять переводы денежных средств в режиме реального времени при помощи мобильных телефонов между счетами различных банков. Оказываются только услуги внутри страны, где платежным средством является индийская рупия. Не допускается использование мобильных услуг для входящих/исходящих трансграничных переводов.

Банки могут также воспользоваться услугами системы корреспондентских отношений: то есть физические и юридические лица, которые как бы расширяют банковское присутствие для своих клиентов. Руководства, выпущенные Резервным Банком о принципе «Знай своего клиента» (ЗСК), «Противодействии отмыванию денег (ПОД), «Противодействии финансированию терроризма» (ПФТ) в некоторой части также применимы к банковским услугам, оказываемым при помощи мобильного телефона.

Банкам разрешено предлагать услуги мобильного банкинга своим клиентам без ежедневного лимита по транзакциям, связанным с покупкой товаров/услуг. В случае перевода денежных средств, который ведет к получению наличных – максимальный лимит, составляющий 10 000 рупий (приблизительно 185 долларов США) применяется и к мобильному банкингу. Банк может предусмотреть приемлемый лимит для быстрого оборота таких транзакций, при условии соблюдения следующих пороговых значений – 25 000 рупий (приблизительно 460 долларов США) в месяц для каждого клиента. Банки должны провести надлежащую проверку лиц до того, назначить их уполномоченными агентами для оказания таких услуг. Банки должны исполнять требование о соблюдении безопасности и конфиденциальности счетов клиентов.

ОНЛАЙН ПЛАТЕЖИ

Аргентина

Новое регулирование системы электронных платежей (MEP) предусматривает необходимость идентифицировать получателя и плательщика (при помощи налогового/рабочего идентификационного номера и счета CBU). Было включено

⁴⁹ Американское регулирование относит поставщиков электронных денег к поставщикам и продавцам предоплаченного доступа

дополнительное поле с тем, чтобы понять, является ли плательщик ПДЛ. Это установит контроль за переводом средств, учитывая его в качестве фактора риска. МЕР – это система электронных платежей, которой управляет BCRA, которая обычно используется для операции, суммы которых значительно выше. В некотором смысле, финансовые учреждения, которые предлагают услуги по оплате в Интернете, должны идентифицировать получателя и плательщика, а также установить не является ли последний ПДЛ.

Европейский Союз

В Европе поставщики услуг по оплате в Интернете подпадают под действие Директивы «Об электронных деньгах» 2009/110/ЕС, если они эмитируют электронные деньги («эмитент электронных денег»), и под действие Директивы о платежных услугах (2007/64/ЕС), если они оказывают платежные услуги без выпуска электронных денег (платежное учреждение). Все уполномоченные поставщики услуг по платежам в Интернете подпадают под все меры по ПОД/ФТ. В случае предоплаченных Интернет счетов, денежные средства, размещенные на них, считаются электронными деньгами и могут применяться упрощенные меры по НПК при соблюдении следующих условий (i) максимальный лимит не превышает 250 евро для счетов, которые не могут быть пополнены или (ii) годовой оборот не выше, чем 2500 евро, в случае счетов, которые могут быть пополнены. Поставщики платежных услуг в Интернете действуют исходя из положений Директивы о платежных услугах (2007/64/ЕС), которые позволяют предлагать услуги на территории всего Европейского Союза на основании разрешения, выданного в одном государстве-члене. Директива содержит требование о наличии публичного реестра уполномоченных платежных учреждений, их агентов и филиалов, который должен вестись государством – членом, где создан провайдер услуг. Также Директива требует, чтобы государства – члены сотрудничали в надзорных целях и осуществляли информационный обмен с органами других государств-членов, занимающихся вопросами регулирования надзора.

Что касается платежных услуг, предлагаемых в Интернете, то Директива об электронной коммерции (Директива 2000/31/ЕС) создала основу для внутреннего рынка электронной коммерции, который обеспечивает правовую определенность для предпринимателей и потребителей. Это позволяет провайдерам так называемых «услуг информационного общества» (которые включают в себя и финансовые услуги, предлагаемые в Интернете) оказывать услуги на территории всего Союза на основании законодательства, преваляющего в государстве-члене, в котором они учреждены, без необходимости физического присутствия в иной стране Европейского Союза и не позволяют получающему/принимающему государству-члену налагать лицензионные или регистрационные обязательства на компании, учрежденные в другом государстве-члене и оказывающие услуги по трансграничным переводам.

Соединенные Штаты Америки

США требует, чтобы все поставщики по УПДЦ, вне зависимости от того, где они находятся в мире, должны быть зарегистрированы в США или получили там лицензию, если поставщик УПДЦ предлагает услуги на территории США. Это требование имеет определенное отношение к провайдерам УПДЦ при помощи сети Интернет, физическое место нахождения которых тяжело установить.

Индия

Только банки, которые получили лицензию, и руководство деятельностью которых осуществляет Резервный Банк Индии (RBI) и имеющие физическое присутствие на территории Индии, могут предлагать интернетовские банковские продукты резидентам Индии. Банки могут открывать счета только после надлежащего знакомства и физической верификации личности клиента, не смотря на то, что заявление об открытии счета может быть направлено при помощи Интернета. Банки должны хранить информацию с разбивкой на виды операции и предоставлять RBI для проведения проверки /аудита, когда их к этому призывают. Банки обязаны сообщать в RBI о любых сбоях в системе безопасности и нарушениях процедур, которое по своему собственному усмотрению, может принять решение об аудите/проверке таких банков. Что касается валютных операций, то банки должны соблюдать закон о валютном регулировании (FEMA) в отношении трансграничных сделок, операций и содержания счетов востро в Индии. Банки должны разработать эффективные меры по управлению рисками, а также не нарушать положения о конфиденциальности информации о банковских счетах клиента.

СПИСОК ЛИТЕРАТУРЫ

См. соответствующие материалы ФАТФ (все они доступны на www.fatf-gafi.org)

Отчет ФАТФ о новых платежных методах, ФАТФ (2006), ФАТФ, Париж

Отчет ФАТФ: Уязвимые места коммерческих интернет-сайтов и систем интернет-платежей, позволяющие использовать их для отмыwania денег и финансирования терроризма, ФАТФ (2008), ФАТФ, Париж

Отчет ФАТФ о новых платежных методах, ФАТФ (2010), ФАТФ, Париж

Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения – Рекомендации ФАТФ (2012), ФАТФ, Париж

Руководство ФАТФ по оценке рисков, ФАТФ (2013а), ФАТФ, Париж

Руководство по применению мер по противодействию отмыванию денег и финансированию терроризма и доступности финансовых услуг, ФАТФ (2013b), ФАТФ, Париж

ИНЫЕ ПОЛЕЗНЫЕ ИСТОЧНИКИ

Платежи и операции через терминалы, при помощи не MNIs, общее число операций: 5. Операции по покупке электронных денег, Европейский Центральный банк (пс), www.ecb.int/stats/payments/paym/html/payments_nea_n_IEM.NT.ZOZ.Z.en.html, будет доступно с 22 июня 2013 г.

«Инновации в розничной системе платежей во всем мире: краткая характеристика», Всемирный банк (2012)

Руководство Вольфсбергской группы о предоплаченных картах и карточках с заложенным лимитом средств, Вольфсбергская группа (2011)