Для официального пользования **ФАТФ/ РГТИП(2010)21/РЕД.1**

Группа разработки финансовых мер борьбы с отмыванием денег
Financial Action Task Force
Groupe d'Action Financière **05 октября 2010г.**

Английская Версия – Язык Оригинала: Английский

Рабочая группа по типологиям

НОВЫЕ СПОСОБЫ ПЛАТЕЖЕЙ

Итоговый проект документа (30 сентября 2010 года)

18 октября 2010 года, Штаб-квартира ОЭСР, Париж, Франция

XXII Пленарное заседание ФАТФ

Пожалуйста, имейте этот документ при себе на заседании, так как бумажные копии на заседании предоставляться не будут.

Винсент ШМОЛЛ (Vincent SCHMOLL), тел.: +33 1 45 24 17 52; vincent.schmoll@fatf-gafi.org
Александра ЭКЕРТ (Alexandra ECKERT), тел.: +33 1 45 24 99 50; alexandra.eckert@fatf-gafi.org

JT03289531

ФАТФ/РГТИП(2010)21/Ред.1 **Английская Версия – Язык Оригинала: Английский**
Для официального пользования

НОВЫЕ СПОСОБЫ ПЛАТЕЖЕЙ
ИТОГОВЫЙ ПРОЕКТ ДОКУМЕНТА (30 СЕНТЯБРЯ 2010 ГОДА)

КРАТКИЙ ОБЗОР

1. После выпуска в 2006 году Отчета о новых способах платежей, увеличившиеся масштабы использования новых способов платежей (НСП) и возросшее понимание связанных с этим рисков отмывания денег и финансирования терроризма привели к выявлению за последние четыре года ряда случаев легализации незаконных доходов.

2. Рабочая группа по проекту провела анализ 33-х ситуационных исследований, в большинстве из которых использовались предоплаченные карты или системы Интернет-платежей. Только в трех из представленных примеров незаконной деятельности были задействованы системы оплаты через мобильные телефоны, однако, суммы отмытых денег в этих случаях оказались невелики. Было выявлено три основных типологии, связанных с незаконным использованием новых способов платежей для целей отмывания денег и финансирования терроризма:

- Вложение денег третьими лицами (включая фиктивных и подставных лиц)
- Использование безличного характера счетов для использования новых способов платежей
- Провайдеры услуг новых способов платежей или их сотрудники, являющиеся соучастниками преступных схем

3. Хотя проведенный анализ ситуационных исследований и подтвердил определенную уязвимость новых способов платежей с точки зрения их незаконного использования в целях отмывания денег и финансирования терроризма, очень трудно оценить масштаб этой угрозы. Суммы отмытых денег значительно отличались от случая к случаю. Несмотря на то, что в некоторых случаях речь идет о суммах в несколько сотен или тысяч долларов США, в более чем половине примеров фигурируют, гораздо, большие суммы денег (в четырех примерах суммы отмытых денег превысили отметку в 1 миллион долларов США, а самая крупная сумма составила 5,3 миллиона долларов США).

4. Для оценки риска отмывания денег и финансирования терроризма, связанного с новыми способами платежей, рабочая группа по проекту применила подход, использовавшийся при составлении отчета от 2006 года, внеся в него некоторые изменения. Группа провела оценку рисков, сопряженных с каждым конкретным продуктом или услугой, а не рисков, представляемых отдельными категориями новых способов платежей.

5. Анонимность, большое количество мест, в которых принимается оплата с помощью новых способов платежей, возможность осуществления различных операций, а также возможность снятия наличных денег через банкоматы являются одними из главных факторов, повышающих привлекательность новых способов платежей для преступных элементов, занимающихся отмыванием денег. Анонимность может быть обеспечена «непосредственно» - путем использования, по-настоящему, анонимных продуктов (т.е. не требующих какой-либо идентификации личности клиента). Кроме того, анонимность может быть достигнута «косвенным образом» - посредством незаконного использования персональных продуктов (т.е. путем обхода проверки личности с помощью поддельных или украденных удостоверений личности, либо за счет использования фиктивных или подставных лиц, и т.д.).

6. Эффективное снижение рисков отмывания денег и финансирования терроризма, представляемых новыми способами платежей, может быть достигнуто за счет ряда контрмер, принимаемых провайдерами услуг НСП. Очевидно, что анонимность, как фактор риска, может быть снижена за счет внедрения строгих и жестких процедур идентификации и проверки личности. Но, даже при отсутствии таких процедур, эффективное снижение риска, представляемого анонимным продуктом, может быть обеспечено за счет принятия других мер,

таких как введение лимитов сумм (т.е. ограничений на суммы операций или их частоту), либо путем внедрения системы жесткого мониторинга. В связи с этим, при оценке общего риска отдельного продукта или услуги НСП необходимо учитывать все факторы рисков, а также меры по их снижению.

7. В юрисдикциях не существует единого стандарта для определения обстоятельств, в которых продукт или услуга могут считаться «представляющими невысокий риск». Во многих юрисдикциях используются установленные пороговые значения сумм операций, осуществляемых с помощью новых способов платежей, или предельные суммы на счетах НСП для определения «сценария, представляющего невысокий риск». Однако такие установленные пороговые значения и размеры предельных сумм различаются в разных юрисдикциях. Кроме того, могут существовать различные мнения относительно «значимости» конкретных факторов риска или эффективности определенных мер снижения рисков вследствие правовых и культурных различий в юрисдикциях.

8. В некоторых юрисдикциях фирмам разрешено применять упрощенные меры надлежащей проверки клиентов (НПК) в случаях заранее определенных сценариев, представляющих невысокий риск. Но опять-таки, при этом следует учитывать, что в юрисдикциях нет единого стандарта, касающегося определения «упрощенных мер НПК». В ряде юрисдикций компании полностью освобождены от необходимости применять меры НПК при определенных сценариях, представляющих невысокий риск.

9. Не все услуги НПС подлежат регулированию во всех юрисдикциях. Несмотря на то, что во всех юрисдикциях, приславших ответы на анкету в рамках настоящего проекта, осуществляется регулирование и надзор за выпуском предоплаченных карт, предоставление услуг Интернет-платежей и мобильных платежей полежит регулированию и надзору в большинстве, но, все же, не во всех юрисдикциях (Рекомендация 23 и Специальная Рекомендация VI ФАТФ).

10. Рабочая группа по проекту также определила области, в которых действующие стандарты ФАТФ в недостаточной степени учитывают вопросы, касающиеся новых способов платежей:

- В случаях, когда услуги НСП предоставляются совместно с третьими лицами (например, управляющими программами карт, провайдерами услуг электронных валют, продавцами, розничными торговцами, различными видами «агентов»), действие законодательства в области ПОД/ФТ часто не распространяется на таких третьих лиц, и поэтому они не подлежат регулированию и надзору в сфере ПОД/ФТ. Понятия «агентов» и «аутсорсинга» лишь частично рассматривается в 40 Рекомендациях и 9 Специальных Рекомендациях ФАТФ (в Рекомендации 9 и Специальной Рекомендации VI). Было бы хорошо, если ФАТФ смогла бы предоставить разъяснения или руководящие указания по этому вопросу, особенно учитывая то, что некоторые юрисдикции в настоящий момент рассматривают новый подход к регулированию и надзору за деятельностью агентов.
- Многие провайдеры услуг НСП предоставляют свои услуги через Интернет и устанавливают деловые отношения без личного контакта, что, в соответствии с положениями Рекомендации 8 ФАТФ, связано со «специфическими рисками». В Рекомендациях не разъясняется, приравнивается ли понятие «специфические риски» к понятию «высокий риск» в том смысле, как оно использовано в Рекомендации 5. Если приравнивается, то это исключит для многих провайдеров услуг НСП возможность применения упрощенных мер НПК. Несмотря на то, что эксперты Рабочей группы ФАТФ по оценкам и имплементации недавно пришли к заключению, что коммерческая деятельность без личного контакта не рассматривается автоматически качестве сценария, представляющего высокий риск, в том смысле как он понимается в Рекомендации 5, было бы полезным подтвердить и разъяснить это в стандартах.

11. Было бы желательно, если члены других Рабочих групп ФАТФ присоединились к обсуждению вышеуказанных вопросов с целью внесения большей ясности в толкование положений

соответствующих Рекомендаций ФАТФ. Такая работа будет не только актуальной и полезной в отношении проблем, касающихся отмывания денег и финансирования терроризма, то также и в плане вопросов связанных охватом бедных слоев населения финансовыми услугами.

12. Новые способы платежей (также как и другие нововведения в финансовой сфере) были признаны эффективным средством для дальнейшего охвата бедных слоев населения финансовыми услугами. Многие из вышеупомянутых вопросов (например, возможность применения упрощенных мер НПК в случае невысокого риска, полное освобождение от обязанности применять меры НПК, а также регулирование и надзор за деятельностью агентов) связаны с глобальной проблемой охвата бедных слоев населения финансовыми услугами и выходят за рамки вопроса лишь одной уязвимости НСП в плане отмывания денег и финансирования терроризма.

СОДЕРЖАНИЕ

- **1. Введение**

Отчет, опубликованный в 2006 году

13. В октябре 2006 года ФАТФ опубликовала свой первый отчет, касающийся новых способов платежей (НСП). Этот отчет стал первой попыткой проанализировать возможные последствия, с точки зрения риска отмывания денег (ОД) и финансирования терроризма (ФТ), нововведений в сфере платежей, которые предоставили потребителям возможность осуществлять платежи напрямую посредством технических устройств, таких как персональные компьютеры, мобильные телефоны или карты, на которых хранятся данные.[1] Во многих случаях такие платежи могут осуществляться без необходимости для клиента иметь личный банковский счет.

14. Поскольку в то время такие новые способы платежей были относительно новым явлением, в отчет, выпущенный в 2006 году, вошли лишь несколько ситуационных исследований, связанных со случаями отмывания денег и финансирования терроризма. Кроме того, лишь некоторые юрисдикции начали рассматривать вопросы, касающиеся четкого определения различных продуктов, связанных с новыми способами платежей, и того, как они должны регулироваться. Поэтому в отчете основное внимание было уделено повышению осведомленности о существование таких новых продуктов и возможности их незаконного использования для целей отмывания денег и финансирования терроризма.

15. В отчете, опубликованном в 2006 году, было установлено, что риски отмывания денег и финансирования терроризма отличаются для каждого продукта, предназначенного для новых способов платежей, и, что оценка рисков ОД/ФТ для категорий НСП является непродуктивной. Вместо этого была разработана методология для оценки рисков, связанных с отдельными продуктами.

16. В отчете содержалось заключение о необходимости его доработки через несколько лет, когда появится больше ясности в отношении рисков, связанных с такими новыми платежными инструментами. Настоящий отчет является дополнением отчета о новых способах платежей, выпущенного в 2006 году, и содержит обзор ситуации, складывающейся в этой сфере.

Цели настоящего отчета

17. С момента опубликования отчета в 2006 году, новые способы платежей (предоплаченные карты, услуги мобильных платежей и Интернет-платежей) получили более широкое распространение и были признаны в качестве альтернативных способов осуществления платежных операций. В ряде стран некоторые новые способы платежей стали превращаться в эффективную альтернативу инструментам, использующимся в традиционной финансовой системе.

18. С 2006 года рост количества операций и объемов финансовых средств, переводимых посредством новых способов платежей, сопровождался увеличением количества выявленных случаев незаконного использования таких платежных систем для целей отмывания денег и финансирования терроризма. В отчете, опубликованном в 2006 году, указаны возможные законные и незаконные пользователи различных новых способов платежей, но не представлены достаточные свидетельства этого. В настоящем отчете приводится сравнение и сопоставление «потенциальных рисков», описанных в отчете, выпущенном в 2006 году, и «реальных рисков», выявленных в ходе анализа новых типологий и ситуационных исследований. Не все потенциальные риски, определенные в 2006 году, нашли подтверждение в ситуационных исследованиях. Однако это не означает, что такие риски не следует принимать во внимание. Юрисдикциям следует продолжать внимательно следить за развитием рынка с целью

[1] Включая различные носители информации, такие как карты с магнитной полосой или электронные чипы смарт-карт.

предотвращения незаконного использования новых продуктов и способов платежей, а также для выявления случаев, которые оставались незамеченными в прошлом.

19. В настоящем отчете также определены «сигналы опасности», которые: а) могут помочь провайдерам услуг НСП выявлять деятельность, связанную с отмыванием денег и финансированием терроризма, в их собственном бизнесе; и б) могут помочь другим финансовым учреждениям выявлять деятельность, связанную с отмыванием денег и финансированием терроризма, при ведении дел с провайдерами услуг НСП для повышения количества и качества сообщений о подозрительных операциях (СПО)

20. Несмотря на то, что в настоящее время появилось большее количество ситуационных исследований, вопросы, касающиеся надлежащего законодательства и регулирования в сфере новых способов платежей, все еще, остаются проблемой для многих юрисдикций. В этой связи в отчете определены трудности законодательного и регулирующего характера, связанные с новыми способами платежей, а также приводится описания различных подходов, используемых национальными законодательными и регулирующими органами для решения этих проблем. Сравнение подходов в области регулирования может помочь довести до сведения заинтересованных сторон решения принимаемые другими юрисдикциями в сфере регулирования новых способов платежей.

21. И наконец, в настоящем отчете рассматривается, в какой мере требования 40+9 Рекомендаций ФАТФ в достаточной степени охватывают вопросы отмывания денег и финансирования терроризма, связанные с новыми способами платежей.

Работа, проведенная рабочей группой по проекту

22. Рабочая группа по проекту провела анализ публикаций, касающихся новых способов платежей, а также вопросов отмывания денег и финансирования терроризма.[2] Члены рабочей группы также проанализировали ответы на анкету, касающуюся вопросов распространения внутренних провайдеров услуг НСП[3], роль регулирования в отношении новых способов платежей и ситуационные исследования случаев, выявленных юрисдикциями (последние также включали зарубежных провайдеров услуг). Ответы на анкету поступили из тридцати семи юрисдикций, а также от Комиссии Европейского Союза.

23. Большинство респондентов указали на наличие и использование новых способов платежей в своих юрисдикциях. Наиболее часто упоминаемым в ответах продуктом были предоплаченные карты (в 34 из 37 стран имеются провайдеры этой услуги), затем следовали провайдеры услуг Интернет-платежей (имеются в 17 странах) и провайдеры услуг мобильных платежей (имеются в 16 странах). Были представлены ситуационные исследования по трем видам НСП: 18 случаев были связаны с предоплаченными картами, в 14 случаях имели место услуги Интернет-платежей, и в 3 случаях речь шла об услугах мобильных платежей[4]. Подробный обзор приведен в Приложении А.

24. Рабочая группа по проекту также провела различного рода консультации с представителями частного сектора. В ежегодных совещаниях экспертов по типологиям, состоявшихся на Каймановых Островах в 2009-2010 годах, представители провайдеров услуг НСП, в том числе,

[2] Список публикаций, использовавшихся при подготовке настоящего отчета, приведен в Приложении С.
[3] Включая описание крупнейших и наиболее важных продуктов и провайдеров услуг.
[4] Были выдвинуты различные объяснения такого небольшого количества выявленных случаев, включая то, что объемы и суммы операций осуществляемых в секторе мобильных платежей остаются, весьма, небольшими; либо, что эти системы могут быть непривлекательными для преступников, занимающихся отмыванием денег; либо, что провайдеры услуг мобильных платежей и правоохранительные органы не сумели выявить преступную деятельность; либо, что преступники или сами правоохранительные органы незнакомы с этой технологией и плохо разбираются в ней.

представители сектора услуг Интернет-платежей, сектора мобильных услуг и представитель Консультативной группы помощи бедным (CGAP), выступили с докладами перед членами рабочей группы. На межсессионном заседании рабочей группы по проекту, состоявшемся в марте 2010 года в Амстердаме, представитель провайдера технологии пластиковых карт в Европе выступил с докладом, посвященным системам предоплаченных карт. Консультации с более широким кругом представителей частного сектора были проведены с помощью электронной системы консультаций ФАТФ, в которой был выложен проект настоящего отчета для обсуждения.

Структура настоящего отчета

25. Настоящий отчет подготовлен на основе отчета ФАТФ, опубликованного в 2006 году. Разработчики данного отчета попытались, по возможности, избегать повторений. Поэтому в настоящем отчете не приводится описание общих механизмов функционирования новых способов платежей[5]. Основное внимание в отчете уделено развитию ситуации в области новых способов платежей. В нем также представлена дополнительная информация, касающаяся оценки рисков, и приведены новые ситуационные исследования.

26. Настоящий отчет состоит из 4 Разделов:

- В Разделе 1 (главы 1 и 2) описывается работа, проведенная в рамках проекта, а также определены общие ключевые вопросы. В нем также представлен обзор развития ситуации в секторе.
- В Разделе 2 (главы 3 и 4) рассматриваются риски и уязвимость новых способов платежей, а также представлены ситуационные исследования и типологии.
- В Разделе 3 (глава 5) рассматриваются вопросы, касающиеся регулирования и надзора, анализируются подходы, используемые различными странами в области законодательства в сфере ПОД, а также вопросы судебного преследования незаконных провайдеров услуг НСП.
- В Разделе 4 (глава 6) представлено заключение и приведены вопросы для дальнейшего рассмотрения.

2. Предыстория вопроса

«Новые способы платежей» и их развитие с 2006 года

27. В 2006 году выпускаемые банками платежные карты, а также операции, осуществляемые через Интернет или с помощью телефона, не были чем-то совершенно новым. Депозитные финансовые учреждения предлагали услуги удаленного доступа к счетам клиентов в течение десятилетий. Новшеством этих технологий в 2006 году было их использование банками без традиционных личных депозитных счетов. Новым было и то, что эти технологии также использовались небанковскими учреждениями, некоторые из которых не попадали в традиционные категории провайдеров финансовых услуг и, следовательно, на них не распространялись меры регулирования, несмотря на то, что они оказывали финансовые услуги, такие как осуществление платежей и ведение счетов. В настоящее время все еще остается несколько юрисдикций, в которых на провайдеров услуг НСП не распространяются меры пруденциального регулирования и/или регулирования в сфере противодействия отмыванию денег.

28. Развитие новых способов платежей создало новые возможности для незаконного использования этих технологий преступными элементами в целях отмывания денег и финансирования терроризма. Это, в свою очередь, привело к возникновению новых типологий и создало новые трудности для правоохранительных органов.

[5] Выдержки из соответствующих разделов отчета, опубликованного в 2006 году (включая определения), приведены в Приложении B.

Содействие развитию новых способов платежей юрисдикциями и государственными органами

29. Новые способы платежей получили развитие в результате законных потребностей рынка в инструментах, являющихся альтернативой традиционным финансовым услугам. В некоторых случаях это было обусловлено потребностью в более удобных и безопасных методах оплаты покупок через Интернет. В других случаях развитие было вызвано стремлением предоставить финансовые услуги тем, кто был лишен доступа к традиционным финансовым услугам (например, лицам с плохим кредитным рейтингом, национальным меньшинствам, но также и жителям регионов, имеющих ограниченные возможности открывать банковские счета).[6] Кроме того, свою роль сыграло предположение о том, что развитие новых способов платежей может положительно сказаться на состоянии национальных бюджетов, а также на общем национальном и мировом экономическом развитии.[7]

США: Четыре миллиона человек, получающих социальные пособия, не имеют банковских счетов. Для снижения зависимости от бумажных чеков, власти Соединенных Штатов начали выплачивать пособия, используя предоплаченные карты, которые могут быть использованы получателем для покупки товаров или снятия наличных денег. До этого, получатели пособия получали наличные деньги по чеку в небанковских учреждениях и осуществляли операции, используя наличные деньги или платежные поручения.[8]

Пакистан: В 2009 году в результате боевых действий более миллиона человек были вынуждены покинуть свои дома. Правительству Пакистана требовалось найти способ для быстрейшего оказания финансовой помощи вынужденным переселенцам. Вместо того, чтобы выплачивать наличные деньги, Правительство Пакистана заключило партнерское соглашение с банком, предусматривающего выдачу предоплаченных карт на сумму 25 000 пакистанских рупий (около 300 долларов США) каждая. Одновременно с этим пакистанский банк и компания, выпускающая платежные карты, установили беспроводные кассовые терминалы в розничных торговых точках, где люди могли приобретать товары первой необходимости. Таким образом, используя карты, а не наличные деньги, Правительству Пакистана удалось оказать немедленную помощь, почти, 300 000 семей, используя прозрачные каналы распределения финансовых средств.[9]

30. В результате некоторые юрисдикции скорректировали свои нормативные базы для активного содействия развитию новых способов платежей на своем внутреннем рынке.

---

[6] Всемирный банк, Консультативная группа помощи бедным (CGAP), Подгруппа «Доступ через инновации» Большой двадцатки и другие организации также признали новые способы платежей и, в частности, услуги мобильных платежей, в качестве возможного инструмента для охвата финансовыми услугами бедных слоев населения и/или слоев, имеющих ограниченные возможности открывать банковские счета. Они выдвинули инициативы по содействию и поддержке внедрения новых способов платежей в соответствующих юрисдикциях.

[7] Это обусловлено большей эффективностью с точки зрения скорости осуществления операций, завершенностью платежей, безопасностью методов платежей, основанных на этой технологии, а также меньшими издержками по сравнению с бумажными платежными инструментами. Другой важной особенностью новых способов платежей, объясняющей поддержку их развития со стороны политиков, является их доступность: в частности, предоплаченные карты и услуги мобильных платежей обеспечивают легкий и удобный доступ к системе платежей всему населению, включая тех, кто не имеет возможности открыть счет в банке. С учетом этих потенциальных возможностей центральные банки, будучи органами, осуществляющими надзор за платежной системой, давно уже обращают пристальное внимание на развитие новых способов платежей. В конечном итоге, Банк международных расчетов выступил с инициативой провести исследование нововведений в сфере розничных платежей.

[8] http://www.directexpress.org/Media/News_9_3_08_West_Announcement.cfm

[9] http://www.currencyofprogress.com/_media/pdfs/case_studies/VISA_Inclusion-Pakistan.pdf

Комиссия Европейского Союза открыто приветствует и поддерживает развитие новых способов платежей и заявляет в Пояснительном меморандуме к первой редакции Директивы, касающейся электронных денег, от 1998 года:[10]

«Электронные деньги имеют потенциал для превращения в действенное и эффективное средство платежей; они могут играть важную роль в развитии и совершенствовании электронной торговли; и они могут быть важным инструментом для завершения создания единого рынка и валютного союза. Комиссия считает, что в интересах как предпринимателей, так и потребителей будет то, чтобы система электронных денег развивалась в рамках регулирования, которое укрепляет доверие и уверенность в этом новом развивающемся платежном инструменте. В то же самое время важно, чтобы развитию не мешали жесткие технологические правила, которые будут препятствовать инновациям и ограничат конкуренцию.

Предложение Комиссии (…) вводит режим регулирования, необходимый для обеспечения финансовой безупречности небанковских эмитентов без удушения развития в сфере электронных денег, и поможет создать условия, в которых развитие этих новых средств платежей будет поддерживается в интересах предпринимателей и потребителей.»

В новой редакции Директивы, касающейся электронных денег, Комиссия подтверждает заявленные цели и намерения:[11]

«Общей целью пересмотра Директивы, касающейся электронных денег, является содействие появлению по-настоящему единого рынка услуг электронных денег в Европе. Содействовать разработке и внедрению новых инновационных и надежных услуг электронных денег. Предоставить доступ на рынок новым игрокам и обеспечить реальную и эффективную конкуренцию между всеми участниками рынка, принося, таким образом, существенные выгоды для расширяющейся экономики Европы.»

В соответствии с этим, пункт (4) Директивы, касающейся электронных денег[12], в новой редакции звучит следующим образом:

«(4) С целью устранения барьеров для доступа на рынок и содействия деятельности по эмиссии электронных денег, правила, распространяющиеся на учреждения, занимающиеся выпуском электронных денег, должны быть пересмотрены для обеспечения равных условий для всех провайдеров платежных услуг.»

Другие исследования новых способов платежей, рисков отмывания денег/финансирования терроризма и уязвимости

31. Новые способы платежей привлекли к себе повышенное внимание прессы. Они также являются предметом растущего количества исследований, проводимых представителями как государственного, так и частного сектора. Помимо этого, имеется ряд недавно завершенных и продолжающихся проектов по типологиям, инициированных ФАТФ и региональными организациями по типу ФАТФ, в которых затрагиваются эта тема[13]. Все это говорит о росте

[10] COM (1998) 461 final, p. 10;
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:1998:0461:FIN:EN:PDF
[11] SEC (2008) 2572, p. 5;
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2008:2572:FIN:EN:PDF
[12] Директива 2009/110/EC; OJ L 267 (10.10.2009), стр.7;
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:EN:PDF
[13] Недавно завершенные и продолжающиеся проекты по типологиям включают: Отчет ФАТФ по типологиям, касающийся уязвимости коммерческих веб-сайтов и систем платежей через Интернет с точки зрения отмывания денег и финансирования терроризма (18 июня 2008г.); семинар MONEYVAL по

осведомленности о возможностях и рисках, связанных с новыми способами платежей, с момента публикации отчета в 2006 году.

32. В отличие от упомянутых исследований, в которых часто рассматривалась лишь одна из категорий новых способов платежей, в настоящем отчете представлен более широкий сравнительный анализ этих вопросов и определены общие характеристики, присущие всем типам новых способов платежей. В нем также определены конкретные трудности и проблемы, представляемые каждой категорией новых способов платежей.

2.1 Ситуация, складывающаяся в секторе предоплаченных карт

33. Предоплаченные карты можно разделить на две основные категории: карты многоэмитентных (открытых) систем и карты одноэмитентной (закрытой) системы.[14] В настоящем отчете речь идет, в основном, о картах многоэмитентных (открытых) систем[15], поскольку карты одноэмитентной (закрытой) системы принимаются к оплате в ограниченном количестве мест. Тем не менее, это не означает, что карты одноэмитентной (открытой) системы представляют небольшой риск с точки зрения ОД/ФТ: в нескольких ситуационных исследованиях речь идет о картах одноэмитентной системы. Однако в большинстве случаев, описанных в ситуационных исследованиях, карты одноэмитентной (закрытой) системы использовались не в качестве платежного инструмента, а только как средство промежуточного хранения денег. Это может быть проиллюстрировано следующими двумя примерами:

Использование украденной информации о кредитных картах для приобретения карт одноэмитентной системы

В 2007 году перед судом предстали два человека, обвиняемые в приобретении предоплаченных подарочных карт одноэмитентной (закрытой) системы с помощью украденной информации, касающейся счетов кредитных карт. Обвиняемые использовали подарочные карты для приобретения товаров, которые они затем возвращали в магазин в обмен на новые подарочные карты, либо сбывали приобретенные товары за наличные деньги. Так как новые предоплаченные карты не были связаны с украденными номерами счетов кредитных карт, подарочные карты оставались действительными даже после обнаружения факта кражи информации с кредитной карты. Обвиняемые были признаны виновными, и с них была взыскана сумма в размере 82 000 долларов США в качестве компенсации за причиненный ущерб. Один из обвиняемых был признан виновным в преступном сговоре и мошенничестве и приговорен в 45 месяцам тюремного заключения с последующим нахождением под надзором в течение трех лет. Второй обвиняемый был признан виновным в преступном сговоре и отмывании денег и приговорен к пяти месяцам тюремного заключения с последующим нахождением под надзором в течение трех лет.
Источник: США

Подозрение в использовании компании, занимающейся распространением карт одноэмитентной (закрытой) системы, для отмывания денег и финансирования терроризма

По информации, полученной правоохранительными органами, владелец компании, занимающейся распространением предоплаченных телефонных карт, был заподозрен в отмывании денег и связях с террористической организацией.
Владелец компании осуществил множество вкладов крупных сумм наличных денег на личный банковский счет и счет своей компании. На допросе он показал, что продавал предоплаченные телефонные карты розничным продавцам и владельцем магазинчиков, торгующих товарами повседневного спроса, а оплату за карты получал не чеками, а наличными деньгами. Он пояснил,

киберпреступности (в процессе осуществления); семинар ЕАГ по платежам через Интернет (в процессе осуществления).

[14] Более подробная информация приведена в определении предоплаченных карт в отчете ФАТФ, опубликованном в 2006 году (определение приведено в Приложении В к настоящему отчету).

[15] Для целей настоящего отчета термин предоплаченные карты включает виды карт, определенные в отчете ФАТФ от 2006 года как «электронные кошельки».

что принимал наличные деньги, поскольку не был уверен, что выданные чеки будут оплачены. Некоторые вклады были также произведены на счета поставщиков предоплаченных телефонных карт.
Кроме того, владелец компании осуществлял электронные переводы средств в пользу физических лиц, находящихся в Европе и на Ближнем Востоке. Такие переводы иногда осуществлялись со счетов, по которым до этого не отмечалось большого движения средств. Помимо этого, владелец компании являлся бенефициаром средств, переводимых в пользу тех же самых физических лиц.
Источник: Канада

34. На пленарном заседании ФАТФ, состоявшемся в июне 2010 года в Амстердаме, рабочей группе по проекту поручили представить информацию о характере и рисках, присущих картам одноэмитентной (закрытой) системы.[16] Однако, за исключением двух приведенных выше случаев, у рабочей группы не было достаточных данных для оценки риска, представляемого такими картами, поскольку в анкете, разосланной в начале проекта, было четко указано, что карты одноэмитентной (закрытой) системы не являются предметом данного проекта. Несмотря на это, ряд факторов риска, а также мер по снижению риска, оценка которых приведена в настоящем отчете, и которые относятся к картам многоэмитентных (открытых) систем, могут также быть применены к картам одноэмитентной (закрытой) системы (например, в отношении мер НПК или лимитов сумм)[17].

35. Можно лишь оценить общий объем операций с использованием предоплаченных карт, поскольку в большинстве юрисдикций ведущие сети платежных карт, банки и небанковские учреждения, занимающиеся выпуском таких карт, а также провайдеры услуг не публикуют отдельную информацию о ежегодных объемах операций с использованием предоплаченных карт.[18] По данным исследования, заказанного компаний «MasterCard» и проведенного Бостонской консультационной группой (BCG)[19], в Соединенных Штатах общий объем финансовых средств, положенных на предоплаченные карты в 2009 году, оценивался в 120,2 миллиардов долларов США.

36. Тогда как в Соединенных Штатах, около, 17% потребителей имеют предоплаченные карты[20], за пределами США процент потребителей, обладающих предоплаченными картами, ниже, и потенциал рынка также может быть меньшим[21].

[16] Этот вопрос возник после проведения взаимной оценки Бразилии. Группа экспертов-оценщиков подвергла Бразилию критике за применение сокращенных мер НПК в отношении таких карт без предварительного проведения тщательной оценки рисков с целью определения рисков, связанных с этим продуктом (Отчет о взаимной оценке Бразилии, 2010г. стр.98).

[17] Исходя из обсуждений в ходе оценки Бразилии и имеющихся показателей, возможно, будет целесообразным провести анализ уязвимости предоплаченных карт одноэмитентной (закрытой) системы с точки зрения отмывания денег и финансирования терроризма в отдельном отчете по типологиям.

[18] Информация об объемах операций с использованием предоплаченных карт компаний «MasterCard» и «Visa» по данным об операциях по дебетовым картам этих компаний. По данным компании «Visa», за год, закончившийся 30 июня 2009 года, объем операций с использованием дебетовых карт этой компании для приобретения товаров и услуг составил 935 миллиардов долларов, немногим более 84% из которых пришлось на Соединенные Штаты. (Отчет 10К компании «VISA», представленный Комиссии по ценным бумагам и биржам, Вашингтон, Округ Колумбия, 20 ноября 2009 года). (См. http://www.sec.gov/Archives/edgar/data/1403161/000119312509239249/d10k.htm). Что касается компании «MasterCard», то за год, закончившийся 31 декабря 2009 года, общий объем операций с использованием дебетовых карт этой компании составил 814 миллиардов долларов, 55% из которых пришлось на Соединенные Штаты (Отчет 10К компании «MasterCard», представленный Комиссии по ценным бумагам и биржам, Вашингтон, Округ Колумбия, 18 февраля 2010 года). (См. http://www.sec.gov/Archives/edgar/data/1141391/000119312510034065/d10k.htm).

[19] http://www.paymentsnews.com/2010/07/mastercard-releases-prepaid-market-sizing-report.html

[20] Федеральный резервный банк Бостона, Исследование предпочтений способов платежей потребителями, опубликованное в 2008 году (См: http://www.bos.frb.org/economic/ppdp/2009/ppdp0910.pdf)

[21] По данным расположенной в Великобритании консалтинговой фирмы «PSE Consulting»: «В США распространение предоплаченных продуктов обусловлено тем, что они приходят на смену выплате

37. Несмотря на то, что предоплаченные карты были введены в ряде стран, в большинстве государств использование предоплаченных карт распространено не так широко, как в Соединенных Штатах. В вышеупомянутом исследовании Бостонской консультационной группы (см. сноску 21) содержится прогноз о том, что в 2017 году на долю Соединенных Штатов будет приходиться 53% мирового рынка предоплаченных карт, а Великобритания и Италия будут оставаться крупнейшими рынками предоплаченных карт в Европе. При этом к 2017 году на долю Великобритании будет приходиться 25%, а на долю Италии 20% всего европейского рынка.[22] Исследование Бостонской консультационной группы, в целом, согласуется с исследованием, проведенным в 2009 году по инициативе международной компании по обработке операций с кредитными картами «First Data». В этом исследовании отмечается, что Италия являлась «наиболее развитым рынком предоплаченных карт в Европе», рынок Великобритании оценивался как «сформировавшийся», а рынки Германии и Австрии были определены, как «находящиеся в зачаточном состоянии».[23] Можно уверенно сказать, что за последние годы наблюдается общая тенденция увеличения использования и распространения предоплаченных карт. По данным Комитета по платежным и расчетным системам при Банке международных расчетов в Базеле[24], количество выпущенных «карт с функцией электронных денег»[25] выросло в выбранных Комитетом странах[26] с 107,6 миллионов в 2004 году до 275,28 миллионов в 2008 году.

Юрисдикция	**Кол-во выпущенных карт (оценка)**	**Юрисдикция**	**Кол-во выпущенных карт (оценка)**
Япония	100 миллионов	**Словакия**	4 миллиона
Сингапур	15 миллионов	**Мексика**	2,6 миллиона
Италия	8 миллионов	**Россия**	2 миллиона
Норвегия	6 миллионов	**Франция**	1,3 миллиона

39. Со времени опубликования первого отчета в 2006 году не произошло никаких существенных технических прорывов: в большинстве предоплаченных карт многоэмитентных (открытых) систем все еще используются магнитные полосы. Электронный чип в, так называемых, «смарт-

---

заработной платы чеками, поскольку люди с невысокими доходами часто вынуждены тратить 50-60 долларов в месяц за «обналичивание» чеков при оплате коммунальных услуг или отправке денег на своим семьям на родину. В Европе распространенная практика электронных выплат заработной платы и государственных пособий, а также наличие бесплатных «основных банковских» продуктов означает, что процент населения, не имеющего банковских счетов, существенно ниже, чем в США, и потребители не привыкли платить такие высокие комиссионные отчисления.»
(См: http://www.pseconsulting.com/pdf/articles/sep06/pse_repaid_press_release_110806.pdf)
Такая точка зрения нашла подтверждение, по крайне мере, в Великобритании в отчете Совета по платежным системам. В отчете под названием «Как мы платим», опубликованном в 2010 году, отмечается, что заработная плата 89% рабочих перечисляется напрямую на их личные банковские счета, а оставшиеся процент рабочих получают зарплату в виде чеков или наличными деньгами. В отчете не упоминаются предоплаченные карты. (Совет по платежным системам, Отчет «Как мы платим», 2010г., Великобритания; см: http://www.paymentscouncil.org.uk//files/payments_council/the_way_we_pay_2010_final.pdf)

[22] http://www.mastercard.com/us/company/en/newsroom/independent_research.html

[23] Компания «First Data», http://www.firstdata.com/en_ae/about-first-data/media/press-releases/11_26_09

[24] Статистические данные по платежным и расчетным системам в определенных странах – Данные за 2008 год (декабрь 2009г.). (См: http://www.bis.org/publ/cpss88.pdf).

[25] Такие карты были определены как «пополняемые предоплаченные карты многоцелевого использования, которые могут быть использованы в торговых точках нескольких провайдеров услуг для широкого круга целей, и которые потенциально могут использоваться в национальном или международном масштабе, хотя, иногда их использование может быть ограничено определенном регионом». Статистические данные по платежным и расчетным системам в определенных странах – Данные за 2008 год (декабрь 2009г.), стр.312

[26] Статистические данные по платежным и расчетным системам в определенных странах – Данные за 2008 год (декабрь 2009г.), Таблица 10, стр.262. Приведенные цифры включают данные, полученные из Бельгии, Франции, Германии, Италии, Японии, Нидерландов, Сингапура и Швейцарии, и не включают информацию из Канады, Гонконга, Швеции, Великобритании и Соединенных Штатов («nav» - означает нет данных).

картах» обычно используется для обработки дополнительной клиентской информации. Использование систем предоплаченных карт, использующих этот чип для хранения денег на карте («электронные кошельки»)[27], обычно ограничено масштабами страны, и они часто имеют небольшие лимиты сумм.

40. Как указано в отчете ФАТФ, опубликованном в 2006 году, предоплаченные карты могут стать альтернативной различным традиционным банковским продуктам и услугам, таким как дебетовые или кредитные карты или дорожные чеки. Многие предоплаченные карты дают возможность клиентам осуществлять международные платежи, а некоторые из них по своим возможностям все больше напоминают обычные банковские счета: такие продукты позволяют клиентам не только осуществлять платежи, но и получать платежи от третьих лиц. Они также могут обеспечить возможность осуществлять трансграничные переводы денег. Это достигается, например, путем выдачи нескольких «дубликатов» или «парных» карт одному клиенту, который может передать их получателям денежных переводов в любой точке мира. Такие «дубликаты» или «парные» карты позволяют их держателю получать деньги владельца «основной» карты через глобальную сеть банкоматов.[28]

41. Известно, что ряд провайдеров услуг Интернет-платежей и мобильных платежей предоставляют своим клиента дополнительные предоплаченные карты для облегчения получения наличных денег через банкоматы внутри страны или за рубежом. Это было отмечено в отчете от 2006 года в отношении сектора мобильных платежей, но сейчас это относится и к услугам Интернет-платежей .

2.2 Ситуация, складывающаяся в секторе услуг Интернет-платежей

42. Услуги Интернет-платежей могут предоставляться финансовыми учреждениями и фирмами, не входящими в сектор финансовых услуг. Они могут использовать банковский счет или осуществлять операции с банковского счета самостоятельно.

43. Способы Интернет-платежей подразделяются на три категории:

- Интернет-банкинг - кредитные учреждения предлагают доступ через Интернет к традиционным банковским услугам при наличии счета, открытого в кредитном учреждении на имя клиента. Интернет-банкинг не является предметом исследования в настоящем документе.
- **Предоплаченные продукты для осуществления Интернет-платежей** – фирмы, которые могут не являться кредитными учреждениями, предоставляют клиентам возможность отправлять или получать деньги через виртуальный предоплаченный счет, доступный через Интернет.
- **Электронные деньги** – клиенты обычно приобретают единицы электронных валют или электронных драгоценных металлов, которые могут быть обменены между владельцами счетов одного и того же провайдера услуги, либо быть обменяны на настоящую валюту и сняты.

44. С 2006 года в ряде стран наблюдалось расширение ассортимента и рост количества предоплаченных продуктов, предназначенных для Интернет-платежей, что возможно, связано с увеличением масштабов использования Интернета и приемом платежей через Интернет онлайновыми торговыми компаниями. Такие продукты также все чаще используются для осуществления денежных переводов между физическими лицами.

---

[27] Определение электронных кошельков приведено в отчете ФАТФ о новых способах платежей, опубликованном в 2006 году, а также включено в данный отчет в Приложении B. Для целей настоящего отчета электронные кошельки включены в категорию «предоплаченных карт» (также см. определение термина «электронные кошельки» в Глоссарии).

[28] См. также главу 5.2 «идентификация вторичных владельцев/держателей карт», пункт 194.

45. В последние годы появилась электронная валюта, связанная с **виртуальным миром**, в котором пользователи конвертируют реальные деньги в виртуальную валюту для совершения покупок в виртуальной среде. В той же самой виртуальной среде пользователи нередко осуществляют денежные переводы между физическим лицами (т.е. пользователи посылают виртуальные деньги знакомым пользователям). Такие виртуальные деньги не ограничены конкретной компьютерной игрой, поскольку ими можно торговать в реальном мире и переводить в реальные деньги.

46. **Денежные сертификаты** становятся все более популярными на ряде рынков. Такие сертификаты можно пробрести на условиях анонимности в магазинах розничной торговли, на автозаправочных станциях и т.д. Обычно они продаются на определенные суммы, начиная от 10 евро и заканчивая 500 фунтов стерлингов (примерно,750 евро).[29] Изначально денежные сертификаты предназначались для осуществления платежей физическими лицами в пользу компаний через Интернет. Но они также могут использоваться для совершения операций между физическими лицами, если принимаются в качестве метода платежа другими провайдерами услуг НСП (например, компаниями-эмитентами предоплаченных карт, или пунктами обмена электронных валют). Кроме того, Денежные сертификаты могут быть использованы для азартных игр в Интернете.

47. **Услуги Интернет-платежей становятся все более взаимосвязанными с различными новыми и традиционными платежными услугами.** В настоящее время деньги могут быть переведены или получены с помощью различных способов платежей: путем передачи наличных денег, с помощью услуг денежных переводов (например, «Western Union»), посредством новых способов платежей, банковским телеграфным переводом, а также с помощью кредитных карт. Более того, некоторые провайдеры услуг Интернет-платежей стали предоставлять своим клиентам предоплаченные карты, давая им, таким образом, возможность **снимать наличные деньги через сети банкоматов во всем мире.**

48. Как отмечалось выше, 15 юрисдикций из общего числа стран, приславших ответы на анкету, указали на то, что провайдеры услуг Интернет-платежей осуществляют свою деятельность на их территории. К сожалению, не было представлено статистики, касающееся количества таких провайдеров и числа действующих клиентских счетов. Однако в странах, предоставивших такую статистку, количество провайдеров, по оценкам, составляло от одного до 23. Что касается количества действующих счетов для осуществления Интернет-платежей, то, по оценкам, их число составило от 45 тысяч до 80 миллионов.

2.3 Ситуация, складывающаяся в секторе услуг мобильных платежей

49. Для целей оценки рисков и уязвимости чрезвычайно важно различать «мобильные платежи», осуществляемые с личных банковских счетов или счетов ценных бумаг каждого клиента (и получателя), открытых в финансовом учреждении, на которое распространяются соответствующие меры регулирования и надзора в области ПОД/ФТ, и услуги, предоставляемые

[29] Денежные сертификаты обладают рядом характеристик, аналогичных характеристикам предоплаченных карт, и поэтому некоторые относят их к категории предоплаченных карт, а не к продуктам, предназначенным для Интернет-платежей. Однако поскольку в настоящем отчете рассматриваются все новые способы платежей, нет необходимости принимать окончательное решение об отнесении таких сертификатов к категории предоплаченных карт или к категории продуктов, связанных с Интернет-платежами.

отдельно с таких счетов.[30] В этом отношении, возможно, будет полезным использовать четыре категории систем мобильных платежей, описанных в документе Всемирного банка[3132]:

- Мобильные услуги по предоставлению финансовой информации: Пользователи могут ознакомиться с данными по личному счету, а также с общей финансовой информацией, но при этом не осуществляется никаких финансовых операций. Поэтому данный вид услуг рассматривается, как представляющий невысокий риск.
- Услуги мобильных банковских счетов и счетов ценных бумаг: Пользователи могут осуществлять операции, аналогичные банковским операциям через Интернет. Эта услуга привязана к личному банковскому счету или счету ценных бумаг. Поэтому она (как и Интернет-банкинг), строго говоря, не рассматривается в качестве нового способа платежей, в том смысле, в котором это термин используется в настоящем отчете. На услуги мобильных банковских счетов и счетов ценных бумаг, скорее всего, будут распространяться меры регулирования и надзора.
- **Услуги мобильных платежей:** Данные услуги позволяют владельцам небанковских счетов, а также счетов отличных от счетов ценных бумаг осуществлять платежи посредством мобильных телефонов. При этом провайдеры платежных услуг могут являться нетрадиционными финансовыми учреждениями, на которые меры контроля и надзора распространяются в различной степени.
- **Услуги мобильных денег:** Пользователи этой услуги могут хранить реальные средства на своих мобильных телефонах. Они могут использовать телефонные кредиты или «эфирное время» в качестве предложения для оплаты. Такие системы являются, весьма, многофункциональными, но также на них нередко могут совсем не распространяться меры регулирования и пруденциального надзора.

50. В настоящем отчете рассматриваются только две последние категории. Тем не менее, вопросы, исследуемые в данном отчете, могут также относиться к услугам мобильных банковских счетов и счетов ценных бумаг (например, вопросы аутсорсинга коммерческой деятельности или использования агентов; или применение упрощенных мер НПК; или открытие счета без личного контакта).

51. Ожидалось, что активное развитие технологий мобильных телефонов, наблюдаемое с 2006 года, должно было привести к росту рынка использования систем мобильных платежей. Ожидаемое распространение таких систем считалось показателем тенденции перехода от бумажных платежей к электронным платежам, являющейся общей для всех нововведений в платежных системах.

52. Однако, несмотря на предсказанное расширение рынка использования и распространения систем мобильных платежей[33], по состоянию на текущий момент только нескольким провайдерам

[30] Такие услуги также могут предоставляться с участием банка. Однако в этих бизнес моделях осуществление платежных операций не основано на личных банковских счетах каждого клиента или получателя.

[31] Рабочий документ Всемирного банка №146 «Целостность финансовых услуг, предоставляемых посредством мобильных телефонов» (“Integrity in mobile phone financial services”) 2008 г., стр. 18

[32] На рынке услуг мобильных платежей могут использоваться другие термины, такие как «мобильные бумажники», «мобильный перевод денег» (означающий оплату, осуществляемую между физическими лицами) или «мобильный платеж» (означающий оплату, осуществляемую физическим лицом в пользу компании, т.е. розничные платежи или оплату счетов). В настоящем отчете эти определения не используются в этом значении.

[33] Оценки различались. Было сделано предположение, что к 2015 году 1,4 миллиарда человек будут использовать сотовые телефоны для перевода денег внутри страны и за рубеж. (Майкл Клейн, Рабочий документ Всемирного банка №146: «Целостность финансовых услуг, предоставляемых посредством мобильных телефонов», 2008г.). Другие источники предполагали, что рост услуг операций, осуществляемых посредством мобильных телефонов, составит 68% в год и достигнет, почти, 250 миллиардов долларов США в 2012 году (Артур Д. Литтл, Дополнение к отчету о мобильных платежах в мире – 2009г.). Эти оценки

удалось создать прибыльную бизнес модель[34], успешно работающую в долгосрочной перспективе[35].

53. Как отмечалось выше, 15 юрисдикций из общего числа стран, приславших ответы на анкету, указали на то, что провайдеры мобильных платежей осуществляют свою деятельность на их территории. К сожалению, не было представлено статистики, касающееся количества таких провайдеров и числа действующих счетов клиентов. Кроме того, не все юрисдикции, приславшие ответы на анкету, четко разграничили мобильные платежи, как они понимаются в настоящем отчете, и мобильный-банкинг. В странах, предоставивших такую статистку, количество провайдеров, по оценкам, составляло от одного до 21. Что касается количества действующих счетов для осуществления мобильных платежей, то, по оценкам, их число варьируется от 26 тысяч до 15 миллионов.

54. Технологическое развитие в сфере систем мобильных платежей включает их объединение с другими способами платежей, в том числе с традиционными методами платежей, а также с другими новыми способами платежей:

- Ряд провайдеров услуг мобильных платежей, предлагают предоплаченные карты многоэмитентных (открытых) систем, связанные со счетами своих клиентов. С помощью этого, изначально «внутренние» провайдеры могут предложить услуги трансграничных платежей, поскольку это предоставляет клиентам, или третьим лицам, которым были переданы предоплаченные карты, возможность доступа к сети банкоматов во всем мире.
- Некоторые провайдеры предоставляют услуги по снятию денег через банкоматы, даже, без использования карты. Клиенты могут осуществлять операции между физическими лицами путем передачи определенного кода третьим лицам, которые могут ввести этот код в банкомат для получения суммы денег, привязанной к такому конкретному коду[36].
- Некоторые провайдеры сотрудничают с компаниями, оказывающими традиционные услуги денежных переводов (например, с компанией «Western Union»). Такая услуга денежных переводов позволяет третьим лицам, не являющимися клиентами провайдера услуг мобильных платежей, посылать клиенту или получать от клиента деньги, а также осуществлять переводы за рубеж.

3. Оценка риска новых способов платежей

Новые способы платежей: риски и возможности

55. С одной стороны, новые способы платежей, как и все остальные финансовые услуги и продукты, могут быть использованы в целях отмывания денег и финансирования терроризма. В

относились не только к услугам мобильных платежей, как они понимаются в настоящем отчете, но также включали услуги мобильного-банкинга.

[34] Это относится только к бизнес моделям мобильных платежей в том смысле, как они понимаются в настоящем отчете, что не включает «банковские» модели (т.е. бизнес модели, предусматривающие сотрудничество между банками и телекоммуникационными компаниями, при котором каждый клиент должен иметь личный банковский счет).

[35] На этот счет имеется несколько возможных объяснений, включая следующие. Норма прибыли в секторе услуг мобильных платежей, относительно, невысока; для получения прибыли необходимо иметь большое количество клиентов и продавцов, принимающих такую оплату; для завоевания доверия клиентов необходимо преодолеть трудности, касающиеся технологических вопросов и вопросов безопасности. Пруденциальное регулирование, а также регулирование в сфере ПОД/ФТ были названы одним из факторов, сдерживающих рыночный успех новых способов платежей в целом и провайдеров услуг мобильных платежей, в частности (более подробная информация приведена в главе 5).

[36] Возможность такого снятия наличных денег через банкомат без использования карты в настоящее время ограничена только внутренними (национальными) банкоматами в юрисдикции провайдера, и для этой цели могут использоваться только банкоматы конкретного банка, с которым заключено соглашение о сотрудничестве.

связи с этим в большинстве юрисдикций на провайдеров услуг НСП наложены обязательства в сфере ПОД/ФТ, а их деятельность регулируется в плане ПОД/ФТ.

56. С другой стороны, если у провайдеров услуг НСП имеются обязательства, касающиеся ПОД/ФТ, а за их деятельностью осуществляется надлежащий надзор в плане ПОД/ФТ, то в этом случае новые способы платежей могут повысить прозрачность платежных операций, а также способствовать недопущению коррупции и других злоупотреблений. Новые способы платежей могут содействовать переходу клиентов из нерегулируемых или, даже, незаконных секторов рынка платежей (например, хавала, подпольные банковские услуги) в официальный сектор. Это означает, что, если на провайдеров распространяются нормы законодательства и надзора в сфере ПОД/ФТ, то большее количество операций поставлено под контроль, а подозрительные операции выявляются, и информация о них доводится до сведения компетентного органа. В конечном итоге, это должно повысить качество надзора за осуществлением платежей в юрисдикции.

Сотрудники афганской полиции и военнослужащие США в Афганистане

По просьбе Правительства Афганистана в мае 2002 года Миссией ООН по содействию Афганистану и Программой развития ООН был учрежден Трастовый фонд для поддержания законности и порядка в Афганистане с целью обеспечения возвращения на службу афганских полицейских. Первоочередной задачей фонда стала выплата заработной платы полицейским. Совместно с Министерствами внутренних дел и финансов Афганистана и Объединенным переходным командованием США по обеспечению безопасности в Афганистане сотрудники указанного трастового фонда открыли более 62 000 банковских счетов для афганских полицейских, а также оказали содействие во внедрении системы электронных переводов для выплаты заработной платы сотрудникам полиции. Кроме того, ООН, а также власти Афганистана и представители США совместно с Первым банком микрофинансирования используют услуги по переводу денег «M-paisa», оказываемые мобильным оператором «Roshan» для выплаты заработной платы через мобильные сотовые телефоны. Мобильные платежи использовались для того, чтобы полицейские не оставляли свои посты для получения зарплаты. Использование электронных переводов денежных средств вместо выдачи наличных денег, также помогло избежать коррупции и взяточничества[37].

Источник: США

57. В отличие от наличных денег, новые способы платежей могут обеспечить дополнительные данные для расследований, проводимых правоохранительными органами, так как операция, осуществленная с использованием новых способов платежей, всегда оставляет «электронный след», тогда как при операциях с наличными деньгами не остается никаких документальных свидетельств. Даже, если меры НПК не применяются (т.е. в ситуации, когда клиент остается анонимным), электронные записи могут, в некоторых случаях, предоставить правоохранительным органам, по крайней мере, минимальные данные, такие как IP-адрес или информацию о месте осуществления платежа или снятия средств. Это, в принципе, может помочь в определении местонахождения и установлении личности пользователя, подозреваемого в отмывании денег или финансировании терроризма[38][39].

[37] http://www.undp.org.af/whoweare/undpinafghanistan/Projects/3rdQ08Reports/2009-01-29%20-%20Third%20Quarter%201387%20Progress%20Report%20-%20LOTFA.pdf

[38] Например, сотрудники правоохранительных органов, возможно, смогут получить видеоизображение подозреваемого в результате анализа материалов системы видеонаблюдения, установленной в месте оплаты или в месте, где был использован продукт (банкоматы, интернет-кафе, и т.д.).

[39] Критики сомневаются в полезности «электронных следов», оставляемых анонимными услугами или продуктами, указывая на то, что IP-адрес может быть подделан или, что может использоваться IP-адрес общественного заведения, такого как популярный клуб или интернет-кафе. В этих случаях информация окажется малополезной для правоохранительных органов в юрисдикциях с неразвитой системой видеонаблюдения.

58. В настоящем отчете приведен ряд случаев, когда для целей отмывания денег были использованы новые способы платежей, хотя преступники могли бы воспользоваться наличными деньгами или другими традиционными методами. В связи с этим можно предположить, что некоторые преступные элементы рассматривают новые способы платежей в качестве более удобного варианта, нежели наличные деньги для целей отмывания денег и финансирования терроризма. Это, в частности, относится к случаям, когда новые способы платежей используются в качестве альтернативы перевозке крупных сумм денег, либо когда безличный характер деловых отношений способствует использованию подставных лиц и поддельных документов, удостоверяющих личность[40].

Новые способы платежей и финансирование терроризма

59. Исходя из материалов, предоставленных юрисдикциями, в настоящем отчете речь идет в основном об отмывании денег. Когда затрагиваются вопросы финансирования терроризма, то это четко указано в тексте документа, а в остальных случаях примеры, относящееся к отмыванию денег, также могут быть отнесены к финансированию терроризма с соответствующими поправками.

60. Из 33 ситуационных исследований, анализируемых в настоящем отчете, только один пример явно связан с финансированием терроризма. (См. Раздел 4 «Типологии», ***пример 4***).

Общие риски, связанные с новыми способами платежей

61. В отчете, опубликованном в 2006 году, был выявлен ряд характеристик, являющихся общими для большинства новых способов платежей. Этих характеристики включают отсутствие кредитного риска, скорость осуществления операций и (часто) безличностный характер деловых отношений:

- Отсутствие кредитного риска

  Денежные средства, используемые в новых способах платежей, обычно являются предоплаченными. Отсутствие кредитного риска означает, что у провайдеров услуг имеется меньше стимулов для получения полной и точной информации о клиенте и о характере деловых отношений.

- Скорость осуществления операций

  Операции с использованием новых способов платежей могут быть осуществлены и деньги могут быть сняты или конвертированы гораздо быстрее, чем в случае использования более традиционных каналов. Это может затруднить мониторинг и потенциально свести на нет усилия по замораживанию денежных средств.

- Деловые отношения без личного контакта

  Многие (но не все) бизнес модели провайдеров услуг НСП основаны на деловых отношениях и операциях без личного контакта, что согласно Рекомендации 8 ФАТФ, представляет «специфические»[41] риски отмывания денег и финансирования терроризма,

[40] См., например, примеры «трансграничного перемещения карт» (глава 4.4, пункт 132) и «использование «мертвых душ» в качестве сотрудников» (глава 4.2, пункт 129, пример 20) в разделах, посвященных типологиям.

[41] Если рассматривать совместно с Пояснительной запиской к Рекомендации (пункт 7) и документом Базельского комитета о надлежащей проверке клиентов (раздел 2.2.6, пункт 48), то «специфический риск», похоже, означает «повышенный» риск: «48. При согласии на сотрудничество с клиентами без личного

вследствие повышенного риска того, что преступники будут действовать под видом законных пользователей, а также возможности того, что клиенты будут не теми лицами, за которых они себя выдают.

Оценка отдельных провайдеров и продуктов, а не новых способов платежей как таковых

62. Одним из выводов, содержащихся в отчете, опубликованном в 2006 году, было то, что риски отмывания денег и финансирования терроризма, а также уязвимость существенно отличаются в зависимости от конкретного провайдера услуг и продукта, даже, в одной и той же категории НСП, какой как предоплаченные карты. Это связано с тем, что различные продукты, обладают различными характеристиками, влияющими на степень их риска.

Модель оценки рисков

63. В отчете, опубликованном в 2006 году, была разработана модель рисков, включающая несколько факторов риска, для целей оценки риска, связанного с конкретными продуктами, используемыми в рамках новых способах платежей[42]. Эта модель была изменена и дополнена следующим образом:

- «Установление личности/идентификация» была заменена на «надлежащую проверку клиента» и теперь включает идентификацию, проверку личности и мониторинг.
- «Хранение данных» было добавлено в качестве дополнительного фактора риска.
- «Лимиты сумм» и «ограничения использования» были более детализированы, и
- В модель риска была включена «сегментация услуг». Сегментация услуг уже была определена в отчете от 2006 года как одна из проблем, стоящих перед регулирующими и правоохранительными органами, но не была включена в модель оценки рисков в то время.

64. Некоторые из рисков (такие как анонимность, методы вложения денег, лимиты сумм, и т.д.) прямо вытекают из характера продукта, тогда как другие риски имеют отношение к мерам НПК, принимаемым провайдерами (такие как порядок проверки личности и процедуры мониторинга).

65. Факторы риска, перечисленные в приведенной ниже модели, должны рассматриваться не по отдельности, а как единое целое. «Высокая степень риска», связанная с одним из факторов риска, не обязательно означает, что продукт представляет «высокий риск» в целом. Для эффективной оценки риска, связанного с конкретным продуктом, используемым в рамках новых способов платежей, важно оценить всю картину целиком, включая не только все факторы риска, но также и все меры, применяемые для снижения риска.

66.

Пример: фактор риска «ограничения использования/возможность использования для различных операций»
Согласно модели риска, услуги по осуществлению платежей между физическими лицами (физическое лицо – физическое лицо) считаются, представляющими более высокий риск, нежели услуги, предусматривающие только платежи, осуществляемые физическими лицами в пользу компаний (физическое лицо – компания). Такое суждение основано на том факте, что возможность платежей между физическими лицами позволяет пользователю переводить средства гораздо большему количеству потенциальных получателей без необходимости совершать покупки

контакта (…) необходимо наличие специальных и достаточных мер для снижения повышенного риска». См. также пункт 165.

[42] В других документах, касающихся оценки риска, были разработаны другие подходы с использованием различных факторов риска, которые не используются в настоящем документе. См., например, рабочий документ Всемирного банка №146 «Целостность финансовых услуг, предоставляемых посредством мобильных телефонов», 2008 г., стр.17.

или каких-либо других причин для совершения операции.
Однако возможность осуществлять платежи между физическими лицами в рамках услуги НСП не приводит автоматически к общей оценке такой услуги, как представляющей «высокий риск». И наоборот, услуги НСП, которые дают возможность осуществлять платежи только физическим лицам в пользу компаний, не могут автоматически считаться, как представляющие «невысокий риск». Следует также учитывать другие факторы риска, включенные в модель. (Например: Имеются ли меры по идентификации/подтверждения личности? Установлены ли лимиты сумм? …)

Факторы рисков способов платежей				
Критерии		**Наличные деньги**	**Новые способы платежей с высоким риском**	**Новые способы платежей с низким риском**
НПК	**Идентификация**	Анонимно	Анонимно	Личность клиентов устанавливается
	Проверка личности	Анонимно	Личность клиента (если установлена) не проверяется с использованием надежных, полученных из независимых источников документов, данных или информации (Рек. 5)	Личность клиента проверяется с использованием надежных, полученных из независимых источников документов, данных или информации (Рек.5)
	Мониторинг	нет	нет	Проводится постоянный мониторинг деловых отношений
Хранение данных		нет	Записи об электронных операциях ведутся, но не хранятся и не предоставляются по требованию правоохранительных органов	Записи об электронных операциях хранятся и предоставляются по требованию правоохранительных органов
Лимиты сумм	**Макс. сумма, хранимая на счету/счетах на человека**	Не ограничено	Не ограничено	Ограничения по сумме на счету (см. пункт 112)
	Макс. сумма операции (включая пополнение/снятие средств)	Не ограничено	Не ограничено	Ограничения по сумме на счету (см. пункт 112)
	Макс. частота операций	Не ограничено	Не ограничено	Ограничения по частоте операций (см. пункт 112)
Методы вложения денег		Не относится	Анонимные источники вложения средств (например, наличные деньги, денежные переводы, анонимные счета НСП); также множественные источники вложения средств, т.е. 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	Перевод средств за рубеж или снятие средств за рубежом	Перевод и снятие средств только внутри одного государства

		конвертировать через посредников		
Ограничения использования	**Возможность приема к оплате (прием продавцами)**	В целом принимаются	Большое количество принимающих продавцов / торговых точек (например, при использовании «VISA» или «MsterCard»)	Небольшое количество принимающих продавцов / торговых точек
	Возможность осуществления различных операций	Платежи: физическое лицо - компания, 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 относится	Анонимное и неограниченное снятие денег (например, снятие наличных через банкоматы)	Ограниченные возможности снятия (например, перевод только на ссылочные счета); ограничения по снимаемым суммам и частоте снятия (например, не более определенной установленной суммы в течение календарного года)
Сегментация услуг	**Взаимодействие провайдеров услуг**	Не относится	Несколько независимых провайдеров услуг выполняют отдельные этапы операции без эффективного надзора и координации	Вся операция проводится одним провайдером услуг
	Аутсорсинг	Не относится	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 наивысшими стандартами

67. Некоторые виды новых способов платежей могут быть в большей степени подвержены определенным факторам риска, нежели другие. Но большинство факторов риска, в определенной степени, распространяются на все виды новых способов платежей. Поэтому анализ **факторов риска (раздел 3.1)** представлен в одном разделе и касается всех новых способов платежей вместе взятых.

68. Риски отмывания денег и финансирования терроризма, связанные с новыми способами платежей, могут быть эффективно снижены за счет использования фирмами своих внутренних мер и процедур в области ПОД/ФТ, а также за счет надзора со стороны регулирующих органов. Как и в случае факторов риска, **меры по снижению рисков**, по всей видимости, аналогичны для всех видов новых способов платежей, и поэтому анализируются в одном разделе **(раздел 3.2)**.

3.1 Факторы риска

Надлежащая проверка клиентов

69. Некоторые предоплаченные карты могут обеспечивать абсолютную анонимности клиента, сохраняя при этом высокую степень своих функциональных возможностей. Например, эмитенты пластиковых карт привлекают клиентов, предлагая анонимные предоплаченные карты с высокими лимитами пополнения и снятия средств или, вообще, без таких лимитов.

	ХОТИТЕ ПОЛУЧИТЬ КАРТУ БЕЗ ПРЕДОСТАВЛЕНИЯ ЗАПОЛНЕНИЯ КАКИХ-ЛИБО ФОРМ ИЛИ ПРЕДОСТАВЛЕНИЯ ДОКУМЕНТОВ?
	Вы можете приобрести уникальную карту «…» прямо сейчас без посредников в тысячах магазинах товаров повседневной необходимости, на которых вы увидите знак «…». Это так же просто, как купить плитку шоколада.

<table>
<tr><td>Мой счет
Регистрация
Зачем покупать карту «…»</td><td>Зачем покупать карту «…»?</td><td>Что представляет собой карта «…»?</td><td>Сколько она стоит?</td><td rowspan="2">Возможность опции пополнения карты здесь</td></tr>
<tr><td>Вопросы и ответы
Прекрасно подходит в качестве подарка</td><td>Идеально подходит в качестве подарка</td><td>Покупайте сейчас</td><td>Покупайте карту «…» в магазинах</td></tr>
<tr><td>Покупайте сейчас</td><td colspan="4">Получение сдачи наличными при оплате покупок картой …
Получайте, пока вы тратите
Нажмите здесь для получения дополнительной информации</td></tr>
<tr><td>Возможность пополнения
Получение сдачи наличными деньгами при оплате картой «…»
Персональные карты
Поддержка розничных продавцов
Карта магазинов
Пресс релизы
Контактная информация
Главная страница</td><td colspan="4">Компания «…» регулируется «…» и является членом «…».</td></tr>
</table>

70. Предоплаченные карты также можно легко передать анонимным третьим лицам, которые в некоторых случаях будут являться их бенефициарными владельцами. В случае, когда выпускаются дополнительные «дубликаты» или «парные» карты, специально рекламируемые и предназначенные для передачи третьим лицам в целях перевода денег, личность таких третьих лиц/ бенефициарных владельцев часто не устанавливается. Это подчеркивает важность идентификации, по крайне мере, основного владельца счета/карты[43].

71. Для большинства провайдеров услуг НСП контакты с клиентом часто сведены к минимуму в связи с тем, что деловые отношения поддерживаются без личного контакта. Как указано в Рекомендации 8 ФАТФ, это повышает такие риски, как использование подложных документов, выдачу клиентом себя за другое лицо или использование продукта третьими лицами для незаконных целей. Отсутствие личного контакта особенно характерно для **провайдеров услуг Интернет-платежей**, которые, в целом, осуществляют большую часть своей коммерческой

[43] Всегда остается возможность использования платежной карты (включая традиционные дебетовые или кредитные карты) совместно с третьими лицами, чьи личности остаются анонимными для учреждения-эмитента карты. Однако, если учреждение надлежащим образом установило личность основного владельца карты, то у сотрудников правоохранительных органов появляется «контакт», который можно связать с сообщениями о подозрительных операциях.

деятельности в Интернете. Это может также относиться и к другим видам новых способов платежей (например, приобретение предоплаченных карт через Интернет).

72. Большинство провайдеров услуг Интернет-платежей запрашивают имена своих клиентов, однако, уровень проверки личности клиента значительно различается, начиная от отсутствия какой либо проверки вообще (некоторые провайдеры требует предоставить только псевдоним), и заканчивая комплексными мерами по проверке личности (см. раздел 3.2 «Меры по снижению рисков»).

73. Проверка и подтверждение личности клиентов может оказаться еще более трудной или вообще невозможной в юрисдикциях, в которых не имеется национальной системы документов, удостоверяющих личность, или иных соответствующих удостоверений личности. С этой проблемой часто сталкиваются провайдеры услуг НСП, работающие в регионах с ограниченными возможностями населения открывать банковские счета, и в, частности, **провайдеры услуг мобильных платежей**. По этой причине Всемирный банк рекомендовал юрисдикциям, стремящимся охватить финансовыми услугами бедные слои населения (например, с помощью провайдеров услуг мобильных платежей), следующее. Если в юрисдикции «национальная инфраструктура удостоверения личности и другие частные базы данных не защищены, и не обеспечена их сохранность, либо доступ к ним со стороны финансовых учреждений для целей проверки личности затруднен и является затратным, государствам следует устранить эти недостатки».[44] В ситуации, когда надлежащая и надежная проверка личности клиента невозможна, может быть, стоит применить альтернативные меры для снижения риска. (Например, установить ограниченные лимиты сумм с тем, чтобы «перевести» продукт в категорию, представляющую «небольшой риск», с возможностью применения упрощенных мер НПК). (См. раздел 3.2 «Лимиты сумм» в качестве меры снижения риска (пункт 112)).

74. При отсутствии идентификации и проверки личности с использованием данных из надежных и независимых источников, провайдеры услуг НСП сталкиваются с риском того, что клиенты могут иметь несколько счетов одновременно без ведома провайдера.

Хранение данных

75. В соответствии с требованиями Рекомендации 10 ФАТФ, как данные по идентификации, так и записи об операциях должны храниться в течение, по крайней мере, пяти лет. Записи об операциях должны быть достаточными для восстановления отдельных операций, чтобы предоставить, если необходимо, доказательства для судебного преследования преступной деятельности. Хотя ни в Рекомендации 10, ни в Пояснительной записке к Рекомендации 10 не дается определения термина «записи об операциях», примеры необходимых записей об операциях приведены в Методологии ФАТФ (10.1.1):

> *«Примеры необходимых элементов записей об операциях включают: имя клиента (и бенефициара), адрес (или иную идентификационную информацию, регистрируемую посредником), характер и дату операции, вид и сумму используемой валюты, а также тип и идентификационный номер любого счета, задействованного в операции».*

[44] «Недопущение отмывания денег и финансирования терроризма – практическое руководство для руководителей надзорных банковских инстанций», Всемирный банк, 2009г., Приложение 1 (Ф1.1), стр.173. Эти рекомендации Всемирного банка основаны и взяты из работы: Х. Бестер, Д. Чанберлейн , Л. де Кокер, С. Хаугаард, Р. Шорт, А. Смит и Р. Уолкер, «Реализация стандартов ФАТФ в развивающихся странах и охват финансовыми услугами бедных слоев населения: проблемы и руководящие указания» (“Implementing FATF Standards in developing countries and financial inclusion: Findings and guidelines”), ПЕРВАЯ инициатива (2008г.); p. xi,; стр. 39, 40.

76. В этих примерах нет явного указания на IP-адреса клиентов, осуществляющих платежные операции с персонального компьютера. Только несколько юрисдикций, регулирующих органов и отраслей выпустили руководящие указания о целесообразности этого[45].

77. Представители правоохранительных органов сообщили о расследованиях дел, в ходе которых выяснилось, что провайдеры хранили недостаточную информацию об IP-адресах или не хранили ее вообще, либо уничтожили (стерли) ее до того, как сотрудники правоохранительных органов смогли получить доступ к таким данным. Повышенный риск ОД/ФТ, связанный с провайдерами, которые не имеют полноценной политики в области хранения данных обо всех операциях, заключается в том, что ненадлежащее хранение записей затрудняет судебное преследование преступников.

Лимиты сумм

78. Термин «лимиты сумм» относится к ограничениям на максимальную сумму, которая может иметься на счету или продукте НСП; либо к ограничениям на максимальную сумму одной платежной операции; либо к ограничениям на частоту или общую сумму разрешенных операций в день/ неделю/ месяц/ год; либо к сочетанию указанных ограничений. Количество счетов или карт, которые может иметь один клиент, также может рассматриваться в качестве одного из видов лимитов сумм.

79. Если лимиты сумм не установлены и ограничения на операции не введены, то доступность средств ограничена только суммой, положенной на счет. Это повышает привлекательность продукта для потенциальных «отмывателей» денег и соответственно увеличивает риск ОД/ФТ, связанный с таким продуктом.

80. Чем больше суммы и/или частота операций, тем выше риск отмывания денег и финансирования терроризма. Кроме того, высокие лимиты сумм, которые разрешено иметь на счету, или отсутствие каких-либо лимитов также повышает риск.

81. Большинство **провайдеров услуг мобильных платежей** устанавливают достаточно низкие (т.е. ограниченные) лимиты сумм для своих продуктов, тогда как в секторе услуг Интернет-платежей и предоплаченных карт можно обнаружить различные подходы. Например, предоплаченные карты могут быть непополняемыми с достаточно небольшой максимальной суммой (100 долларов США); но с другой стороны, существуют пополняемые карты без каких-либо ограничений на лимиты сумм или с достаточно большой максимальной суммой, например 30 000 долларов США в месяц.

Карточка для снятия наличных денег через банкоматы с лимитом в 30 000 долларов США в месяц!

Банковское учреждение, с которым мы работаем, получило указание выпустить ограниченное количество этих уникальных и редких банковских карт, позволяющих снять через банкомат до 30 000 долларов США в месяц. Самое главное это то, что срок действия карты никогда не истекает. Ее можно использовать в любом месте, где имеются логотипы/сеть банкоматов, насчитывающая более 900 000 банкоматов во всем мире. На карте не указывается ваше имя, и для того, чтобы приобрести ее, не требуется никаких удостоверений личности.
Данная карта для снятия денег через банкоматы выпушена финансовым учреждением, предлагающим самые выгодные условия для своих клиентов. Эту уникальную карту можно приобрести за доллары США. Став владельцем карты, вы можете использовать ее в любом уголке мира для осуществления покупок и снятия наличных денег через банкоматы в местной валюте. *(Страница из Интернета, июль 2010г.)*[46]

[45] Например, в Разделе 3, Части II Руководства , выпущенного Совместной руководящей группой по противодействию отмыванию денег (JMLSG) Великобритании, объясняется, как IP-адреса могут стать частью идентификационной информации о клиенте.

82. Провайдеры продуктов с высокими лимитами сумм или без каких-либо лимитов, часто находятся в юрисдикциях, в которых регулирование и надзор за деятельностью провайдеров в плане ПОД/ФТ являются недостаточными или вообще отсутствуют. При этом такие провайдеры торгуют своими продуктами по всему миру (через сеть агентов или через Интернет). В то же самое время таких провайдеров анонимных предоплаченных карт с высокими лимитами сумм или вообще без каких-либо лимитов можно обнаружить и в юрисдикциях, в которых режимы регулирования и надзора, в целом, считаются жесткими.[47] Часто рекламой и продвижением таких анонимных карт занимается само не учреждение-эмитент, а посредники, некоторые из которых специализируются на учреждении и продаже компаний за рубежом, в основном в налоговых гаванях, и таким образом обеспечивают своим клиентам полную анонимность. Однако было установлено, что некоторые из таких анонимных предоплаченных карт являются мошеннической подделкой.

83. Лимиты сумм могут быть увязаны с мерами НПК, принимаемыми в отношении продукта (т.е. при жестких лимитах уровень мер НПК невысокий, а при высоких лимитах или их отсутствии уровень мер НПК высокий). (См. также раздел 3.2 «Меры по снижению рисков», лимиты сумм).

Методы вложения денег

84. Вложение денег для целей использования новых способов платежей может быть осуществлено различными способами, в том числе и анонимно, посредством наличных денег, денежных переводов или перевода средств с других анонимных продуктов, также используемых для новых способов платежей. При использовании анонимных методов вложения денег может не остаться никаких документальных свидетельств, касающихся операции по вложению средств и происхождения вкладываемых денег, либо такие документальные свидетельства могут оказаться недостаточными.

85. Метод вложения наличных денег является особенно популярным среди провайдеров услуг НСП, продающих предоплаченные продукты через агентов-распространителей (например, предоплаченные карты и денежные сертификаты, продаваемые розничными торговцами, или предоплаченные средства для мобильных платежей, продаваемые в салонах связи).[48] Вложение наличных денег через агентов-распространителей может увеличить риск ОД/ФТ, особенно в ситуации, когда продавцы не имеют обязательств по надлежащей проверке клиентов и не прошли достаточного обучения в области соблюдения требований ПОД/ФТ.

86. Помимо ситуации, связанной с вложением денег из анонимных источников, риск ОД/ФТ также возрастает в случае, если средства поступают из различных источников, в том числе от третьих лиц. Например, в случае сотрудничества с компаниями, предоставляющими услуги денежных переводов, такие компании могут быть использованы для перевода средств не только на личные счета клиентов, но и на счета третьих лиц.

---

[46] Как отмечалось выше, некоторые предложения и реклама анонимных предоплаченных карт являются мошенничеством. Рабочая группа по проекту не выясняла, является ли продукт, рекламируемой на этой странице из Интернета, случаем мошенничества.

[47] В 2007 году Федеральное управление уголовной полиции (BKA) ФРГ провело специальное расследование, касающееся платежных карт. В ходе расследования сотрудники управления выявили шесть случаев продажи анонимных предоплаченных карт через Интернет, причем банки-эмитенты таких карт располагались в Европе и Центральной Америке.

[48] В регионах с неразвитой банковской инфраструктурой, в которых только небольшое количество клиентов имеет банковские счета, и где предполагается, что услуги НСП (часто услуги мобильных платежей) помогут компенсировать отсутствие банковских счетов, могут использоваться другие методы вместо вклада наличных средств.

87. Поскольку большинство услуг Интернет-платежей и мобильных платежей основано на наличии соответствующих счетов, еще одна возможность «непрямого вклада денег» появляется в ситуации, когда провайдер услуг позволяет осуществлять переводы средств между физическими лицами в рамках системы. В этих случаях ограничения, установленные провайдером на вложение денег, можно обойти путем использования наличных денег для помещения их на счет через пункт по обмену электронных валют (или иных третьих лиц), который затем переведет средства на счет клиента.

Регистрация Главная страница О нашей компании Наши ставки Правила обмена Контакты Есть Вопрос? нажмите *(Страница из Интернета, май 2010г.)*	**ОБМЕН WEBMONEY, PAYPAL EPASSPORTE, MONEYBOOKERS** Обменный курс: Евро/Доллар США = 1,336; Доллар США/Евро = 0,749 Сумма обмена 1000 Webmoney WMZ Вам нужно иметь ? Вам необходимо: Комиссия: Webmoney WMZ Webmoney WMR Вы имеете: Webmoney WME PayPal Счет электронных ePassporte денег, на который VoneyBookers следует перевести средства ? Ваше имя: Адрес вашей электронной почты ? Наша контактная информация: Icq Дополнительная информация: Я согласен с правилами перевода средств Отправка заявки

88. Поскольку у различных провайдеров услуг НСП имеются разные методы вложения и снятия средств, пункты обмена электронных валют позволяют клиентам обойти установленный порядок путем простого конвертирования денежных средств в более подходящую валюту провайдера.

Географические ограничения

89. Чем более широко распространены продукты, связанные с новыми способами платежей, в географическом плане, тем выше риск ОД/ФТ. Возможность осуществления трансграничных операций делает услугу более привлекательной для преступных элементов, занимающихся отмыванием денег. Это также позволяет провайдерам платежных услуг вести свою деятельность из юрисдикций, в которых на них могут не распространяться меры надлежащего регулирования и надзора в сфере ПОД/ФТ, и где они могут находиться вне досягаемости для расследований, проводимых зарубежными правоохранительными органами.

90. Хотя многие провайдеры услуг платежей, предлагающие трансграничные услуги, могут надлежащим образом сотрудничать со своими национальными надзорными и правоохранительными органами, некоторые провайдеры могут отказаться предоставлять информацию зарубежным органам или быть не в состоянии сделать это вследствие законодательных препон. Направление официальных запросов об оказании правовой помощи может занять очень много времени и часто не имеет шансов на успех. В результате этого некоторые органы могут не обращаться за правовой помощью и просто закрывать расследования. Ситуация становится еще более проблемной в случае, когда услуга предоставляется совместно несколькими провайдерами, находящимися в разных юрисдикциях (см. «сегментация услуг», пункт 96).

91. Предоплаченные карты многоэмитентных (открытых) систем могут использоваться для быстрого перевода денег по всему миру путем использования банкоматов для снятия средств, и при этом не требуется осуществлять операции, предусматривающие личный контакт. Мировые сетевые провайдеры (VISA, MasterCard) могут ограничить использование предоплаченных карт определенными юрисдикциями или регионами, но большинство бизнес моделей предоплаченных карт многоэмитентных (открытых) систем созданы для функционирования в глобальном масштабе. Хотя система банкоматов и не была изначально предназначена для использования в качестве системы перевода денег между физическими лицами, в настоящее время она рекламируется в качестве таковой.

Почему стоит посылать деньги с помощью карты «…»?	Для поиска распространителей денежных карт в Мексике нажмите здесь
Мгновенный перевод через **31 000** банкоматов в Мексике! Вы получаете полную сумму в песо **без КАКОЙ-ЛИБО дополнительной комиссии**	
Выгодные ставки! Очень выгодные ставки **без каких-либо скрытых комиссионных сборов** для вас или для лица, которому вы посылаете деньги.	
Возможность быстрой покупки – без заполнения сложных форм в США и Мексике **в любое время каждый день!**	
Простой доступ – можно снять деньги через банкоматы в Мексике в любой день и любое время!	
	Выгода для вас и вашей семьи: Мгновенный перевод! Возможность мгновенно перевести/снять деньги через банкоматы! Никаких комиссий за использование банкоматов! Работает круглосуточно – даже в праздники! Безопасно! Надежно! Никаких очередей! Никаких агентов!
Простота приобретения в розничной сети – Отправленные деньги получаются через банкоматы	
Карта «…» является превосходной альтернативным решением вместо существующих устаревших услуг телеграфных переводов, которые являются медленными, дорогими, неудобными, небезопасными и	Mand dincro a Mecxico

ненадежными как для отправителя, так и для получателя. В отличие от этого карта «…» является простым продуктом, который можно купить и активировать в розничной сети. *(Страница из Интернета, август 2010г.)*	

92. Провайдеры услуг Интернет-платежей (УИП) могут располагаться или получить лицензию на свою деятельность в юрисдикциях, отличных от тех, в которых находятся их клиенты. Поскольку в сфере услуг Интернет-платежей могут использоваться различные методы перевода денег, и платежи могут, в принципе, отправляться и получаться в любой точке мира. Большинство провайдеров УИП предлагают свои услуги в глобальном масштабе, обеспечивая, таким образом, осуществление трансграничных переводов.

93. Большинство провайдеров услуг мобильных платежей изначально были ориентированы на обеспечение переводов средств только внутри страны. Однако сейчас все большее число провайдеров предлагает возможность осуществлять трансграничные переводы между конкретными странами за счет открытия, так называемых, «платежных коридоров» (например, между Великобританией и Кенией или между Филиппинами и Малайзией). Несмотря на попытки внедрения международных моделей в секторе мобильных платежей, в настоящее время еще не существует, по настоящему, глобального провайдера услуг мобильных платежей.

94. Несмотря на это, некоторые провайдеры услуг мобильных платежей расширили охват своих услуг за счет подсоединения к глобальной сети банкоматов (выдавая свои клиентам предоплаченные карты) или путем сотрудничества с мировыми компаниями, предоставляющими услуги денежных переводов. Благодаря этому провайдер услуг, изначально работавший на только внутреннем рынке, может обеспечить осуществление трансграничных переводов средств из и в свою юрисдикцию.

Ограничения использования

95. Ограничения использования продуктов, связанных с новыми способами платежей, могут различаться в зависимости от конкретного продукта и провайдера услуг. Продукты, предназначенные для новых способов платежей, с ограниченными возможностями использования подвержены меньшим рискам в плане ОТ/ФТ, нежели продукты, дающие клиентам возможность их более широкого применения.

96. Предоплаченные карты многоэмитентных (открытых) систем, особенно, когда речь идет об устоявшемся и широко распространенном техническом стандарте (VISA, MasterCard), в целом имеют наименьшие ограничения по использованию, поскольку активно применяются в существующей широко развитой системе платежных операций, включая глобальную сеть банкоматов и очень большое количество продавцов/ торговых точек, принимающих их к оплате.

- Возможность приема к оплате (прием продавцами)

  Предоплаченные карты «VISA» и «MasterCard» принимаются к оплате национальными и зарубежными продавцами, входящими в платежную сеть «VISA» или «MasterCard». Поскольку стандарты, касающиеся платежей с помощью предоплаченных карт, обычно в основном схожи[49] со стандартами, касающимися платежей с помощью обычных дебетовых или кредитных карт, такие предоплаченные карты принимаются в качестве средства платежа

[49] Существуют меры контроля, которые страны или учреждения могут применять с целью недопущения использования карт для определенных покупок; либо для недопущения их использования в банкоматах; либо которые могут ограничить суммы операций и т.д. Поэтому возможности предоплаченных карт могут быть разными и не обязательно совпадать с возможностями кредитных карт.

почти везде, где для оплаты принимаются кредитные карты (при условии, что сумма предоплаченных средств достаточна для осуществления соответствующего платежа), включая Интернет-магазины.

В случае провайдеров услуг Интернет-платежей и мобильных платежей платежные операции часто могут осуществляться только между клиентами одного и того же провайдера УИП. Платежные услуги, принимаемые широким кругом торговых точек, будут более привлекательны для преступников, занимающихся отмыванием денег, нежели услуги, позволяющие тратить деньги только у ограниченного круга продавцов.

На некоторых рынках услуги мобильных платежей используются исключительно для осуществления микроплатежей (например, для приобретения билетов на общественный транспорт, для оплаты покупок через торговые автоматы, для оплаты мелодий звонка мобильного телефона). В связи с этим количество продавцов принимающих такие платежи ограничено. На других рынках, где услуги мобильных платежей могут быть использованы в качестве альтернативы банковским счетам и телеграфным денежным переводам, круг продавцов, принимающих такие платежи гораздо шире, что приводит к повышенному риску.

- Возможность использования для осуществления различных операций

Для осуществления платежа с использованием стандартной предоплаченной карты получатель должен иметь соответствующее техническое оборудование (считыватель карт, Интернет-доступ в систему). Поэтому большинство получателей платежей с использованием карт являются компаниями (платежи физических лиц в пользу компаний). Однако, если предоплаченные карты позволяют получать платежи/денежные средства, отправляемые из внешних источников, или, если карты или конкретные «дубликаты» карт могут передаваться третьим лицам или использоваться для вложения денег на счета НСП, то могут также осуществляться платежи между физическими лицами.

Большинство услуг Интернет-платежей и мобильных платежей предусматривают осуществление платежей между физическими лицами, но некоторые услуги обеспечивают возможность платежей физическими лицами в пользу компаний, правда, только при совершении соответствующих покупок (например, денежные сертификаты). В этих случаях общий риск отмывания денег и финансирования терроризма является низким. Однако, когда «продавцы»[50], принимающие такие платежи, используются для оказания финансовых услуг (например, компания, оказывающая услуги денежных переводов, принимает такие способы платежей в качестве метода вложения денег) или для преступных целей (например, владельцы незаконных сайтов азартных игр в Интернете принимают такой способ платежей), риск отмывания денег и финансирования терроризма остается высоким.

- Снятие денег

Наличные деньги можно снять с многих предоплаченных карт многоэмитентных (открытых) систем через сети банкоматов. Кроме того, в некоторых юрисдикциях торговые точки могут быть легко использованы для снятия наличных денег путем переплаты за покупку и получения сдачи наличными деньгами (получение сдачи наличными при оплате картой).[51] Простота снятия наличных денег и широкий круг продавцов, принимающих предоплаченные карты, а также тот факт, что предоплаченные карты[52] гораздо более удобны для перевозки, по сравнению с наличными деньгами (карта для совершения финансовых операций, соответствующая стандарту ИСО, может быть гораздо более компактной, нежели наличные

[50] Этот термин гораздо шире и включает не только классические Интернет-магазины.
[51] Такой способ снятия денег путем получения сдачи наличными был изначально предназначен и используется повсеместно для обычных кредитных или дебетовых карт.
[52] Карта часто используется в качестве устройства доступа для снятия денег и осуществления платежей.

деньги[53]), может сделать предоплаченные карты удобной заменой наличных денег в схемах контрабанды наличности в целях отмывания денег[54], при условии высокого лимита суммы и/или отсутствия проверки личности клиента.

Большинство провайдеров услуг Интернет-платежей и мобильных платежей ограничивают возможность снятия денег таким же образом, как вводят ограничения на использование методов вложения денег. Например, снятие денег может быть ограничено только возможностью перевода средств на счет, открытый на имя клиента в кредитном или финансовом учреждении.

В случаях, когда наличные используются в качестве метода вложения средств, обычно также имеется возможность снятия наличных денег со счета мобильных платежей, т.е. через агентов. Это не только повышает риск отмывания денег и финансирования терроризма, то также может создать дополнительные трудности для провайдера услуг мобильных платежей. Например, были сообщения о мошенничестве агентов или о проблемах достаточной кассовой наличности при поступлении запросов о снятии денег.

Провайдеры могут обеспечить выдачу наличных денег за счет сотрудничества с компаниями, оказывающими услуги денежных переводов, или с офисными пунктами обмена, которые могут приобрести электронные деньги за наличные. Некоторые провайдеры услуг Интернет-платежей и мобильных платежей предлагают положить деньги на предоплаченную карту, предоставляя, таким образом, своим клиентам возможность снять наличные через глобальную сеть банкоматов. Один провайдер услуг мобильных платежей (совместно с банком, осуществляющим деятельность в его стране), даже, обеспечил возможность снятия денег через банкоматы этого банка без необходимости для клиента иметь банковский счет и предоплаченную карту. Клиенту, по требованию, выдается одноразовый код авторизации, который он (или третье лицо) может ввести в банкомат вместе с номером телефона клиента и суммой, которую он хочет снять.[55]

Сегментация услуг

97. Новые способы платежей могут быть подвергнуты большему риску, если в оказании услуг одновременно принимают участие несколько сторон, например, эмитенты карт, управляющие программами, пункты обмена валют, дистрибуторы и другие посредники или агенты. Чем больше таких лиц, тем выше риск сегментации и потери информации. Проблема может стать еще серьезнее, если важные услуги передаются на аутсорсинг потенциально нерегулируемым третьим лицам, не имеющим четкой ответственности и надзора или расположенным за рубежом. Платежные схемы с высокой степенью сегментации могут создать проблемы для регулирующих органов в плане компетенции, международного сотрудничества, полномочий и средств эффективного надзора и контроля таких схем.

98. Провайдеры часто используют **агентов** не только для осуществления операций по приему и выдаче наличных денег, но и для установления отношений с новыми клиентами. В большинстве юрисдикций агенты, не являющиеся кредитными или финансовыми учреждениями, сами по себе не имеют обязательства в сфере ПОД/ФТ. В рамках правовой и регулирующей системы ответственность за выполнения требований в сфере ПОД/ФТ, установленных в законодательстве или регулирующих актах, лежит на провайдере услуг НСП. Это означает, что Провайдер несет

[53] Объем «карты для совершения финансовых операций», соответствующей стандарту ИСО, составляет 3 525,8 кубических миллиметров. Объем банкноты достоинством 20 евро составляет 1 435,6 кубических миллиметров, а объем банкноты номиналом 20 долларов США составляет 1 129 кубических миллиметров. Таким образом, карта, позволяющая снять только 100 евро или 100 долларов уже значительно компактней по сравнению с пятью банкнотами по 20 евро или пятью 20-долларовыми банкнотами.
[54] См. главу 4.4, пункт 132.
[55] Cf. www.finextra.com/news/fullstory.aspx?newsitemid=20963.

ответственность за невыполнение агентом обязательств провайдера, касающихся вопросов ПОД/ФТ («риск, связанный с агентами»).[56] Таким образом, провайдер должен убедиться в том, что агент выполняет свои функции эффективно и надлежащим образом. С учетом большого количества агентов, на которых приходится полагаться ряду провайдеров (например, сотни отделений крупной розничной компании), это может оказаться непростым делом, особенно, если агенты находятся в зарубежной юрисдикции, либо, возможно, если агент сам использует услуги других агентов («субагентов»).[57]

99. Если провайдер сотрудничает с компаниями, оказывающими услуги денежных переводов, то последние обычно используются для осуществления операций по вложению и/или снятию наличных денег. Это может, в некоторой степени, повысить уровень выполнения требований в области ПОД/ФТ, поскольку в большинстве юрисдикций на компании, оказывающее услуги денежных переводов, распространяются меры регулирования и надзора в сфере ПОД/ФТ. Однако регулирующие требования могут различаться: для компаний, оказывающих услуги денежных переводов, операция, осуществляемая клиентом, является единичной, тогда как для провайдера услуг НСП такая операция является частью постоянных деловых отношений с клиентом. Более того, риск может возрасти, если компания, оказывающая услуги денежных переводов, с которой осуществляется взаимодействие, расположена в юрисдикции, в которой не применяются аналогичные стандарты в области ПОД/ФТ.

100. Особое явление, касающееся сегментации услуг, связано с определенным видом провайдеров услуг Интернет-платежей, так называемыми провайдерами электронных денег, которые используют «пункты обмена валют» в качестве составной части цепочки платежной операции. Поскольку провайдеры электронных денег не выдают «электронные деньги» напрямую своим клиентам/владельцам счетов, они также не получают эквивалентные суммы денег от клиентов. Вместо этого клиенты приобретают их электронные деньги в пунктах обмена электронных валют, которые затем переводят приобретенную сумму электронных денег на счет клиента у провайдера услуг электронных денег. Некоторые пункты обмена электронных валют являются дочерними предприятиями провайдеров электронных денег, но многие являются законными независимыми компаниями или физическими лицами. Пункты обмена электронных валют могут иметь офис (т.е. осуществлять обмен наличных денег и других традиционных платежных инструментов на электронную валюту и обратно). Однако они также могут быть в чистом виде Интернет-компаниями (осуществляющими обмен переведенных электронным методом денег на электронную валюту, либо обмен электронной валюты на другую электронную валюту или на средства для Интернет-платежей).

3.2 Меры по снижению риска

101. Также как и в случае любого финансового продукта, риск отмывания денег и финансирования терроризма, связанный с новыми способами платежей, возрастает при отсутствии соответствующих мер контроля. Однако имеются эффективные меры по снижению риска, которые могут существенно уменьшить выявленные риски.

102. Приведенные ниже меры по снижению риска следует рассматривать не по отдельности, а как единой целое; некоторые из них имеют отношение сразу к несколькими факторами риска. Для эффективной оценки риска, сопряженного с конкретным продуктом, использующимся в области новых способов платежей, важно иметь перед глазами общую картину, включая все факторы риска и все меры по снижению рисков.

---

[56] Термин «риск, связанный с агентами» взят из документа ФАТФ «Основанный на оценке риска подход: Руководство для компаний, оказывающих денежные услуги», июль 2009г., стр.32.

[57] Хотя такое явление как субагенты пока не отмечено в сфере деятельности провайдеров услуг НСП, использование субагентов является очевидным фактом, который отмечен в последнем отчете по типологиям, касающимся компаний, оказывающих денежные услуги, подготовленном рабочей группой ФАТФ по типологиям.

Меры по идентификации и проверки личности

103. Меры по идентификации и проверке личности позволяют фирмам понять, кем является их клиент и, при необходимости, кем является бенефициарный владелец. Это является важным, поскольку такая информация формирует основу для постоянного мониторинга деловых отношений. Это также дает фирмам возможность проверить, что клиент является тем, за кого он себя выдает, выяснить, имеются ли у клиента несколько счетов (или карт или денежных сертификатов), а также вести записи и хранить документальные свидетельства, необходимые для правоохранительных органов.

104. В случае продуктов и услуг, реализуемых через Интернет, адрес протокола сети Интернет (IP-адрес) должен являться частью идентификационной информации, собираемой и хранимой провайдером. Наличие информации об IP-адресе может помочь минимизировать возможность клиента иметь несколько счетов, даже, если они являются анонимными.

105. В некоторых юрисдикциях провайдеры освобождены от обязанности принимать меры по надлежащей проверке клиентов в ситуациях, когда риск отмывания денег и финансирования терроризма считается небольшим. Иногда провайдеры освобождаются от этой обязанности при условии введения низких лимитов сумм и пороговых уровней на суммы операций. В некоторых юрисдикциях провайдеры услуг НСП освобождаются от обязанности принимать меры НПК в случае одноразовых операций. В таких случаях очень важно, чтобы учреждения имели системы, позволяющих выявить наличие у клиента нескольких карт или счетов, что может указывать на попытку клиента обойти меры НПК путем размещения денег в нескольких продуктах, представляющих «невысокий риск».

106. В случае проверки личности без личного контакта важно, чтобы фирмы использовали соответствующие меры проверки для того, чтобы убедиться, что клиент является тем, за кого он себя выдает. Такие меры проверки включают, но не только: переписку с клиентом по проверенному домашнему адресу; требование об осуществлении первого платежа через счет, открытый на имя клиента в регулируемом кредитном учреждении, расположенном в юрисдикции, выполняющей требования ФАТФ; требование заверки копий документов соответствующим лицом.[58] Дополнительные проверки для исключения возможного обмана (например, использование кодов, изменяющихся при проведении каждой отдельной операции или при осуществлении каждого Интернет-платежа), либо проверки биометрических данных (например, использования систем распознавания отпечатков пальцев и голоса)[59] могут повысить эффективность политики в области противодействия отмыванию денег. Такие дополнительные проверки также могут помочь не допустить незамеченного открытия одним клиентом нескольких счетов.

107. Если провайдеры услуг платежей использует третьих лиц для установления контакта с клиентами, а также для приема и выдачи наличных денег (например, розничных торговцев или компании, оказывающие услуги денежных переводов), фирмы могут снизить риск путем обеспечения компетентности и надлежащего обучения таких третьих лиц в области выполнения требований ПОД/ФТ. Кроме того, предпочтительно, чтобы на деятельность указанных третьих лиц распространялись меры регулирования и надзора в юрисдикции, в которой действуют стандарты регулирования в области ПОД/ФТ.

108. В случае, когда новые способы платежей могут использоваться для перевода денег между физическими лицами, провайдеры могут снизить риск путем обеспечения того, чтобы получатель

[58] Документ Базельского комитета о надлежащей проверке клиентов, октябрь 2001г., пункт 2.2.6; Руководство совместной координационной крупы по вопросам отмывания денег, 2010г., Часть I, Глава V.
[59] Рабочий документ Всемирного банка №174: «Новые технологии, новые риски? Инновации и противодействие финансированию терроризма», 2009г.

не оставался анонимным, а также за счет ведения мер контроля, аналогичных тем, которые должны использовать фирмы, осуществляющие телеграфные переводы.

Мониторинг

109. Поскольку новые способы платежей основаны на компьютерных технологиях, имеются достаточные условия для осуществления эффективного мониторинга и направления сообщений. Операции, осуществляемые с помощью услуг новых способов платежей, всегда оставляют «электронные след», который можно контролировать и анализировать, даже, если провайдер услуг НСП освобожден от обязанности принимать меры НПК (т.е. клиент остается анонимным). Это означает, что провайдеры могут заблокировать счет в случае выявления необычных схем операций, либо в случае возникновения у них подозрений о возможном использовании продукта в целях отмывания денег и/или финансирования терроризма.

110. Системы мониторинга могут быть весьма эффективными инструментом снижения риска использования продукта, связанного с новыми способами платежей, для совершения финансовых преступлений.

Для того чтобы быть эффективными, такие системы должны, как минимум, обеспечивать возможность выявления:

- Расхождений, например между предоставленной клиентом информацией и IP-адресом
- Необычных или подозрительных операций
- Случаев использования одного и того же счета несколькими пользователями
- Случаев использования одним и тем же пользователем нескольких счетов
- Случаев вложения денег в несколько продуктов из одного и того же источника

111. Если провайдеры определенных продуктов освобождены от обязанности принимать меры НПК, системы должны быть в состоянии определить момент, когда клиент «приближается» к установленному лимиту (будь то лимит на продукт/операцию, либо общий лимит), после которого должны применяться меры надлежащей проверки клиента в полном объеме.

112. Эффективные системы мониторинга также являются основой для своевременного направления сообщений провайдерами услуг НПС, которые обязаны направлять СПО.

Лимиты сумм

113. Лимиты на остаток средств на счету и на суммы операций, а также ограничения на частоту совершения операций могут перекрыть постоянный доступ преступным элементам к крупным суммам денег для использования их в незаконных целях. При применении основанного на оценке риска подхода лимиты сумм могут устанавливаться, исходя из потребностей и рисков, сопряженных с каждым сектором рынка и продуктом, связанным с новыми способами платежей. Например, если услуга связана с полностью идентифицированным и проверенным банковским счетом или счетом кредитной карты, то лимиты сумм операций могут не устанавливаться, но в случае сниженных требований по идентификации будут установлены низкие лимиты на сумму операций или услуг.

114. Если на провайдеров услуг НСП распространяется действие режима регулирования и надзора в сфере ПОД/ФТ, то при применении основанного на оценке риска подхода им не требуется применять меры по проверке личности клиента в полном объеме (достаточно применять «упрощенные или сокращенные меры НПК»). Это могут быть сокращенные обычные меры НПК или полное освобождением от обязанности применения мер НПК.[60] Лимиты сумм нередко

[60] См. главу 5.2 («Освобождение от обязательств, касающихся ПОД»), пункт 162

являются определяющим фактором при решении вопроса, можно ли считать продукт представляющим «невысокий риск» и, следовательно, можно ли применять упрощенные меры НПК.

115. Лимиты сумм и ограничения на сумму операций могут быть очень эффективными мерами по снижению риска, поскольку они делают продукт менее привлекательным для преступных элементов, занимающихся отмыванием денег. Они особенно действенны в сочетании с эффективными системами мониторинга и процедурами, не допускающими покупки одним клиентом нескольких карт на мелкие суммы денег или открытия нескольких счетов на небольшие суммы денег. К примеру, ограничительные лимиты сумм, установленные большинством провайдеров услуг мобильных платежей, называются одной из главных причин выявления на сегодняшний день очень небольшого количества случаев отмывания денег с помощью мобильных платежей.

116. Одна из проблем при установлении лимитов сумм связана с определением соответствующего порогового уровня, который может рассматриваться как представляющий невысокий риск. Различные юрисдикции и провайдеры услуг пришли к разным заключениям на счет того, какие пороговые значения могут считаться представляющими «невысокий риск».[61] Однако небольшие суммы операций, которые могут отбить интерес у преступных элементов, занимающихся отмыванием денег, могут в то же самое время оставаться привлекательными для целей финансирования терроризма, поскольку считается, что в этих операциях, в целом, задействованы меньшие суммы, нежели в схемах отмывания денег.

Методы вложения денег

117. Риск отмывания денег, связанный с анонимными методами вложения средств, может быть снижен путем ограничения методов вложения денег источниками, при использовании которых провайдеры могут полагаться на меры НПК, применяемые другими учреждениями, например, ранее идентифицированными банковскими счетами, кредитными или дебетовыми картами или другими персонализированными методами платежей.[62] Хотя исключение возможности использования наличных денег или иных анонимных источников в качестве метода вложения денег существенно снижает риск, это может оказаться невыполнимым на тех рынках, на которых провайдеры услуг НСП являются единственным доступом к финансовой системе для большой части населения, имеющего ограниченные возможности открывать банковские счета. (Например, услуги мобильных платежей в юрисдикциях со слабой банковской инфраструктурой).

118. Эмитенты, вводящие ограничения на методы вложения денег, должны быть в состоянии выявлять случаи непрямого вложения денег через третьих лиц (например, через пункты обмена валют) за счет осуществления тщательного мониторинга. Они также могут еще более снизить риск ОД/ФТ не только путем запрета метода вложения денег, но и за счет введения ограничений на количество лиц, которым разрешено вкладывать деньги в продукт (например, в случае предоплаченных карт это может быть только владелец карты, либо сотрудник компании в случае карты, на которую перечисляется заработная плата), ограничивая, таким образом, возможность вложения денег третьими лицами.

4. Типологии и ситуационные исследования

119. В 2006 году после опубликования отчета ФАТФ, касавшегося новых способов платежей, потенциальная возможность использования новых способов платежей для незаконных целей была уже очевидна. Однако в то время было мало свидетельств, подтверждающих это. С тех пор

[61] См. главу 5.2 («Определение случаев, представляющих невысокий риск»), пункт 160

[62] Это не то же самое, что «полагаться», как установлено в Рекомендации 9 ФАТФ, и само по себе, вряд ли, является выполнением требования Рекомендации 5, касающегося использования надежного и независимого источника для проверки личности клиента.

доступность и использование новых способов платежей увеличились, так же как выросло количество случаев их использования для незаконных целей (особенно это касается предоплаченных карт и услуг Интернет-платежей), что подтверждается приведенными ниже ситуационными исследованиями. При этом следует отметить, что большинство ситуационных исследований касается отмывания денег. Только в нескольких отдельных случаях имеются подозрения на связь с финансированием терроризма, хотя было установлено, что новые способы платежей также уязвимы с точки зрения финансирования терроризма.[63]

120. В ситуационных исследованиях приведены следующие типологии: 1) Вложение денег третьими лицами (включая фиктивных и подставных лиц); 2) Использование безличного характера счетов для использования новых способов платежей; и 3) Провайдеры услуг новых способов платежей или их сотрудники, являющиеся соучастниками преступных схем. Порядок представления типологий основан на следующем: все виды новых способов платежей, используются для этого, или два вида НСП используются в этих целях, или хотя бы один вид НСП используется таким образом.

121. Рабочая группа по проекту пришла к выводу о нецелесообразности представления четвертой типологии «анонимность». Хотя во многих ситуационных исследованиях используется возможность сохранить анонимность, только в трех случаях (***примеры 8, 10 и 31***) были использованы продукты, связанные с НСП, которые обеспечили «непосредственную» анонимность, т.е. не требовалось никаких мер идентификации/проверки личности. Ряд других случаев, в которых использованные продукты могли обеспечить «косвенную» анонимность, представлены в других трех типологиях (например, подставные лица, украденные или поддельные данные клиентов или манипулирование данными в Интернете). Как таковая, «анонимность» может быть общей проблемой, связанной с новыми способами платежей, но она является слишком расплывчатой для того, чтобы выделять ее в отдельную типологию.

4.1 Типология 1: Вложение денег третьими лицами (включая фиктивных и подставных лиц)

122. Вложение денег на счета НСП может осуществляться анонимно, если это позволяет конкретная бизнес модель.

123. Средства на предоплаченные карты можно вкладывать наличными деньгами, с помощью банковских переводов и посредством переводов денег между физическими лицами. Клиенты провайдеров услуг Интернет-платежей также могут осуществлять переводы денег между физическими лицами. Такие методы вложения денег могут позволить третьим лицам, являющимся соучастниками, вносить деньги на предоплаченные карты или счета Интернет-платежей добровольно (например, в качестве оплаты на нелегальные товары или азартные игры, см. примеры 1-3 и 6).[64] В то же самое время такие методы платежей могут также использоваться мошенниками для получения денег от ничего не подозревающих жертв их преступной деятельности. В таких случаях бывает очень трудно провести грань между предикатным преступлением и последующим этапом размещения денег для целей отмывания. В девяти ситуационных исследованиях приведены примеры того, как вложение средств на предоплаченные карты и счета Интернет-платежей через третьих лиц может использоваться для целей отмывания денег.

---

[63] Целевая группа ООН по осуществлению контртеррористических мероприятий: Отчет рабочей группы «Борьба с финансированием терроризма» (октябрь 2009г.), стр.14; а так же см. рабочий документ Всемирного банка №174«Новые технологии, новые риски? Инновации и противодействие финансированию терроризма», 2009г.

[64] Представители Евроюста также указали на то, что новые способы платежей часто используются для покупки или продажи в Интернете детской порнографии с тем, чтобы не привлекать внимание государственных органов. В настоящее время Европейская финансовая коалиция по борьбе с детской порнографией в Интернете (EFC) находится в контакте с определенным числом таких провайдеров услуг НСП.

124. Также как и в случае провайдеров услуг Интернет-платежей и предоплаченных карт, услуги мобильных платежей дают возможность вложения денег третьими лицами, что может быть использовано преступными элементами для незаконных целей. В трех случаях преступники использовали возможность перевода денег между физическими лицами, предоставленную провайдером мобильных платежей, для пополнения своих счетов. Во всех трех случаях имел место обман или введение в заблуждение третьих лиц, которые отправляли свои деньги преступникам. Это привело к тому, что использование провайдера услуги мобильных платежей также стало частью предикатного деяния. Однако следует отметить, что суммы, фигурирующие в этих примерах, оказались небольшими.

125. Также имеются свидетельства того, что, даже, жесткие требования по идентификации и проверке личности можно обойти за счет использования третьих сторон в качестве подставных лиц или финансовых агентов.

a. Предоплаченные карты:

Пример 1: Отмывание доходов от незаконной торговли стероидными препаратами в Интернете

В 2007 году имело место три случая, в которых фигурировали в общей сложности семь обвиняемых, которым были предъявлены обвинения в незаконной продаже через Интернет стимуляторов, таких как гормонов роста человека и анаболических стероидов, и отмывании полученных доходов. Во всех трех случаях, в качестве одного из способов платежей при продаже незаконных веществ через Интернет использовался перевод денег на предоплаченные карты обвиняемых. В одном случае обвиняемый заработал 60 000 долларов США за 11 месяцев, осуществляя незаконную торговлю стероидами в Интернете. В другом случае обвиняемый отмыл, порядка, 125 000 долларов США в течение 21 месяца с помощью предоплаченных карт. Во всех трех случаях обвиняемые признали свою вину и были приговорены к различным срокам тюремного заключения.
Источник: США

Пример 2: Отмывание доходов от запрещенных азартных игр с использованием предоплаченных карт

В 2007 году нескольким обвиняемым были предъявлены обвинения в организации незаконных азартных игр. Организация включала агентов, находящихся в США, которые занимались привлечением игроков, сбором проигранных денег и распределением выигрышей, а также организацию, находившуюся за пределами США, занимавшаяся управлением Интернет-сайтом, на котором обрабатывались ставки и устанавливались коэффициенты выигрышей.
Одним из способов, использовавшихся для перевода доходов от незаконной игорной деятельности между агентами, находившимися в США, и организаторами, расположенными за пределами США, было открытие и пополнение счетов предоплаченных карт в Соединенных Штатах. После этого информация с карты (номер карты, срок действия карты и код проверки подлинности карты) посылалась операторам Интернет-сайта. При этом сами карты оставались в США. Вместо непосредственного использования карты организаторы, находившиеся за рубежом, использовали счета карт для совершения покупок через Интернет или по телефону. Доход от этой незаконной деятельности по организации азартных игр в Интернете составлял около 100 000 долларов США в месяц.
Шесть обвиняемых признали свою вину в организации незаконных азартных игр и были приговорены к трем годам лишения свободы условно. Один обвиняемый признал себя виновным в организации незаконных азартных игр и отмывании денег и был приговорен к трем годам лишения свободы условно и шести месяцам домашнего ареста. Один обвиняемый признал себя виновным в преступном сговоре и был приговорен к четырем годам лишения свободы условно. Один обвиняемый признал себя виновным в контрабанде наличных денег и был приговорен к четырем месяцам тюремного заключения и трем годам лишения свободы условно.

Источник: США

Пример 3: Оплата за наркотики с использованием предоплаченных карт

В 2009 году нескольким обвиняемым были предъявлены обвинения в организации сети распространения наркотиков в федеральной тюрьме и получении оплаты за пределами тюрьмы посредством использования предоплаченных карт. Члены преступной группировки, находившиеся на свободе, открыли счета предоплаченных карт на имя обвиняемых, которые, по утверждению стороны обвинения, сообщили своим клиентам – другим заключенным, что оплата за наркотики должна производиться членами их семей путем помещения денег на счета предоплаченных карт обвиняемых. Обвиняемые пока не предстали перед судом.
Источник: США

Пример 4: Возможное использование предоплаченных карт для целей финансирования терроризма

В данном случае отец и сын, подозреваемые в осуществлении деятельности по переводу денег, имели множество предоплаченных карт, на которых ежедневно поступали деньги со всей Италии. Вскоре после поступления денег они снимались с предоплаченных карт таким образом, что остатки на счетах карт приближались к нулю. Часть денег, снятых с предоплаченных карт, переводилась на банковский счет отца. Помимо этого деньги на этот счет также поступали от пакистанцев. Деньги, находящиеся на счету, в дальнейшем использовались для осуществления кредитовых переводов. Было установлено, что отец и сын имеют отношение к террористическому акту, совершенному в Мумбаи в 2008 году.
Источник: Италия

Пример 5: Использование предоплаченных карт для отмывания доходов от торговли наркотиками

После передачи в правоохранительные органы полученных сообщений о подозрительных операциях, внимание сотрудников ПРФ Австралии (Австралийского центра информации об операциях и их анализа (AUSTRAC)) было обращено на подозреваемого и его приятеля. Информация касалась студента, который несколько раз вносил на свои предоплаченные дебетовые карты и предоплаченные дебетовые карты своего приятеля суммы, каждая из которых составляла 9 900 австралийских долларов с тем, чтобы не были направлены СПО (т.е. имело место вложение денег третьим лицом). Ранее подозреваемый попадал в поле зрения правоохранительных органов в связи с арестом партии кокаина, доставка которой была, якобы, организована им. После дальнейшего расследования и сбора разведывательной информации была начата операция, в которой принимали участие представители сразу нескольких правоохранительных органов.
В базу данных AUSTRAC поступило еще 15 СПО, указывавших на то, что подозреваемый и его приятель вносили депозиты в размерах, не дающих основания направлять СПО, на предоплаченные дебетовые карты. По информации, получаемой AUSTRAC, были выявлены еще несколько случаев совершения финансовых операций, связанных с обоими подозреваемыми. Результаты оценки информации, полученной AUSTRAC, были направлены в правоохранительные органы и оказались полезными в расследовании, которое завершилось арестом обоих подозреваемых. Приятель студента уехал из Австралии в Южную Америку и через 12 дней вернулся из другой южноамериканской страны с, примерно, 5,8 килограммами кокаина в багаже. Позднее он признался, что до этого два раза ввозил кокаин в Австралию, получив за это каждый раз по 28 000 австралийских долларов. Он был арестован, и ему было предъявлено обвинение в импорте и владении запрещенным к ввозу товаром. Главному подозреваемому также были предъявлены обвинения в преступном сговоре с целью ввоза в Австралию около 5,8 килограммов кокаина и отмывании почти 400 000 австралийских долларов. Он был признан виновным и приговорен к семи годам тюремного заключения.
Источник: Австралия

b. Услуги Интернет-платежей:

Пример 6: Использование услуг Интернет-платежей для перевода незаконных доходов от продажи запрещенных пропагандистских материалов расистского характера

Провайдер услуг Интернет-платежей сыграл решающую роль в, по крайней мере, двух судебных процессах, связанных с незаконным распространением компакт-дисков с музыкой ультраправого националистического характера.

Услуги Интернет-платежей использовались для перевода денежных средств за продажу и приобретение пропагандистских материалов расистского характера от и в адрес физических лиц в Германии и за рубежом, включая покупателей, розничных торговцев и, по всей вероятности, оптовых торговцев и производителей (учитывая крупные суммы некоторых переводов).

По немецкому уголовному законодательству распространение таких материалов является уголовным преступлением.

Источник: Германия

Пример 7: Использование услуг Интернет-платежей для перевода незаконных доходов от продажи украденных товаров через коммерческий Интернет-сайт

В 2004 году злоумышленнику было предъявлено обвинение в хранении краденных товаров и получении преступных доходов. В течение трех лет этот человек занимался кражей товаров, скупкой краденных товаров и их продажей через коммерческий сайт в Интернете. Доходы от этой незаконной деятельности перечислялись через счет Интернет-платежей, связанный со счетами пользователей Интернет-сайта. Злоумышленник продал более 9 000 единиц товара, включая цифровые видеодиски (DVD-диски), программно-аппаратные средства для компьютеров, портативные игровые устройства на батарейках фирмы «Nintendo» на общую сумму свыше 459 000 долларов США. Сотрудники правоохранительных органов обнаружили сберегательные облигации на общую сумму более 188 000 канадских долларов, приобретенных этим лицом на часть полученных им незаконных доходов. Злоумышленник был приговорен к двум годам тюремного заключения и штрафу в размере 83 000 канадских долларов.

Источник: Канада

Пример 8: Использование денежных сертификатов для получения вымогаемых денег

Неизвестный преступник направил письмо с угрозами в адрес владельца магазина, торгующего продовольственными товарами по сниженным ценам, в Германии, требуя выплатить 250 000 евро денежными сертификатами, эмитированными провайдером услуг Интернет-платежей, расположенным в Великобритании. Провайдер услуг Интеренет-платежей обеспечил выдачу денежных сертификатов по запросу. При этом провайдеру удалось отследить номера сертификатов через компьютерную систему и сообщить полиции адрес торговой точки, в которой был использован один из выданных сертификатов. Деньги не были заплачены, поскольку к этому времени преступник уже был арестован в Интернет-кафе после того, как попал под наблюдение сотрудников немецкой полиции.

Источник: Германия

Пример 9: Предполагаемое отмывание незаконных доходов от возможной продажи контрафактных товаров через Интернет

Злоумышленник, работавший на зарубежную компанию, имел счет для осуществления Интернет-платежей, а также банковский счет во Франции. Зарубежная компания, подозреваемая в соучастии в преступной схеме, также имела банковский счет во Франции.

На счет подозреваемого поступило 138 платежей на общую сумму 357 245 евро. В 44 случаях деньги на общую сумму 300 000 евро поступили через провайдера услуг Интернет-платежей. Такие поступления через провайдера УИП, похоже, имели отношение к продаже товаров через коммерческий Интернет-сайт. Вскоре после зачисления денег на счет почти вся сумма была перечислена на счет зарубежной компании во Франции.

Возникло подозрение, что подозреваемый использовался компанией в качестве подставного лица для открытия счета Интернет-платежей, поскольку во Франции компании не могут открывать счета у провайдеров УИП. Кроме того, подозреваемый был известен французским таможенным органам, как человек занимающийся подделкой товаров. Выяснилось, что за пять лет он продал

18 650 единиц товара.
Источник: Франция

Пример 10: Отмывание незаконных доходов с использованием денежных сертификатов

В 2010 году немецкое подразделение финансовой разведки получило сообщение о нескольких случаях, в которых были использована следующая схема. Средняя сумма отмытых доходов от преступной деятельности колебалась в пределах 4 500 – 6 000 евро. Номера операций были изначально «выужены» с помощью троянской программы с банковского счета, открытого в Германии. «Фишигновый перевод» был осуществлен на банковский счет, владельцем которого являлся финансовый агент.

Финансовый агент снимал деньги со счета в форме наличных за вычетом свой комиссии. После этого он приобретал денежные сертификаты провайдера услуг Интернет-платежей (максимальная сумма одного сертификата составляла 500 евро) в различных местах, таких как автозаправочные станции, газетные киоски и т.д. Покупки осуществлялись анонимно без указания личности покупателя. Финансовый агент (т.е. третье лицо) посылал номера сертификатов или отсканированные копии сертификатов лицу, отдававшему распоряжения. После этого ПИН-код использовался для оплаты товаров или услуг через Интернет, а также для участия в азартных играх в Интернете.

Правоохранительным органам не удалось отследить каналы этой операции.

Следует отметить, что в этом случае несколько денежных сертификатов на небольшие суммы денег, приобретенные в разных местах, могут использоваться совместно. Также возможен их перевод в электронные деньги через различные обменные пункты в Интернете.

Источник: Германия

Пример 11: Использование электронных денег для целей мошенничества в Интернете и отмывания денег

Молодой человек, действующий в качестве подставного лица, открыл счет в электронной валюте для получения доходов от кражи средств с банковских счетов в Интернете, осуществляемой его знакомым, находившимся за рубежом. После этого он попытался снять деньги со счета электронной валюты, обратившись в пункт обмена электронных валют с просьбой выдать ему почтовые платежные поручения. Для того, чтобы скрыть свою личность, он сообщил, что потерял паспорт и попросил сотрудника обменного пункта позвонить в контору компании, оказывающей денежные услуги, и сообщить им, что человек с его внешностью придет в их контору в определенное время для получения наличных по платежному поручению. Предполагалось, что он не собирался отправлять деньги за рубеж, а оставить весь доход себе. Он был арестован и предстал перед судом.

Источник: Австралия

Пример 12: Использование провайдеров услуг Интернет-платежей и подставных лиц для приобретения запрещенных препаратов и отмывания доходов от их продажи

В ходе расследования, проводимого правоохранительными органами в отношении лиц, занимавшихся контрабандой стероидов, гормонов роста и других запрещенных стимуляторов, был установлен ряд лиц, подозреваемых в ввозе и распространении запрещенных препаратов по всей Австралии. Было установлено, что находящиеся в Австралии контрабандисты отправили за рубеж деньги на общую сумму в несколько тысяч долларов для приобретения запрещенных препаратов. Корме того, выяснилось, что они еженедельно получали несколько тысяч долларов в качестве выручки от продажи таких запрещенных препаратов.

Контрабандисты использовали законным образом выданные удостоверения личности, полученные на вымышленные имена, для открытия нескольких абонементных почтовых ящиков для получения препаратов. Для привлечения клиентов и получения заказов через Интернет использовались «чаты» и форумы в Интернете. Для осуществления платежей подозреваемые использовали услуги провайдеров Интернет-платежей и денежных переводов в Австралии, причем сумма каждого платежа обычно не превышала 1 000 австралийских долларов.

Зарубежные поставщики были в курсе того, что препараты запрещены к ввозу в Австралию, и

специально указывали неправильные наименования препаратов для того, чтобы обойти режим таможенного контроля. Контрабандисты привлекли друзей и супругов для осуществления платежей от их имени и использовали различные отделения для отправки платежей. Они также часто меняли имена и преднамеренно допускали ошибки в написании имен и адресов. Полные адреса зарубежных бенефициаров никогда не указывались, а указывался только регион.
В ходе этой операции правоохранительные органы арестовали более 140 человек по всей Австралии по выданным ордерам.
Источник: Австралия

c. Услуги мобильных платежей

Пример 13: Предположительное использование мобильных платежей для перевода денежных средств, полученных мошенническим путем
Женщина стала жертвой мошенников, поверив что, что ее супруг попал в автомобильную аварию. Ее попросили перевести деньги через провайдера мобильных платежей на оплату счета за услуги врача или на оплату лечения в больнице.
Источник: Филиппины

Пример 14: Предположительное использование мобильных услуг для перевода средств в результате мошенничества в сфере телемаркетинга
Жертвам мошенничества посылались SMS-сообщения, в которых сообщалось, что они стали победителями электронной лотереи. Для получения приза, их просили перевести деньги через провайдера мобильных платежей для оплаты налогов, связанных с призом.
Источник: Филиппины

Пример 15: Продажа украденных телефонных карт с помощью мобильных платежей между физическими лицами
В апреле 2010 года злоумышленник был приговорен к тюремному заключению на Каймановых Островах за использование информации, украденной с кредитных карт, в целях незаконного приобретения телефонных кредитов, которые он впоследствии продавал, используя услуги мобильных платежей между физическими лицами. Хотя сумма оказалась небольшой, ему предъявили обвинение в отмывании денег в рамках судебного разбирательства в соответствии с уголовным законодательством Каймановых Островов.
Источник: Генеральная прокуратура Каймановых Островов

4.2 Типология 2: Использование безличного характера счетов для использования новых способов платежей

126. В основе многих новых способов платежей лежит бизнес модель, предусматривающая минимальный личный контакт с клиентами, или вообще отсутствие такого контакта. Это может способствовать использованию новых способов платежей преступными элементами в целях отмывания денег.

127. В ряде случаев продукты, связанные с новыми способами платежей, использовались для отмывания незаконных доходов после хищения персональных данных или кражи денег с банковских счетов посредством взлома компьютерных сетей или «фишигна». Поскольку банковские счета или кредитные и дебетовые карты были изначально открыты на имя законных клиентов, преступники могли использовать их в качестве ссылочных счетов (с которых будут поступать деньги) для вложения средств на предоплаченные карты или счета, используемые для Интернет-платежей. В этих случаях провайдеры услуг НСП не могли установить, что операции проводились не их законными клиентами, а также не могли выявить никакой другой подозрительной деятельности.

128. В других случаях украденные или поддельные персональные данные использовались для открытия счетов НСП, которые также использовались в качестве транзитных счетов для отмывания незаконных доходов, либо для одновременного совершения преступлений (например, мошенничества) и отмывания денег.

129. В большинстве случаев в качестве транзитных счетов использовались счета предоплаченных карт или счета Интернет-платежей. Как только незаконно полученные средства переводились на такие счета, преступники или их сообщники снимали наличные деньги через банкоматы, либо тратили деньги на покупку товаров (часто через Интернет).

130. Хотя во многих приведенных ниже ситуационных исследованиях провайдеры услуг Интернет-платежей или эмитенты предоплаченных карт не могли выявить подозрительную деятельность, определенные недостатки процедуры идентификации и проверки личности, а также систем мониторинга ряда провайдеров способствовали тому, что незаконная деятельность оставалась незамеченной в течение определенного периода времени. Так, в примере 27, хотя отдельные банковские переводы и выглядели законными, использование четырех ссылочных банковских счетов (с которых переводились деньги) в разных городах для одного и того же счета Интернет-платежей должно было вызвать подозрения провайдера УИП.

a. Предоплаченные карты

Пример 16: Отмывание денег, украденных с банковских счетов физических лиц

В 2007 году шесть обвиняемых предстали перед судом по обвинению в использовании украденной информации для незаконного перевода средств с банковских счетов на счета, контролируемые обвиняемыми, включая счета предоплаченных карт. Обвиняемые использовали компьютерную программу, имевшуюся в свободной продаже, для поиска в Интернете уязвимых компьютеров физических лиц или компаний, в которых хранилась информация о финансовых счетах. После этого обвиняемые осуществляли мошеннические операции по переводу средств со счетов своих жертв на счета, открытые на имя подставных компаний. Часть незаконных доходов со счетов подставных компаний использовалась для пополнения средств на предоплаченных картах, которые обвиняемые использовали для покупок. Обвиняемым было предъявлено обвинение в отмывании, порядка, 166 000 долларов США. Все шесть обвиняемых признали свою вину и были приговорены к тюремному заключению сроком от 3 до 36 месяцев.
Источник: США

Пример 17: Отмывание денег, украденных со счетов заработной платы компании

В 2009 году двум обвиняемым было предъявлены обвинения в незаконном проникновении через Интернет в компьютерную систему компании и мошенническом переводе средств с банковских счетов своих жертв на предоплаченные карты. По утверждению стороны обвинения, обвиняемые использовали украденные регистрационные коды и пароли для получения доступа к Интернет-счетам своих жертв, которые помимо прочего, позволяли пользователям прямое депонирование заработной платы сотрудников компании. По мнению стороны обвинения, обвиняемые переводили заработную плату сотрудников на счета предоплаченных карт хакеров. Сумма незаконно полученных и переведенных обвиняемыми средств за 11 месяцев, составила 19 976,43 долларов США. Обвиняемые пока не предстали перед судом.
Источник: США

Пример 18: Отмывание доходов, полученных в результате «фишинга», с использованием предоплаченных карт

В данном случае предоплаченные карты использоваться в качестве транзитных счетов, на которые преступники переводили средства с банковских счетов после хищения персональных данных владельцев счетов. Злоумышленник под видом владельца банковского счета переводил деньги на предоплаченную карту, выданную на имя подставного лица. Как только средства переводились на карту, соответствующая сумма наличных денег снималась через банкомат.

Дополнительная типология: использование подставного лица
Источник: Италия

Пример 19: Отмывание доходов от контрафакции и мошенничества с использованием предоплаченных карт многогоэмитентных (открытых) систем

В течение нескольких месяцев на счета г-на ПОЛ и компании «BE» поступили международные переводы на сумму около 500 000 евро от швейцарской компании, выступающей в качестве агента и брокера ценных бумаг. Эти средства использовались для пополнения предоплаченных карт. В большинстве случаев на карты клались суммы, равные 5 000 евро (максимально разрешенная сумма). Г-н ПОЛ заявил, что вносил деньги на предоплаченные карты, так как выдавал их своим сотрудникам на профессиональные расходы. Как только средства поступали на карты, держатель карты быстро снимал их путем многократного снятия наличных денег через банкоматы.
В отношении г-на ПОЛ проводилось судебное расследование, касающееся контрафакции и мошенничества. По информации, имевшейся у полиции в отношении г-на ПОЛ, средства, поступавшие из Швейцарии, могли иметь незаконное происхождение или быть связаны с контрафакцией и мошенничеством, в котором был замешан г-н ПОЛ. Это предположение подтверждалось сложной схемой (международные переводы денег, использование предоплаченных карт, снятие наличных денег), использованной для возвращения денег в Бельгию.
Источник: Бельгия

Пример 20: Использование «мертвых душ» в качестве сотрудников для отмывания незаконно полученных средств с использованием предоплаченных карт

В 2009 году обвиняемому было предъявлено обвинение в присвоение средств своего работодателя и отмывании денег через предоплаченные карты, на которые перечислялась заработная плата. Обвиняемый, являвшийся управляющим административно-хозяйственного отдела, проводил собеседования с претендентами на рабочие места для получения от них персональной информации, которую он потом использовал для создания «несуществующих» рабочих мест, на каждое из которых выдавалась предоплаченная карта для перечисления заработной платы. Обвиняемый оставлял такие карты у себя, используя их для снятия денег через банкоматы и приобретения товаров. За три года он отмыл, порядка, 200 000 долларов США. Обвиняемый пока не предстал перед судом.
Источник: США

Пример 21: Мошенничество с кредитными картами и отмывание денег

В 2006 году двое обвиняемых предстали перед судом по обвинению в использовании 61 украденных номеров счетов кредитных карт для пополнения «виртуальных предоплаченных карт». Такие карты имели номер счета, срок действия и код проверки подлинности карты, но не предусматривали выдачу материальной карты, используемой для клиентских операций без личного контакта. После этого обвиняемые использовали эти «виртуальные карты» для оплаты за обучение в университете в США. При этом они переплатили за обучение. Университет выдал им чек на сумму 31 045 долларов США, составлявшей размер переплаты, способствуя, таким образом, отмыванию незаконно полученных средств обвиняемыми. Один из обвиняемых признал свою вину в мошенничестве с использованием телефонной линии и был приговорен к 28 месяцам тюремного заключения с последующим нахождением под надзором в течение пяти лет. Второй обвиняемый был признан виновным в указании ложных данных в заявке на получение кредита, отмывании денег, мошенничестве с использованием почты, хищении персональных данных с отягчающими обстоятельствами и владении неразрешенными средствами доступа. Он был приговорен к 61 месяцу тюремного заключения с последующим нахождением под надзором в течение пяти лет.
Источник: США

Пример 22: Отмывание доходов, полученных в результате хищения персональных данных

В 2006 году обвиняемый, являвшийся управляющим программы предоплаченных карт, предстал перед судом по обвинению в использовании возможностей программы предоплаченных карт для

отмывания незаконных доходов в интересах преступников, занимающихся хищением персональных данных. Преступники, «специализировавшиеся» на краже персональной информации, открыли 21 счет предоплаченных карт и положили на карты в общей сложности, порядка, 1 миллиона долларов США, украденных с банковских счетов своих жертв. Информация о банковских счетах была украдена со счетов пользователей провайдера услуг Интернет-платежей. Преступники снимали наличные со счетов предоплаченных карт через банкоматы в России. Обвиняемый признал свою вину в отмывании денег и был приговорен к 120 месяцам тюремного заключения.
Дополнительная типология: Провайдер НСП или управляющий программой, являющийся соучастником преступных схем
Источник: США

Пример 23: Мошенничество и отмывание денег
В 2007 году трое обвиняемых предстали перед судом по обвинению в незаконном доступе к процессору обработки платежей и осуществлении мошеннических операций, в результате которых на 80 предоплаченных карт было перечислено, примерно, 700 000 долларов США. По утверждению стороны обвинения, обвиняемые действовали из гостиничного номера. Они использовали переносной компьютер, устройство кодирования карт и телефонную линию для доступа к процессору обработки платежей под видом представителей компаний, осуществляющих операции по возврату средств, и использовали устройство кодирования карт для перевода, якобы, возвращаемых денег на свои предоплаченные карты. В день обвиняемые снимали, примерно, 200 000 долларов США из сумм, поступавших на их предоплаченные карты, через расположенные поблизости банкоматы или приобретая почтовые денежные поручения. Главный обвиняемый был признан виновным, но обжаловал приговор. Два других обвиняемых признали свою вину.
Источник: США

Пример 24: Мошенничество и отмывание денег
В 2009 году троим обвиняемым были предъявлены обвинения в краже 5 миллионов долларов США путем взлома базы данных компании-эмитента предоплаченных карт, хищения информации с карт и подделке остатков средств на счетах и лимитов сумм операций. По утверждению стороны обвинения, обвиняемые использовали украденную с карт информацию для изготовления поддельных дубликатов карт и использовали их для снятия денег через банкоматы по всему миру. За один месяц обвиняемые сняли 750 000 долларов США. Два обвиняемых признали свою вину в преступном сговоре, отмывании денег, банковском мошенничестве и владении поддельным устройством доступа, но приговор им еще не вынесен. Третий обвиняемый признал свою вину в преступном сговоре и владении поддельным устройством доступа, но приговор ему еще также не вынесен.
Источник: США

b. Услуги Интернет-платежей

Пример 25: Отмывание незаконно полученных доходов через провайдера электронных денег
В 2009 году подозреваемый незаконным образом получил доступ к банковским Интернет-счетам физических лиц и отдал распоряжение компьютерной системе перевести, примерно, 740 000 иен (8 300 долларов США) в пункт обмена электронных валют для получения электронных денег. После этого обвиняемый продал часть электронных денег в другой пункт обмена электронных валют за реальные деньги. И, наконец, обвиняемый отдал распоряжение сотрудникам пункта обмена электронных валют перевести деньги на несколько банковских счетов, которые были открыты незаконным образом и контролировались обвиняемым.
Источник: Япония

Пример 26: Использование мошеннической схемы и отмывание денег с использованием услуг Интернет-платежей
Злоумышленник разработал схему с целью обмана пользователей, искавших возможность купить

учебники на коммерческом сайте в Интернете. Этот человек открыл, примерно, 384 фиктивных банковских счетов в банке, расположенном в юрисдикции «Z», для несуществующих сотрудников, которые, как он проинформировал банк, будут заниматься продажей институтских учебников. Затем он использовал информацию о банковских счетах для открытия, примерно, 468 счетов продавцов, связанных с коммерческим Интернет-сайтом, используя услуги Итернет-платежей между физическими лицами (т.е. провайдера УИП).
Мошенник разместил рекламу о продаже институтских учебников на всех открытых им фиктивных счетах продавцов коммерческого Интернет-сайта. Покупатели, думая, что покупают учебники через коммерческий Интернет-сайт, перевели в качестве оплаты более 5,3 миллионов долларов США на счета продавцов, используя услуги провайдера Интернет-платежей.
После этого мошенник перевел незаконно полученные доходы со счетов продавцов, открытых у провайдера УИП, на несколько банковских счетов, открытых в банке, расположенном в Сингапуре.
Представители правоохранительного органа юрисдикции «Z» связались со своими коллегами в Сингапуре, которые быстро наложили арест на «грязные» деньги. Благодаря тесному взаимодействию правоохранительных органов деньги были возвращены жертвам мошенничества. Мошеннику также предъявили обвинения в незаконном доступе в сеть с использованием телефонной линии в юрисдикции «Z».
Источник: Сингапур

Пример 27: Отмывание денег, украденных с банковских счетов, через счета Интернет-платежей

Преступник, «специализирующийся» на компьютерных преступлениях, украл персональные данные своей жертвы для осуществления банковских операций через Интернет (включая данные о клиенте и счете), а затем незаконным образом открыл подложный счет у провайдера услуг Интернет-платежей под именем своей жертвы. Личные данные, предоставленные при открытии счета (номер телефона, домашний адрес, дата рождения и т.д.), были не нестоящими. Указанный адрес электронной почты был предоставлен, так называемыми, «свободными провайдерами», которые сами не осуществляют идентификацию и проверку личностей клиентов.
Преступник указал ссылочный банковский счет (с которого будут переводиться деньги) для подложного счета Интернент-платежей. Этот ссылочный счет был счетом жертвы преступника. После этого преступник мошенническим образом перевел деньги со ссылочного банковского счета своей жертвы на подложный счет, открытый у провайдера услуг Интернет-платежей. Поскольку деньги были перечислены со ссылочного банковского счета, система мониторинга провайдера УИП сочла эту операцию законной. Полученные деньги были перечислены на другие счета, открытые у провайдера УИП. Правоохранительным органам так и не удалось отследить денежные потоки и установить личности преступника.
Преступник несколько раз использовал эту схему в отношении нескольких жертв, но всегда использовал один и тот же счет Интернет-платежей. Таким образом, за два месяца он изменял ссылочный счет для счета ИП четыре раза. Четыре указанных ссылочных счета были открыты в различных банках, расположенных в разных городах.
Источник: Германия

4.3. Типология 3: Провайдеры услуг НСП или их сотрудники, являющиеся соучастниками преступных схем

131. В ряде представленных случаев фигурируют эмитенты предоплаченных карт и провайдеры УИП, которые контролируются преступниками и которые (либо намеренно, либо по неосторожности) содействуют осуществлению деятельности по отмыванию денег и финансированию терроризма. В указанных случаях ограничения по выходу на рынок (например, проверка на профессиональную пригодность и добросовестность) оказались либо не эффективны, либо не применимы к той или иной организации, находящейся на территории соответствующей юрисдикции.

132. В некоторых случаях (примеры 28, 30, 31) под подозрением в соучастии и сговоре с целью содействия деятельности по отмыванию преступных доходов и финансированию терроризма оказывались как провайдеры УИП, так и эмитенты предоплаченных карт.

а. Предоплаченные карты

Пример 28: Предполагаемое использование предоплаченных карт открытых (многоэмитентных) систем и платежных систем Интернета для отмывания денег от продажи наркотиков

Расследование данного случая было начато после получения информации от одного из иностранных ПФР о предъявлении обвинения ряду физических лиц в отмывании многомиллионных сумм, полученных от торговли наркотиками, через компанию-эмитента предоплаченных карт открытых (многоэмитентных) систем в стране А. Предположительно, денежные средства вносились на предоплаченные карты, после чего перемещались, например, в страну В, находящуюся в Южной Америке, возвращаясь к торговцам наркотиками. Источниками преступных доходов предположительно являлись и другие виды преступной деятельности.

Было установлено, что двое из указанных лиц, связанных с компанией-эмитентом предоплаченных карт, пользовались адресами как в стране А, так и в Канаде. Они также открыли банковские счета и учредили по крайней мере одну компанию в Канаде.

Компания-эмитент предоплаченных карт находилась в стране А, но имела множество счетов как в стране А, так и в Канаде. Банковские счета в стране А и Канаде использовались для получения денежных средств от различных физических и юридических лиц, расположенных в разных странах Центральной Америки, Европы, Карибского бассейна, Африки, Азии и Южной Азии, а также для получения денежных средств в пределах страны А и Канады.

Было также установлено, что двое канадских провайдеров услуг Интернет-платежей (УИП) направляли денежные средства указанной компании-эмитенту предоплаченных карт из страны А.

Полученная информация свидетельствовала о том, что оба провайдера УИП предлагали своим клиентам услуги предоплаченных карт, выпускаемых компанией-эмитентом предоплаченных карт из страны А.

Один из канадских провайдеров УИП являлся фигурантом еще одного расследования, в рамках которого его подозревали в содействии отмыванию денежных средств, полученных с помощью схемы Понци (финансовой пирамиды).

Подозрительные транзакции включали в себя взносы наличных денег на счета третьих сторон и международные электронные денежные переводы (ЭДП). Большая часть средств, поступивших на счета в Канаде, перечислялась обратно на счета в стране А, принадлежащие компании-эмитенту предоплаченных карт и двум ассоциированным компаниям, которые также находились в стране А.

Смежная типология: «Финансирование третьих сторон».

Источник: Канада.

Пример 29: Присвоение чужого имущества и отмывание денег

В 2007 году против сотрудника одной из национальных сетей продовольственных магазинов было возбуждено уголовное дело о хищении средств на сумму свыше 375 000 долларов США. Сотрудник, при выполнении текущих операций по обслуживанию клиентов магазина, предположительно перечислял часть выручки на счета предоплаченных карт, якобы принадлежавших реальным клиентам. При этом деньги, необходимые для покрытия перечисленных средств, в кассу магазина не вносились. И хотя соответствующие транзакции регистрировались компанией-эмитентом предоплаченных карт, для сокрытия хищения предполагаемый преступник предположительно принял меры к тому, чтобы в самом магазине данные транзакции нигде не фиксировались.

Источник: США.

b. Услуги Интернет-платежей

Пример 30: Предполагаемое использование УИП (в т.ч. услуг, связанных с электронными драгоценными металлами) и предоплаченных карт многоэмитентных (открытых) систем для отмывания денег, полученных в результате использования мошеннических схем

Расследование данного случая было начато после получения информации от одного из правоохранительных органов и одного из иностранных подразделений финансовой разведки (ПФР) о том, что некий канадский провайдер УИП, его филиал в США и иные ассоциированные предприятия предположительно причастны к отмыванию преступных доходов, полученных в результате использования схемы Понци (финансовой пирамиды) и мошеннических схем телемаркетинга.

Было установлено, что у данного провайдера УИП из Канады также имелись филиалы в одной из европейских стран и в одной из стран Азии. Кроме того, было обнаружено, что в данной комплексной схеме по отмыванию денег участвовали (преднамеренно или непреднамеренно) не менее пяти контор по обмену электронных валют (расположенных в Канаде, США и в одной из стран Северной Европы), два провайдера услуг, связанных с драгоценными металлами (из США), и три эмитента предоплаченных карт многоэмитентных (открытых) систем (из Канады и США). Было установлено, что один из эмитентов предоплаченных карт многоэмитентных (открытых) систем предложил виртуальным игрокам использовать такие предоплаченные карты для пополнения виртуальных счетов и обналичивания виртуальных валют через банкоматы.

Как правило, денежные средства, поступающие из других стран на счета банков в Канаде, принадлежавшие канадскому провайдеру УИП и эмитентам предоплаченных карт, использовались либо для пополнения предоплаченных карт, либо для расчета[65] с другими провайдерами УИП и эмитентами предоплаченных карт из других стран. В некоторых случаях подозрительные средства поступали в финансовую систему Канады, откуда впоследствии перечислялись в другие страны в рамках операций, направленных на сокрытие незаконных источников их происхождения («расслоение» денежных средств). В ряде случаев такие средства в конечном итоге возвращались в Канаду.

Подозрительные транзакции также включали в себя выставление банковских тратт и крупные взносы наличными на банковские счета, после совершения которых средства зачастую перечислялись с помощью электронных денежных переводов (ЭДП) в другие страны в рамках операций, направленных на сокрытие незаконных источников их происхождения («расслоение» денежных средств) с использованием различных банковских счетов.

Источник: Канада.

Пример 31: Отмывание незаконных средств с помощью электронных валют и предоплаченных карт

При проведении расследования было установлено, что международная преступная группировка использовала одного из провайдеров финансовых услуг для перечисления незаконных денежных средств в восточно-европейские страны, в которых члены данной группировки обналичивали и обращали указанные средства в электронные деньги в конторах по обмену электронных валют.

Электронные деньги перечислялись на счета, открытые членами данной группировки у одного из провайдеров финансовых услуг, занимавшегося операциями с электронной валютой в указанных странах. Указанный провайдер финансовых услуг выпускал, совместно с одним оффшорным банком, предоплаченные карты MasterCard *Cirrus*, которые можно было приобретать анонимно и вносить на них суммы в электронной валюте. Такие карты можно было использовать в любых странах - в банкоматах и при оплате покупок через терминалы, принимающие карты *Cirrus*.

[65] В большинстве случаев, информация о таких транзакциях была представлена кредитно-финансовыми учреждениями. В рамках указанных транзакций совершались переводы денежных средств между объединенными банковскими счетами, принадлежащими провайдерам УИП и эмитентам предоплаченных карт.

Данная схема позволяла преступникам эффективно скрывать незаконные денежные средства и обеспечивала быстрый и анонимный доступ к таким средствам.

Источник: Германия.

Пример 32: Отмывание денег, полученных с помощью незаконных онлайновых азартных игр, с помощью провайдера УИП

В 2007 году провайдер услуг Интернет-платежей, расположенный на острове Мэн, ценные бумаги которого публично котировались на рынке альтернативных инвестиций (РАИ) Лондонской фондовой биржи, признал свою вину в совершении уголовного преступления и дал свое согласие на выплату 136 млн. долл. США, полученных преступным путем, в рамках соглашения об отсрочке судебного преследования.

Провайдер УИП являлся соучастником сговора, целью которого было получение прибыли с помощью незаконных (по законодательству США) онлайновых азартных игр и руководства деятельностью по незаконному перечислению денежных средств.

Источник: США.

Пример 33: Отмывание денег с помощью провайдера услуг, связанных с электронными драгоценными металлами

В 2008 году Интернет-провайдер услуг электронных валют, а также три главных директора и владельца данного предприятия признали себя виновными по всем пунктам уголовного обвинения в отмывании денег и руководстве деятельностью, связанной с незаконным перечислением денежных средств.

Определенные возможности, предоставляемые указанным провайдером услуг электронных валют, привлекли к нему пользователей, занимающихся незаконной деятельностью (например, отсутствие необходимости указывать не только свою настоящую личность, но и какие-либо идентификационные данные вообще). Указанный провайдер позволял открывать счета без проверки личности пользователя, несмотря на то, что ему было известно об их использовании для совершения преступлений, в т.ч. таких преступлений, как эксплуатация детского труда, инвестиционные аферы, мошенничество с кредитными картами, отмывание денег и хищение персональных данных. Кроме того, мониторинг сотен тысяч счетов осуществлялся в указанной компании лицами, не имевшими необходимого опыта работы. Компания также участвовала в разработке системы, в рамках которой пользователей, о преступной деятельности которых становилось известно, прямо призывали перечислять незаконные средств через другие счета данной компании. В отличие от других провайдеров УИП, указанная компания не включила в свое пользовательское соглашение каких-либо положений, запрещающих использование ее услуг для

осуществления преступных действий.

Источник: США

4.4. Трансграничное перемещение предоплаченных карт

133. В отчете ФАТФ 2006 года было указано на еще один потенциально возможный риск / типологию неправомерного использования предоплаченных карт, а именно, на возможность замены трансграничного перемещения наличности на трансграничное перемещение предоплаченных карт. Лучше всего это видно на примере мошеннической схемы с использованием обычных банковских дебетовых карт (предоплаченные карты многоэмитентных (открытых) систем в рамках данной схемы не использовались). В 2007 году в США против двух физических лиц было выдвинуто обвинение в отмывании денег. Указанные лица перечисляли в Колумбию доходы от продажи наркотиков с помощью сети банкоматов. Предположительно, обвиняемые поручили членам своих семей, друзьям и иным лицам открыть 380 банковских счетов в шести разных штатах. После чего один из обвиняемых сделал множество денежных вкладов на сумму от 500 до 1500 долл. США, предположительно разместив в течение одного дня более 100 000 долл. США на 112 банковских счетах. При открытии каждого счета его владелец получал две карты, предназначенные для использования исключительно в банкоматах. Обвиняемые оставляли себе одну карту, а вторую карту отправляли по почте в Колумбию, с помощью которой денежные средства и обналичивались через банкоматы в указанной стране.

134. Известны и другие подобные случаи трансграничного перемещения предоплаченных карт одноэмитентных (закрытых) систем, а также несколько случаев трансграничного перемещения предоплаченных карт многоэмитентных (открытых) систем:

- Предоплаченные карты с нулевым балансом, дающие право на получение товара на сумму не более 1000 долл. США были отправлены из США в Канаду. Хотя они и были отправлены в Канаду, получить товар по указанным картам можно было только в США. Данные карты были предположительно приобретены с помощью точных копий кредитных карт, снятых с настоящих кредитных карт.
- Предоплаченные карты были отправлены из Южной Америки в Канаду. Карты были выпущены на имя разных физических лиц, но были отправлены одному физическому лицу. Банк, выпустивший эти карты, в прошлом являлся фигурантом другого расследования. Физическое лицо, которому были отправлены указанные карты, ранее также попадал в поле зрения европейских и американских правоохранительных органов. В результате проведенного расследования карты были аннулированы, так как банк не захотел портить свою репутацию.
- В Австралии владелец предоплаченной карты регулярно пополнял ее наличными на сумму, немногим менее 10 000 австралийских долларов (пороговая сумма, при превышении которой необходимо уведомлять соответствующие органы). Еще одна карта, с помощью которой можно было осуществлять операции с тем же счетом, была отправлена в другую страну и

использовалась там для снятия денежных средств с указанного счета через банкоматы. Данная операция осуществлялась многократно. С помощью указанной схемы было отмыто свыше 100 000 австралийских долларов.

- Расследование, проводившееся в Австралии, позволило обнаружить физическое лицо, имевшее 12 водительских удостоверений, полученных им на законных основаниях, но с использованием фальшивых личных данных, и 1 водительское удостоверение, полученное на собственное имя. Кроме того, у него было обнаружено множество фальшивых удостоверений личности и заграничных паспортов. Сотрудники правоохранительных органов, задержавшие указанное лицо, обнаружили при нем 140 000 австралийских долларов наличными, полученных в результате преступной деятельности, и 46 предоплаченных карт. После обыска на складе, арендованного данным лицом, были обнаружены другие предоплаченные и подарочные карты. Предположительно, денежные средства перемещались в Индию для отмывания. По всей видимости, данный гражданин покупал их в почтовых отделениях и на станциях техобслуживания, торгующих картами стоимостью 50 и 100 австралийских долларов. Стоимость некоторых карт составляла 500 австралийских долларов, что указывает на то, что они были приобретены через Интернет.

135. Если первые два примера и свидетельствуют о том, что предоплаченные карты, возможно, использовались для отмывания денег и финансирования терроризма, однозначной уверенности в этом нет, тогда как третий и четвертый пример однозначно указывают на их использование для отмывания денег (при этом в четвертом примере показан механизм использования анонимных предоплаченных карт в соответствующих преступных схемах).

136. Два из представленных примеров (***примеры 22 и 28***) также указывают на то, что предоплаченные карты могли быть перемещены в другую страну, так как денежные средства были обналичены в юрисдикции, отличной от той, в которой они были пополнены. Однако какой-либо дополнительной информации, подтверждающей данное предположение (например, обнаружение или конфискация карт с помощью средств пограничного контроля), не имеется.

137. Таким образом, с 2006 года было зафиксировано определенное количество случаев трансграничного перемещения предоплаченных карт. Учитывая небольшое количество обнаруженных случаев, составители отчета считают, что включать их в одну типологию несколько преждевременно. Малое количество обнаруженных случаев можно объяснить тем, что в большинстве юрисдикций предоплаченные карты не считаются денежными инструментами, и что таможенным работникам сложно отличить предоплаченные карты от обычных кредитных карт из-за сильного внешнего сходства.

4.5 Сигналы опасности

138. В результате анализа конкретных примеров были определены сигналы опасности, характерные для всех продуктов и услуг НПМ. Кроме того, было обнаружено несколько сигналов опасности, указывающих на возможное соучастие эмитентов предоплаченных карт в преступных

схемах. Было установлено, что некоторые примеры сами по себе являются сигналами опасности, при этом полный список примеров, связанных с каждым сигналом опасности, еще не определен.

139. Сигналы опасности указывают на наличие подозрительной деятельности, в рамках которой фактическое использование того или иного продукта либо отличается от его целевого назначения, либо нецелесообразно с экономической точки зрения. Например, снятие денежных средств с предоплаченных туристических карт за рубежом вполне естественно, тогда как продажа таких карт несовершеннолетним вызывает подозрения. Поэтому сигналы опасности необходимо оценивать рационально, с учетом специфики конкретного продукта.

Сигналы опасности, связанные со всеми провайдерами услуг НСП:

- Расхождения между информацией, предоставленной клиентом, и информацией, полученной с помощью систем мониторинга (***пример 19***).
- Физические лица, имеющие большое количество счетов НСП у одного и того же провайдера (***примеры 21 и 23***).
- Крупные и разнообразные источники денежных средств, использующиеся для пополнения одного и того же счета(ов) НСП (например, банковские переводы, кредитные карты и наличные средства, использующиеся в разных географических точках) (***примеры 6, 7, 16 и 17***).
- Многочисленные счета в банках, расположенных в различных городах, использующиеся для пополнения одного и того же счета НСП (***пример 27***).
- Пополнение счета только третьими сторонами (***примеры 1 и 3***).
- Одно и то же физическое лицо многократно пополняет одну и ту же предоплаченную карту (карты) наличными на суммы, немногим менее 10 000 долларов (пороговая сумма, при превышении которой необходимо уведомлять соответствующие органы), время от времени повторяя указанную операцию (***пример 5***).
- Многократное внесение средств или пополнение счета НСП третьими сторонами с последующим переводом средств на счет или счета, не имеющие к счету НСП никакого отношения (***примеры 9 и 26***).
- Многократное пополнение одних и тех же счетов с последующим обналичиванием денежных средств в банкоматах через короткий промежуток времени (***примеры 18 и 19***).
- Многократное обналичивание денежных средств с помощью разных банкоматов (в том числе и в странах, расположенных за пределами юрисдикции, в которой осуществлялось пополнение счета НСП) (***примеры 4 и 24***).
- Использование счета НСП исключительно для обналичивания денежных средств, а не для совершения покупок через платежные терминалы или Интернет (***примеры 18 и 19***).
- Нетипичное использование платежного инструмента (в т.ч. нестандартное и многократное трансграничное использование такого инструмента или нестандартные транзакции, многократно совершаемые с его помощью) (***примеры 2 и 24***).

Сигналы опасности, связанные с эмитентами предоплаченных карт, являющимися соучастниками преступных схем:

- Большое количество банковских счетов, принадлежащих одной компании-эмитенту предоплаченных карт (которые в некоторых случаях могут находиться в разных странах), предположительно использующихся в качестве транзитных счетов (для «расслоения» денежных средств) (***пример 28***).
- Компания-эмитент предоплаченных карт находится в одной стране, но имеет счета в других странах (использование которых не имеет очевидных коммерческих выгод и поэтому является подозрительным) (***пример 28***).
- Перевод денежных средств с одних банковских счетов на другие и обратно, владельцами которых являются разные компании-эмитенты предоплаченных карт (свидетельствует о возможном использовании указанных счетов для «расслоения» денежных средств, если такие переводы не соответствуют использующейся бизнес-модели) (***пример 30***).
- Транзакции с наличными средствами (которые иногда дробятся на суммы, не превышающие порога, при достижении которого о транзакции должны быть уведомлены соответствующие органы («структуринг»)), осуществляемые владельцем компании-эмитента предоплаченных карт, объемы и частота которых нецелесообразны с экономической точки зрения (***пример 30***).

5. Правовые вопросы, связанные с услугами НСП

140. В данной главе рассматриваются вопросы правового регулирования деятельности провайдеров услуг НСП в различных юрисдикциях.[66] В **Разделе 5.1** представлены различные подходы, использующиеся в настоящий момент для регулирования услуг НСП. В **Разделе 5.2** говорится о конкретных задачах, стоящих перед регуляторными, правоохранительными и надзорными органами.

5.1 Регуляторные модели, использующиеся для регулирования деятельности провайдеров услуг НСП

141. В соответствии с Рекомендациями ФАТФ, все юридические и физические лица, осуществляющие определенные виды деятельности, подлежат надзору и обязаны соблюдать обязательства ПОД/ФТ. К указанным лицам относятся юридические и физические лица, осуществляющие переводы денежных средств или стоимости, выпуск и управление платежными средствами.[67] Следовательно, большинство провайдеров услуг НСП являются кредитно-финансовыми учреждениями и подлежат регулированию и надзору в соответствии с требованиями Рекомендации 23 или Специальной Рекомендации VI.

[66] В настоящее время специалисты Всемирного банка работают над докладом о регулировании «новых инструментов оплаты розничных покупок», включающим в себя услуги НСП, о которых говорится в настоящем отчете. В рамках подготовки указанного доклада в июле 2012 года заинтересованным сторонам была направлена анкета, составленная на основе «Исследования платежей, совершаемых с помощью электронных денег, сети Интернет и мобильных телефонов», опубликованного в 2004 году Комитетом по платежам и расчетным системам (КПРС) Банка международных расчетов в Базеле.

[67] Глоссарий ФАТФ: «кредитно-финансовое учреждение».

142. В бизнес-моделях с четко выраженной сегментацией услуг НСП (например, в случаях, когда определенные финансовые услуги предоставляются несколькими юридическими лицами совместно), определить, является ли объем работ, выполняемый каким-либо одним лицом в рамках такой совместной деятельности, достаточным для того, чтобы считать его кредитно-финансовым учреждением (и, следовательно, обязать такое лицо соблюдать регуляторные и надзорные требования), может быть непросто. Примерами такой сегментации являются бизнес-модели, использующиеся провайдерами услуг электронных валют,[68] а также использование агентов.[69] Существуют различные точки зрения относительно того, нужно ли осуществлять регулирование и надзор в указанных случаях, или нет.

143. Анализ ответов, представленных в анкете отчета, показал, что существует три различных подхода к регулированию новых способов платежа. В некоторых юрисдикциях регуляторные требования ПОД/ФТ к провайдерам услуг НСП либо не применяются вообще, либо применяются лишь к провайдерам услуг НСП определенного типа. В других юрисдикциях нормативная база, действующая в отношении традиционных кредитно-финансовых учреждений (таких как банки или компании по предоставлению денежных услуг) применяется и в отношении провайдеров услуг НСП, либо же к ним применяются регуляторные требования, разработанные специально для таких провайдеров.

5.1.1 Провайдеры услуг НСП, не подлежащие регулированию

144. В некоторых юрисдикциях регуляторные требования ПОД/ФТ к некоторым провайдерам услуг НСП не применяются. В других юрисдикциях степень регулирования зависит от типа НСП.

145. Эмитенты **предоплаченных карт** подлежат как пруденциальному регулированию, так и регулированию ПОД во всех юрисдикциях, ответивших на вопросы анкеты отчета, на территории которых находятся эмитенты таких карт.[70]

146. Однако если для оказания услуг привлекаются третьи стороны, не соответствующие стандартному определению кредитно-финансового учреждения (например, менеджеры программ банковских карт, розничные продавцы и т.д.), их деятельность обычно регулированию не подлежит. К третьим сторонам относятся также агенты и внешние подрядчики. Более подробно этот вопрос рассматривается в пункте 174 Главы 5.2 («МНПК при использовании агентов / внешних подрядчиков»).

[68] Более подробно этот вопрос рассматривается в пункте 169.
[69] Более подробно этот вопрос рассматривается в пункте 174.
[70] См. таблицу В в Приложении А (предоплаченные карты).

147. Предоставление **услуг Интернет-платежей**. Пятнадцать юрисдикций сообщили о наличии на их территории провайдеров услуг Интернет-платежей. В четырех из указанных юрисдикций такие провайдеры не обязаны регистрироваться или получать лицензию.[71] Соответственно, никакие законодательные требования ПОД/ФТ в этих юрисдикциях к ним не применяются. Одному из таких провайдеров, не подлежащему регулированию (провайдер услуг электронных валют), принадлежит более 11 млн. счетов, открытых клиентами из разных стран мира. Остальные нерегулируемые провайдеры также могут оказывать услуги в глобальном масштабе, хотя и не являются такими же крупными.

148. Третьи стороны, участвующие в предоставлении услуг Интернет-платежей, обычно нужны для зачисления или снятия средств со счета УИП. Некоторые из них могут подлежать регулированию, к другим регуляторные требования могут оказаться неприменимы. Стороны, подлежащие регулированию, обязаны соблюдать обязательства ПОД/ФТ. К ним относятся компании по переводу денежных средств (например, «Вестерн Юнион»), эмитенты предоплаченных карт и банки.

К третьим сторонам, не подлежащим регулированию, требования ПОД/ФТ, как правило, не применяются. К таким третьим сторонам относятся пункты по обмену электронных валют, являющиеся ключевым звеном в бизнес-моделях провайдеров услуг электронных валют, т.к. с их помощью осуществляется обмен электронных валют на обычные деньги или другие электронные валюты.

149. Предоставление **услуг мобильных платежей** подлежит регулированию в большинстве из пятнадцати юрисдикций, сообщивших о наличии на их территории провайдеров таких услуг.[72] Однако в некоторых юрисдикциях данные услуги предоставляют провайдеры, в отношении которых регуляторные требования не применяются (например, телекоммуникационные компании) и которые не имеют каких-либо юридических обязательств ПОД/ФТ.

В Рабочем документе №146[73] Всемирный банк рекомендует обеспечить регулирование деятельности провайдеров услуг мобильных платежей:

«1. ФАТФ следует рассматривать телефонные компании в качестве кредитно-финансовых учреждений (…).

2. После чего группе экспертов следует учитывать финансовые услуги, предоставляемые посредством мобильных телефонов, при использовании методологии оценки выполнения требований ПОД/ФТ соответствующей страной (…)».

[71] См. таблицу В в Приложении А (услуги Интернет-платежей).
[72] См. таблицу В в Приложении А (услуги мобильных платежей).
[73] Рабочий документ Всемирного банка «Безопасность финансовых услуг, предоставляемых посредством мобильных телефонов» №146 (май 2008 года, стр. 53).

150. Провайдеры услуг мобильных платежей зачастую привлекают к работе сторонних агентов – например, для открытия новых клиентских счетов или для расчетов с клиентами наличными средствами. Как правило, количество таких агентов велико, при этом никакие регуляторные требования непосредственно к агентам не применяются.

5.1.2 Провайдеры услуг НСП, в отношении которых применяются регуляторные требования, действующие в отношении провайдеров традиционных финансовых услуг

151. В некоторых юрисдикциях к провайдерам услуг НСП применяются регуляторные требования, действующие в отношении традиционных кредитно-финансовых учреждений. Поэтому такие услуги вправе оказывать только банки или иные традиционные кредитно-финансовые учреждения.

152. В соответствии с регуляторными требованиями всех юрисдикций, ответивших на вопросы анкеты, выпуск **предоплаченных карт многоэмитентных (открытых) систем** вправе осуществлять только кредитно-финансовые учреждения, подлежащие регулированию. Кроме того, разработчики технологии использования банковских карт (такие как Visa, MasterCard) сотрудничают только с кредитно-финансовыми учреждениями, подлежащими регулированию.[74]

153. Хотя юрисдикции и не указали в анкете точные количественные данные, очевидно, что некоторые юрисдикции применяют в отношении **услуг Интернет-платежей**, оказываемых провайдерами услуг НСП, те же правовые и регуляторные требования, что и в отношении традиционных кредитно-финансовых учреждений, остальные же разрешают оказывать услуги НСП только банкам, или рассматривают провайдеров УИП в качестве компаний по предоставлению денежных услуг или по переводу денежных средств.[75]

154. Наконец, в некоторых юрисдикциях **услуги мобильных платежей** могут оказывать только лишь банки или банки совместно с телекоммуникационными компаниями. Как правило, в рамках таких «моделей на базе банка» у каждого клиента имеется отдельный банковский счет, которым он пользуется с помощью мобильного телефона, в результате чего такая услуга является, скорее, разновидностью мобильного банкинга, а не мобильным платежом в значении, в котором он рассматривается в настоящем отчете.

[74] В основном это кредитно-финансовые учреждения, однако к ним могут относиться и иные виды учреждений, подлежащих регулированию, например, учреждения ЕС, оказывающие услуги, связанные с электронными деньгами (см. пункт 5.1.3 «Провайдеры услуг НСП, подлежащие регулированию на основе специально разработанных норм»).

[75] См. таблицы B и C в Приложении A (услуги Интернет-платежей).

155. Несмотря на то, что услуги мобильного банкинга выходит за рамки настоящего отчета, следует сказать, что с ними связаны некоторые проблемы и риски, характерные для услуг мобильных платежей (особенно это касается рисков, возникающих при осуществлении заочных транзакций и использовании агентов, а также при использовании упрощенных МНПК), которые показаны на следующих примерах.

Пример: Мексика

В рамках усилий, направленных на увеличение количества потребителей финансовых услуг, финансовые органы Мексики внедрили модель мобильного банкинга (на основе существующей телекоммуникационной сети), позволяющую жителям страны (в том числе жителям, проживающим в сельских и удаленных районах) пользоваться некоторыми основными банковскими услугами.

В Мексике услуги мобильного банкинга делятся на две категории:

При использовании традиционного мобильного банкинга пользователи мобильных телефонов получают доступ к своему банковскому счету (дебетовая или кредитная карта) с помощью мобильного телефона.

При использовании новой модели мобильных платежей[76] пользователи мобильных телефонов открывают (банковские) счета в телекоммуникационной компании, выступающей в качестве банковского агента. Так называемые «счета для транзакций с небольшой стоимостью» используются только для оказания основных банковских услуг (вклады, снятие средств, совершение входящих и исходящих платежей), а общая сумма транзакций не может превышать около 700 долл. США в месяц, что позволяет применять упрощенные МНПК.[77]

Пример: ЮАР

Для оказания банковской услуги, позволяющей пользователям открывать и активировать счета с помощью телефона, т.е. без личного контакта с сотрудниками или представителями банка, один из южноафриканских банков вступил в партнерские отношения с провайдером услуг мобильной связи. Южно-Африканский резервный банк выпустил инструкцию, определяющую минимальные требования к установлению и проверке личности клиента, подлежащие соблюдению при открытии таких счетов.[78]

[76] Термин «мобильный платеж», использующийся мексиканскими властями, отличается от термина «мобильный платеж», использующегося в настоящем отчете; см. глоссарий.

[77] Подробная информация изложена в пункте 160 главы 5.2 («Определение ситуаций с низкой степенью риска».

[78] Инструкция 06/2008;
http://www.reservebank.co.za/internet/Publication.nsf/LADV/18B4D18670F4E8EC422574520032B728/$File/G6+of+2008.pdf

5.1.3 Провайдеры услуг НСП, подлежащие регулированию на основе специально разработанных норм

156. В некоторых юрисдикциях применяются регуляторные требования, разработанные специально для провайдеров услуг НСП. Например, в Директиве ЕС «Электронные деньги» используется термин «учреждения, осуществляющие операции с электронными деньгами», определяющий новую категорию кредитно-финансовых учреждений. К учреждениям, осуществляющим операции с электронными деньгами, и традиционным кредитно-финансовым учреждениям применяются одинаковые требования ПОД, но разные пруденциальные требования (отличающиеся в части ограничений на деятельность учреждений, осуществляющих операции с электронными деньгами).

Концепция электронных денег, использующаяся в ЕС

В новой редакции Директивы ЕС «Электронные деньги» (пункт 2 Статьи 2)[79], термину «электронные деньги» дано следующее определение:

«Термин "электронные деньги" означает денежную стоимость, которая хранится на электронном (в т.ч. на магнитном) устройстве, представленную требованием на эмитента. Электронные деньги выпускаются эмитентом после получения денежных средств от иных лиц, для совершения платежных операций, определение которым дано в пункте 5 Статьи 4 Директивы 2007/64/ЕС, и принимаются в качестве средства платежа другими (помимо эмитента) физическими или юридическими лицами;…:»

Определение было тщательно сформулировано для того, чтобы обеспечить технологическую нейтральность и включить в него бизнес-модели, в рамках которых стоимость может храниться как на индивидуальном устройстве пользователя (карта, мобильный телефон), так и на центральном сервере эмитента. Поэтому термин «электронные деньги» включает в себя все НСП, рассматриваемые в настоящем отчете.

Право на выпуск электронных денег закреплено за банками и «учреждениями, осуществляющими операции с электронными деньгами» (новая категория кредитно-финансовых учреждений, введенная Директивой ЕС «Электронные деньги»). Кредитно-финансовые учреждения обеих типов подлежат как пруденциальному надзору, так и надзору ПОД/ФТ. В отличие от банков, виды деятельности, которыми могут заниматься учреждения, осуществляющие операции с электронными деньгами, ограничены, и включают в себя a) выпуск электронных денег; b) любые виды платежных услуг, определение которым дано в Директиве ЕС «Платежные услуги»[80]; c)

[79] Директива 2009/110/ЕС; OJ L 267 (10.10.2009), стр. 7;

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:EN:PDF

[80] Директива 1007/64/ЕС; http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:0036:EN:PDF

предоставление кредитов, связанных с оказанными платежными услугами; и d) иные коммерческие операции помимо выпуска электронных денег. При этом такие учреждения не вправе принимать денежные вклады. Для компенсации ограничений по видам деятельности, к учреждениям, осуществляющим операции с электронными деньгами, применяются упрощенные пруденциальные требования. Делается это для того, чтобы облегчить новым участникам выход на рынок.

В соответствии с Директивой ЕС «Электронные деньги» и 3-й Директивой «Отмывание денег», каждое государство-член ЕС вправе применять упрощенные МНПК к продуктам с низкой степенью риска, стоимость которых не превышает определенных значений. Подавляющее большинство государств-членов ЕС уже воспользовалось возможностью применения упрощенных МНПК.[81]

157. В настоящее время США рассматривают возможность введения новой категории компаний по предоставлению денежных услуг - категории «провайдеров предоплаченного доступа».[82] В отличие от законодательства ЕС, о котором говорилось выше, целью данной законодательной инициативы является заполнение регуляторных пробелов, а не облегчение выхода на рынок платежных услуг для новых участников.

5.2 Особенности регулирования и надзора за провайдерами услуг НСП

158. В тех случаях, когда провайдеры услуг НСП подлежат регулированию, надзорным, правоохранительным и законодательным органам сталкиваются с рядом юридических и практических проблем. В отношении некоторых из них определенные рекомендации уже разработаны, а некоторые еще только предстоит изучить.

Далее в настоящем отчете будут рассмотрены следующие вопросы:

- Упрощенные меры по надлежащей проверке клиентов:
  - Определение ситуаций с низкой степенью риска;
  - Освобождение от обязательств ПОД: виды финансовой деятельности и кредитно-финансовые учреждения с низкой степенью риска / клиенты и продукты с низкой степенью риска;
  - Объем МНПК, необходимых для бизнес-моделей с заочными отношениями.
- Провайдеры услуг электронных валют: использование контор по обмену электронных валют;
- МНПК при использовании агентов / внешних подрядчиков;
- «Гибридные» провайдеры услуг;
- Уведомление о подозрительных транзакциях при трансграничных операциях;

[81] Подробная информация о Директиве ЕС «Электронные деньги» и о ее взаимосвязи с Директивой «Платежные услуги» представлена в Приложении D.

[82] См. пункт 161, текстовый блок об «Уведомлении о предполагаемом пересмотре правил» Федерального агентства по борьбе с финансовыми преступлениями США.

- Обеспечение соблюдения законов и осуществление надзора за иностранными провайдерами;
- Установление личности владельцев вторых экземпляров карт.

159. Указанный список не является исчерпывающим и включает в себя главным образом вопросы, связанные с недопущением и привлечением к ответственности лиц, занимающихся отмыванием денег и финансированием терроризма, правовым регулированием и иными аспектами 40+9 Рекомендаций ФАТФ.[83]

Упрощенные меры по надлежащей проверке клиентов

160. В некоторых юрисдикциях кредитно-финансовые учреждения вправе применять упрощенные или сокращенные меры по надлежащей проверке клиентов в ситуациях с низкой степенью риска. При этом какого-либо единого подхода к применению упрощенных или сокращенных МНПК не существует, либо отсутствуют общие критерии (1) признания того или иного продукта низкорисковым продуктом и (2) определения степени, в которой МНПК могут быть сокращены.

Определение ситуаций с низкой степенью риска

161. В некоторых юрисдикциях, ситуации с низкой степенью риска, позволяющие применять упрощенные МНПК, определены законодательно. В большинстве юрисдикций для этой цели используются пороговые значения стоимости и предельные суммы транзакций, которые для провайдеров услуг НСП считаются транзакциями с низкой степенью риска. В других юрисдикциях учитывается большее количество факторов риска, в т.ч. возможность трансграничного использования того или иного продукта, механизмы зачисления средств и ограничения на использование продукта (см., например, подходы, использующиеся в ЮАР, в текстовом блоке ниже). Для получения максимально точной и достоверной оценки риска авторы настоящего отчета рекомендуют учитывать максимально возможное количество факторов риска (перечисленных в таблице рисков выше)[84]. В действующих стандартах ФАТФ каких-либо рекомендаций в отношении ситуаций с низкой степенью риска не предусмотрено, определения ситуаций с низкой степенью риска не имеется, пороговые значения стоимости для провайдеров услуг НСП не указаны. По словам некоторых представителей частного сектора, такие рекомендации были бы полезны.

162. В тех случаях, когда для определения ситуаций с низкой степенью риска используются пороговые значения стоимости, такие значения существенно отличаются в зависимости от юрисдикции (5100 долл. США в год в Швейцарии, 700 долл. США в месяц в Мексике или 1000 долл. США в день в США).[85]

[83] Другие задачи могут включать в себя обеспечение честной конкуренции и создание равных конкурентных условий, обеспечение защиты прав потребителя и т.д.

[84] См. пункт 65 выше.

[85] Некоторые из указанных пороговых значений установлены для продуктов, не являющихся НСП, например, для банковских счетов. Тем не менее, они были включены в настоящий отчет для того, чтобы дать более четкое представление о подходах, использующихся для определения ситуаций с низкой степенью риска.

ЕС:

Подавляющее большинство государств-членов ЕС воспользовалось возможностью предоставления права на применение упрощенных МНПК, предусмотренной пунктом 5d Статьи 11 3-й Директивы «Отмывание денег»[86] (с изменениями и дополнениями, предусмотренными 2-й Директивой ЕС «Электронные деньги»[87]), в котором указано, что государства-члены ЕС вправе разрешить учреждениям применять упрощенные МНПК в отношении электронных денег в тех случаях, когда: «максимальная сумма, хранящаяся в электронном устройстве, не превышает 250 евро (при отсутствии возможности пополнения), или, при наличии возможности пополнения, общая сумма всех транзакций, совершенных в течение календарного года, ограничена лимитом в 2500 евро, за исключением случаев, когда в том же календарном году по требованию владельца электронных денег ему предоставляется сумма в размере 1000 долл. США или более в соответствии со Статьей 11 3-й Директивы «Отмывание денег». В отношении платежных транзакций, совершаемых внутри страны, государства-члены ЕС или их компетентные органы вправе увеличивать указанный лимит в 250 евро до 500 евро».

США:

В соответствии с «Уведомлением о предполагаемом пересмотре правил»[88], новые правила не применяются к некоторым видам предоплаченных платежных инструментов с небольшой стоимостью:

«Предоставление предоплаченного доступа при условии ограничения максимальной стоимости суммой в размере (…), в случае если указанная стоимость четко указана на продукте с предоплаченным доступом» и

(i) не превышает максимальную стоимость, которую можно изначально внести в момент покупки предоплаченного доступа, на 1000 долл. США;
(ii) не превышает общую максимальную стоимость (например, в результате множественных переводов стоимости на один и тот же продукт с предоплаченным доступом), относящуюся к предоплаченному доступу в течение всего периода использования продукта, на 1000 долл. США;
(iii) не превышает максимальную стоимость, которую можно снять с устройства предоплаченного доступа в течение одного дня, на 1000 долл. США.[89]

Новые правила не применяются к предоплаченным платежным инструментам так как считается, *«что возможность их неправомерного использования является незначительной»*.[90]

[86] ДИРЕКТИВА ЕВРОПЕЙСКОГО ПАРЛАМЕНТА И СОВЕТА ЕС 2005/60/ЕС от 26 октября 2005 года о недопущении использования финансовой системы ЕС в целях отмывания денег и финансирования терроризма; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:0036:EN:PDF

[87] ДИРЕКТИВА ЕВРОПЕЙСКОГО ПАРЛАМЕНТА И СОВЕТА ЕС 2009/110/ЕС от 16 сентября 2009 года о создании, внедрении и использовании механизмов пруденциального надзора за коммерческой деятельностью организаций, осуществляющих операции с электронными деньгами, вносящая изменения и дополнения в Директивы 2005/60/ЕС и 2006/48/ЕС, а также аннулирующая Директиву 2000/46/ЕС; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:EN:PDF

[88] См. пункт 182.

[89] «Уведомление о предполагаемом пересмотре правил» (см. пункт 182.), стр. 75.

[90] Тот же источник, стр. 40.

ЮАР:

В мае 2010 года в ЮАР были приняты законодательные акты об освобождении предоплаченных платежных инструментов с небольшой степенью риска от некоторых МНПК. Кредитно-финансовые учреждения, выпускающие такие инструменты, освобождаются от некоторых МНПК при соблюдении следующих условий:

«*(a)* стоимость каждой отдельной транзакции, совершенной с использованием предоплаченного платежного инструмента, не превышает 200 южноафриканских рандов;

(b) доступный остаток никогда не превышает 1500 южноафриканских рандов;

(c) общая сумма денежных средств, зачисленных на предоплаченный платежный инструмент в течение месяца, не превышает 3000 южноафриканских рандов;

(d) предоплаченный платежный инструмент можно использовать только в ЮАР;

(e) пополнение предоплаченного платежного инструмента (необходимо для того, чтобы начать или продолжить его использование) возможно только через какую-либо Интернет-систему с обязательным указанием личного номера клиента;

(f) предоплаченный платежный инструмент нельзя использовать для перевода, обналичивания или получения денежных средств при оплате товаров или услуг, или каким-либо иным способом».[91]

Мексика:

В рамках усилий, направленных на увеличение количества потребителей финансовых услуг, в частности, малообеспеченных слоев населения, в Мексике стали применять упрощенные требования ЗСК и МНПК в отношении некоторых транзакций, продуктов и финансовых услуг. К таким продуктам с низкой степенью риска относятся банковские счета двух типов, которые отличаются от обычных банковских счетов:

Счета для транзакций с небольшой стоимостью предоставляются только физическим лицам, пополняющим счет на сумму, не превышающую 2000 инвестиционных единиц (около 700 долл. США) в месяц. Упрощенные правила действуют в отношении требований ЗСК, требований к открытию счета, мониторинга и предоставления отчетности. [92]

Счета с низкой степенью риска предоставляются физическим и юридическим лицам, осуществляющим транзакции (в т.ч. внесение и снятие денежных средств) на сумму, не превышающую 40 000 инвестиционных единиц (около 14 000 долл. США) в месяц. К таким

[91] [соответствующие законодательные акты ЮАР будут указаны позже].

[92] Регистрируются только основные данные о клиенте (имя, адрес и дата рождения), однако копии документов хранить не нужно. При этом применяется требование, согласно которому заявитель обязан лично предъявить официальное удостоверение личности при открытии счета такого типа.

счетам применяются те же упрощенные правила, то и к счетам для транзакций с небольшой стоимостью, однако для открытия такого счета требуется больше информации о клиенте.[93]

Освобождение от обязательств ПОД: виды финансовой деятельности и кредитно-финансовые учреждения с низкой степенью риска / клиенты и продукты с низкой степенью риска

163. Действующие стандарты ФАТФ обеспечивают юрисдикциям определенную свободу действий, позволяющую им наиболее эффективно распределять свои ресурсы для решения наиболее важных, неотложных проблем ОД/ФТ. Для ситуаций с низкой степенью риска ОД/ФТ, указанные стандарты предусматривают два варианта действий, которые необходимо четко разграничивать: (1) частичное или полное неприменение регуляторных и надзорных обязательств ПОД к видам деятельности и учреждениям с низкой степенью риска и (2) применение упрощенных или сокращенных МНПК к клиентам или продуктам с низкой степенью риска.

1. В соответствии с глоссарием Методологии ФАТФ (см. определение термина «кредитно-финансовое учреждение»), теоретически, частичное или полное освобождение от регуляторных и надзорных обязательств возможно в двух случаях:

a. Юрисдикциям разрешается освобождать или ограничивать применение стандартов ФАТФ в отношении **некоторых видов финансовой деятельности** при условии доказанной низкой степени риска и только в особых, оправданных обстоятельствами случаях;

Пример: Австралия

В соответствии с австралийским Законом ПОД/ФТ, выпуск предоплаченных карт с хранимой стоимостью, а также увеличение стоимости, хранящейся на такой карте, является обособленной услугой (т.е. связанной с рисками ОД/ФТ), в случае если сумма хранящейся стоимости превышает:

- 1000 австралийских долларов, при условии, что денежная стоимость, хранящаяся на карте, может быть полностью или частично обналичена;

или

- 5000 австралийских долларов, при условии, что денежная стоимость, хранящаяся на карте, не может быть обналичена.

В случае если карты с хранимой стоимостью выпускаются на сумму, не превышающую 1000 австралийских долларов, услуги, связанные с такими картами, для целей Закона ПОД/ФТ обособленными услугами не считаются, и поэтому никакие требования ПОД/ФТ, предусмотренные указанным Законом, к ним не применяются.

[93] Регистрируются все данные о клиенте, предусмотренные соответствующими требованиями, однако копии документов хранить не нужно. При этом применяется требование, согласно которому заявитель обязан лично предъявить официальное удостоверение личности при открытии счета такого типа.

b. Кроме того, в случае если определенный вид финансовой деятельности осуществляется физическим или юридическим лицом **нерегулярно или очень редко** (в соответствии с количественными и абсолютными критериями), и риск отмывания денег и финансирования терроризма является незначительным, юрисдикция вправе принять решение о частичном или полном неприменении мер по борьбе с отмыванием денег к такому физическому или юридическому лицу. Данное положение в первую очередь предназначено для применения к нефинансовым учреждениям (таким как, например, отели, которые иногда оказывают своим постояльцам услуги по обмену небольших сумм в иностранной валюте), время от времени осуществляющим некоторые виды финансовой деятельности в рамках своей основной деятельности.

2. В случае если какой-либо вид финансовой деятельности подлежит регулированию и надзору, в соответствии Рекомендацией 5, кредитно-финансовые учреждения обязаны обеспечить выполнение мер по надлежащей проверке клиентов. Степень применения таких мер можно определять на основе оценки риска, с учетом возможного применения **упрощенных или сокращенных МНПК** в ситуациях с низкой степенью риска.

Пример: ЕС

В соответствии с законодательством ЕС, выпуск электронных денег является регулируемой финансовой деятельностью – независимо от пороговых значений стоимости и предельных сумм транзакций, действующих в отношении того или иного продукта. Поэтому деятельность эмитентов электронных денег подлежит регулированию в соответствии с национальными законодательствами государств-членов ЕС.

В соответствии с 3-й Директивой ЕС «Отмывание денег», государства-члены ЕС вправе разрешить своим кредитно-финансовым учреждениям применять упрощенные МНПК в специально определенных ситуациях с низкой степенью риска. Конкретные ситуации с низкой степенью риска указаны в пункте 5d Статьи 11 Директивы (подробная информация изложена в пункте 161 выше).

164. Несмотря на то, что определение термину «упрощенные МНПК» еще не дано (ни в стандартах ФАТФ, ни в нормативных положениях или рекомендациях), Секретариат ФАТФ рекомендует предоставлять освобождение от применения МНПК только в случаях, указанных в варианте 1), и не предоставлять его в случаях, указанных в варианте 2). Следовательно, освобождение компаний, которые осуществляют специально определенную финансовую деятельность и, следовательно, обязаны выполнять обязательства ПОД/ФТ, от применения МНПК, является нарушением положений Рекомендации 5.[94] Поэтому в течение последних пяти лет в адрес более десяти

[94] ФАТФ также подтвердила такое толкование Рекомендации 5 в нескольких публикациях, посвященных использованию подхода, основанного на оценке риска (см. «Руководство по применению подхода, основанного на оценке риска, для противодействия отмыванию денег и финансированию терроризма: общие принципы и процедуры», июнь 2007 года, пункты 1.24 и 1.26 (стр. 6); «Подход, основанный на оценке риска: руководство для компаний по предоставлению денежных услуг», июль 2009 года, пункт 48 (стр. 14)).

юрисдикций звучала критика за предоставление освобождений от МНПК в ситуациях с низкой степенью риска.[95]

165. Несмотря на вышесказанное, несколько юрисдикций заявляют, что до тех пор, пока в стандартах ФАТФ не появится определение термина «упрощенные или сокращенные МНПК», освобождение от МНПК можно считать случаем применения упрощенных или сокращенных МНПК и, соответственно, что текст Рекомендации 5 не исключает возможности предоставления освобождений в ситуациях с низкой степенью риска. Например, по законодательству ЕС государства-члены ЕС вправе освободить эмитентов электронных денег от применения МНПК в специально определенных ситуациях с низкой степенью риска[96,97], и многие государства-члены ЕС воспользовались данной возможностью. В результате несколько продуктов НСП, выпускаемых в ЕС, являются, по сути, анонимными.[98]

Объем МНПК, необходимых для бизнес-моделей с заочными отношениями

166. Вопросы, связанные с заочными операциями, учтены в Рекомендации 8, в которой по этому поводу сказано следующее: «*кредитно-финансовые учреждения должны применять правила и процедуры, позволяющие им противодействовать любым* ***конкретным рискам****, связанным с заочными деловыми отношениями или транзакциями*». Несмотря на то, что словосочетание «высокая степень риска» в Рекомендации 8 не используется, в Пояснительном примечании к Рекомендации 5 (пункт 7) говорится о конкретных рекомендациях, изложенных в Базельском докладе о МНПК (раздел 2.2.6), в котором, в частности, сказано следующее:

«48. При осуществлении заочных транзакций с клиентами (...) необходимо применять конкретные и надлежащие меры для снижения ***высоких рисков****».*

Также, Секретариат ФАТФ сообщил составителям отчета о том, что при подготовке к 4-му раунду взаимных оценок специалисты ФАТФ пришли к однозначному выводу о том, что заочные деловые отношения или транзакции характеризуются ***высокой степенью риска ОТ/ФТ***.

167. В Рекомендации 5 говорится о том, что *«кредитно-финансовым учреждениям следует применять усиленные МНПК в отношении* ***категорий с высокой степенью риска****».*

Кроме того, в Пояснительном примечании к Рекомендации 5 (пункт 13) сказано следующее:

---

[95] Указанные освобождения не всегда предоставлялись в отношении услуг НСП.

[96] Европейская комиссия подтвердила такое толкование Статьи 11(5)(d) 3-й Директивы «Отмывание денег» 2005/60/ЕС в своих ответах на вопросы анкеты отчета.

[97] В Статьях 11 и 40 Директивы 2005/60/ЕС и в Статье 3 Директивы 2006/70/ЕС, Европейская комиссия определила технические критерии признания определенных ситуаций ситуациями с низкой степенью риска.

[98] В основном это денежные сертификаты и некоторые предоплаченные карты (многоэмитентных (открытых) и одноэмитентных (закрытых) систем), при выдаче которых провайдеры УИП обычно узнают, по крайней мере, имя клиента (но не всегда проверяют его).

«Упрощенные МНПК не применяются **во всех случаях, когда** возникает подозрение в отмывании денег или финансировании терроризма или **имеется вероятность возникновения конкретных ситуаций с высокой степенью риска**».

При этом в стандартах ФАТФ не указано, равнозначен ли «особый риск» в значении Рекомендации 8 «ситуациям с высокой степенью риска» в значении Рекомендации 5. Если такие риски тождественны, упрощенные МНПК к продуктам НСП с заочными отношениями применять не следует.

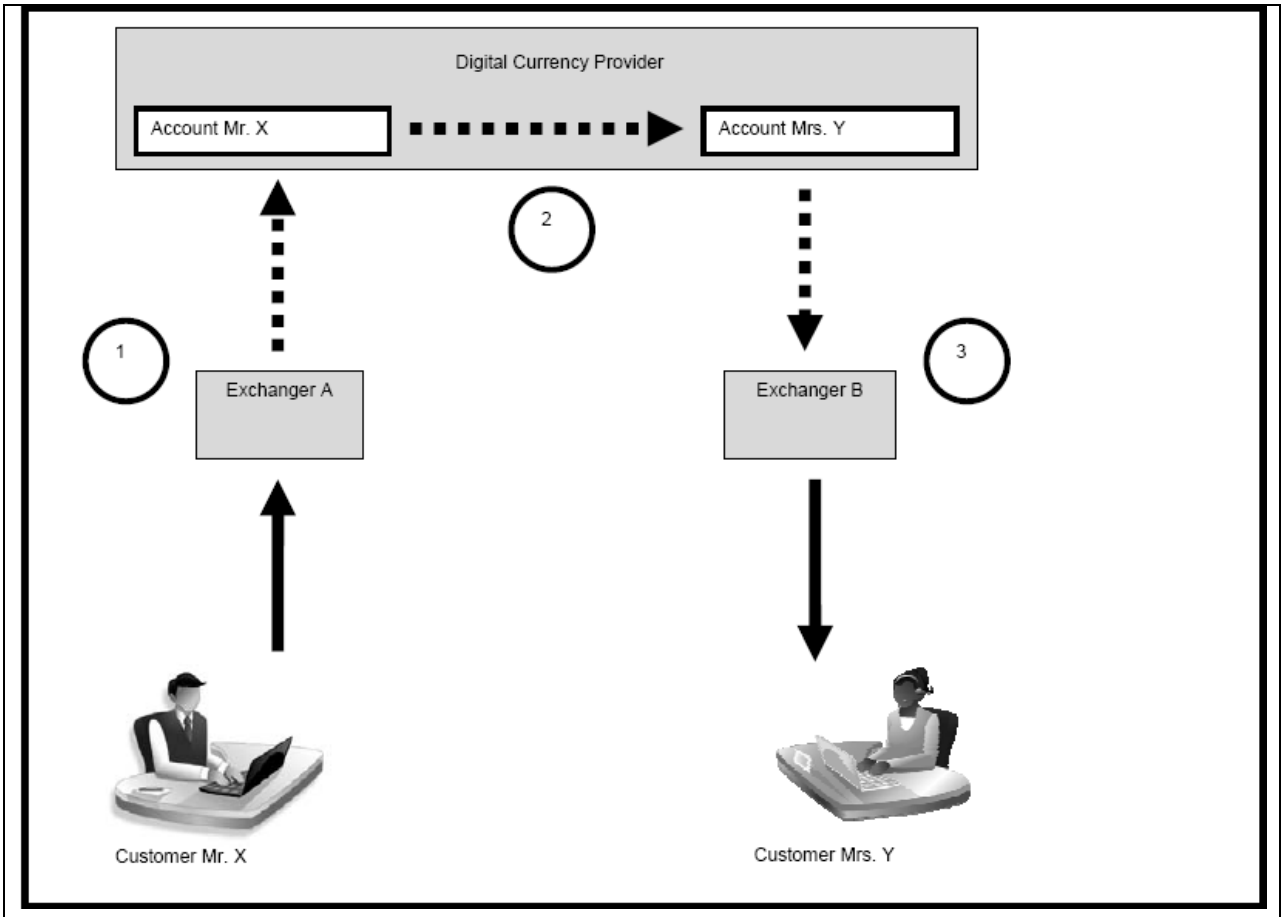
168. В случае если степень риска, связанного с тем или иным продуктом, определяется на основе одного, основного фактора риска (который в данном случае представлен заочным характером транзакций), принципы оценки риска, изложенные в отчете о НСП 2006 года (которых придерживались авторы данного отчета), останутся за рамками такой оценки. Согласно указанным принципам, при оценке риска, связанного с конкретной услугой или продуктом НСП, необходимо учитывать все факторы риска, указанные в таблице рисков (пункт 65 настоящего отчета). Заочный характер деловых отношений и транзакций действительно увеличивает степень риска, связанного с той или иной услугой или продуктом НСП, однако другие характеристики (например, эффективные процедуры установления и проверки личности клиента или жесткие пороговые значения стоимости) могут существенно снизить такой риск и даже привести к тому, что продукт или услуга будут считаться низкорисковыми. Поэтому требование к применению усиленных МНПК по отношению к таким бизнес-моделям не является обязательным, и в некоторых ситуациях с низкой степенью риска к ним могут применяться упрощенные МНПК.

169. Составители отчета были уведомлены о том, что данный вопрос обсуждался экспертами ФАТФ на недавнем заседании подгруппы EGA Рабочей группы ФАТФ по оценке и внедрению (РГОВ). Участники заседания пришли к выводу, что бизнес-модели с заочными отношениями, считающиеся в соответствии со стандартами ФАТФ бизнес-моделями с высокой степенью риска, не обязательно тождественны «ситуации с высокой степенью риска» в значении Рекомендации 5. Было бы уместно указать на это в стандартах ФАТФ (например, в Пояснительном примечании к Рекомендации 5 или Рекомендации 8).

Провайдеры услуг электронных валют: использование контор по обмену электронных валют

170. Сегментация услуг в бизнес-моделях, использующихся провайдерами услуг электронных валют, не позволяет однозначно определить лицо, которое является провайдером платежных услуг и, следовательно, подлежит регулированию.

171. На схеме ниже показана сегментация услуг, которые предоставляются в рамках одной из бизнес-моделей, использующихся провайдерами услуг электронных валют. Платеж совершается в три этапа, за каждый из которых отвечает три разных юридических лица:



Digital currency provider	Провайдер услуг электронных валют
Customer Mr. X	Г-н X, клиент
Exchanger A	Пункт по обмену валют A
Account Mr. X	Счет г-на X
Account Mrs. Y	Счет г-жи Y
Exchanger B	Пункт по обмену валют B
Customer Mrs. Y	Г-жа Y, клиент

Этап 1: зачисление средств на счет клиента

Клиент X вносит определенную сумму обычными деньгами в пункт по обмену валют A, который имеет определенную сумму в электронной валюте. В обмен на полученные деньги, пункт по обмену валют перечисляет со своего счета электронной валюты эквивалентную сумму на счет электронной валюты клиента X.

Этап 2: зачисление средств на счет клиента

Клиент X поручает провайдеру услуг электронных валют перечислить определенную сумму в электронной валюте на счет электронной валюты клиента Y.

Этап 3: снятие средств

Клиент Y перечисляет определенную сумму в электронной валюте со своего счета электронной валюты на счет электронной валюты пункта по обмену валют B. В обмен на полученную сумму в электронной валюте пункт по обмену валют перечисляет эквивалентную сумму обычных денег клиенту Y.

Источник: Составители отчета о НСП

172.В некоторых юрисдикциях ни один из указанных этапов сам по себе не считается регулируемой деятельностью:

- Конторы по обмену электронных валют меняют обычные деньги на электронные деньги или даже электронные деньги одного провайдера на электронные деньги другого провайдера. Они переводят стоимость, но только между счетами одного и того же лица, и не переводят деньги на счета третьих сторон.
- Провайдер услуг электронных валют переводит стоимость от одного лица другому, однако при этом такой провайдер не получает обычных денег от плательщика и не выплачивает обычные деньги получателю платежа.

173. Другие юрисдикции полагают, что такие виды деятельности являются регулируемыми, и что лица, которые их выполняют, подлежат регулированию:

США: компании по предоставлению денежных услуг

В рамках судебного дела, возбужденного в отношении иностранного провайдера, предлагавшего гражданам США услуги Интернет-платежей, был поднят вопрос о необходимости применения национального законодательства, действующего в отношении учреждений, оказывающих услуги по перечислению денежных средств, ко всем провайдерам, участвующим в совершении Интернет-платежей. В США используется следующее определение учреждений, оказывающих услуги по перечислению денежных средств (приводится частично):

«Любое лицо, независимо от того, имеет ли оно соответствующую лицензию или нет, или

должно ли оно иметь соответствующую лицензию или нет, которое занимается деятельностью, связанной с принятием валют или денежных средств, выраженных в валюте, и перечислением такой валюты или денежных средств, или стоимости такой валюты или денежных средств, с помощью каких-либо средств…»

Помимо эффективного применения данного определения и обеспечения соблюдения национальными провайдерами услуг Интернет-платежей (в т.ч. провайдерами услуг электронных валют) требований к учету и отчетности, органы прокуратуры США обеспечили эффективное применение аналогичных механизмов и к иностранным провайдерам, осуществляющим отправку и получение денежных средств для клиентов из США.

Германия: компании по предоставлению денежных услуг

В соответствии с немецким Законом о банках, надзорные органы ФРГ вправе издавать приказы о прекращении противоправного действия не только в отношении юридических лиц, занимающихся незаконной коммерческой деятельностью, но и в отношении организаций, участвующих в подготовке и осуществлении такой деятельности.

Кроме того, провайдер считается «фактическим филиалом» кредитно-финансового учреждения в случае, если он участвует (осуществляет «частичные действия») в предоставлении такому учреждению какой-либо финансовой услуги. Поэтому такой «фактический филиал» подлежит лицензированию, за исключением случаев, когда кредитно-финансовое учреждение, на которое он работает, лицензировано в ФРГ или другом государстве Европейской экономической зоны.

Руководствуясь вышеуказанными принципами, власти ФРГ инициировали разбирательство по делу об административном правонарушении в отношении нелицензированной конторы по обмену электронных валют, обосновавшейся в Германии и осуществлявшей торговые операции с цифровыми деньгами провайдера из Юго-Восточной Азии. Разбирательство по делу об административном правонарушении продолжается.

174. Проблема регулирования и надзора за деятельностью провайдеров услуг электронных валют и связанных с ними юридических лиц (таких как, например, пункты по обмену электронных валют) усугубляется еще и тем, что во многих случаях такие услуги не требуют физического присутствия провайдера в соответствующей юрисдикции и могут предоставляться из любой точки мира через Интернет. Поэтому юридические лица, участвующие в предоставлении таких услуг, могут выбрать для себя такую страну, в которой они не подлежат регулированию, и оказывать услуги оттуда.

МНПК при использовании агентов / внешних подрядчиков[99]

[99] Для целей настоящего отчета, термины «агент» и «привлечение внешних подрядчиков» используются в качестве синонимов. РГОВ ФАТФ была создана рабочая группа по вопросам, связанным с Рекомендацией 9, работавшая над разграничением таких понятий, как «агентское соглашение», «соглашение о привлечении

175. МНПК и другие меры ПОД обычно осуществляются самими служащими или сотрудниками кредитно-финансового учреждения, подлежащего регулированию. Однако во многих бизнес-моделях НСП к выполнению указанных задач часто привлекаются третьи стороны – агенты, посредники, внешние подрядчики. И хотя в этом случае такие отношения могут относиться к разным правовым концепциям, предусматривающим разные правовые обязательства и требования, для целей настоящего отчета такие концепции считаются равноценными.

В 40+9 Рекомендациях ФАТФ использование агентов и внешних подрядчиков рассматривается в двух разных документах, а именно, в Рекомендации 9 и в Специальной Рекомендации VI.

176. В Рекомендации 9 данный вопрос рассматривается частично: затрагиваются только вопросы привлечения и доверия к третьим сторонам, при этом ничего не сказано об агентских соглашениях и соглашениях о привлечении внешних подрядчиков, не содержится определений агентской деятельности и деятельности по привлечению внешних подрядчиков. При этом практически единственным местом в стандартах ФАТФ, в котором четко изложен текущий подход ФАТФ к использованию агентов и внешних подрядчиков, является ссылка в тексте Методологии, прилагаемой к Рекомендации 9: «*внешнего подрядчика или агента следует рассматривать в качестве лица, тождественного кредитно-финансовому учреждению, т.е. в качестве лица, которое должно использовать те же процедуры и документацию, что и само кредитно-финансовое учреждение*».[100]

177. Единственной Рекомендацией, в которой четко говорится об агентах, является СР VI: *«каждая страна должна принять меры к тому, чтобы физические или юридические лица, в т.ч. агенты, оказывающие услуги, связанные с перечислением денежных средств или стоимости, в т.ч. посредством неформальной системы или сети для перечисления денежных средств или стоимости, имели лицензию или были зарегистрированы, и руководствовались всеми Рекомендациями ФАТФ, применимыми к банкам и небанковским кредитно-финансовые учреждениям»*. В Пояснительном примечании к СР VI агентам дано следующее определение: *«любое лицо, оказывающее услуги по перечислению денежных средств или стоимости под руководством или по договору с официально зарегистрированной или имеющей официальную лицензию компанией по переводу денежных средств (например, владельцы лицензий, франшизополучатели, дилеры)»*.

178. В соответствии с наиболее распространенным толкованием СР VI, в ней также не содержится требований о том, что агенты должны подлежать надзору и соблюдать обязательства ПОД сами по себе, автономно от принципала. Несмотря на то, что формулировка СР VI может давать основания и для других толкований, данный вывод подтверждается определением понятия «агент», которое дано этому термину в глоссарии методологии (и которое подразумевает, что агенты подчиняются принципалу, подлежащему регулированию) и Пояснительным примечанием к СР VI, в пункте 8

внешних подрядчиков» и «привлечение третьих сторон». Специалисты группы пришли к предварительному заключению, что концепции агентской деятельности и привлечения внешних подрядчиков «отличаются в зависимости от страны и в некоторых случаях даже от вида финансовой деятельности (документ ФАТФ WGEI(2010)45, стр. 3).

[100] Примечание 16 в Методологии оценки соответствия требованиям 40 Рекомендаций ФАТФ и 9 Специальных Рекомендаций ФАТФ.

которого сказано, что достаточно того, что принципал постоянно ведет *«список агентов, подлежащий передаче в соответствующий компетентный орган»*.

179. В соответствии с данными принципами, изложенными в действующих стандартах ФАТФ, в большинстве юрисдикций в отношении агентов и внешних подрядчиков, привлеченных кредитно-финансовыми учреждениями, законы или регуляторные нормы ПОД, как правило, не применяются, и поэтому сами по себе они не обязаны соблюдать какие-либо требования ПОД/ФТ.[101] Вместо этого, принципал (или аутсорсер), будучи регулируемым учреждением, является единственным лицом, ответственным за соблюдение обязательств ПОД/ФТ при осуществлении своей деятельности, в т.ч. и за действия (бездействие) своих агентов или внешних подрядчиков. Упущения агента считаются упущениями его принципала (например, кредитно-финансового учреждения), который может быть наказан за нарушение имеющихся у него обязательств ПОД/ФТ, совершенное его агентом.

Говоря о компаниях по предоставлению денежных услуг, нужно упомянуть, что ФАТФ были опубликованы рекомендации по работе с агентами, содержащие некоторую полезную информацию о требовании «знай своего клиента», мониторинге и обучении агентов. И хотя нигде четко не сказано, что указанные рекомендации относятся к провайдерам услуг НСП, скорее всего, они применимы и к указанным провайдерам.

180. Некоторые юрисдикции, в т.ч. США и ФРГ, проанализировав использующиеся ими подходы, пришли к выводу о наличии определенных регуляторных пробелов. Теперь они предлагают применять юридические обязательные требования ПОД/ФТ также и к агентам. В данном случае термин «агент» может относиться к лицам, осуществляющим множество различных видов деятельности, включая в себя, например, менеджеров программ банковских карт или продавцов платежных инструментов с предоплаченными денежными средствами.

а) Менеджеры программ банковских карт

181. В некоторых бизнес-моделях руководство программами предоплаченных карт фактически осуществляется менеджерами программ банковских карт. Менеджеры программ банковских карт могут владеть такими бизнес-моделями, контролировать их и принимать важные деловые решения, тогда как банк-эмитент может всего лишь обеспечивать доступ к средствам технического обслуживания карт. Поэтому в определенных бизнес-моделях НСП менеджер программ банковских карт может играть более важную роль, чем обычный внешний подрядчик или агент.[102] Несмотря на это, менеджер программ банковских карт (так же, как и обычный агент) обычно не подлежит надзору и не обязан соблюдать требования законодательства ПОД/ФТ – юридическая

[101] Во многих случаях агенты обязаны соблюдать договорные обязательства ПОД/ФТ, предусмотренные агентским соглашением, которое они заключают с принципалом. Однако в этом случае прямой юридической ответственности агенты не несут, а органы власти не вправе применять к ним меры наказания в случае нарушения агентами своих договорных обязательств ПОД/ФТ. Как правило, законодательство не обязывает принципала налагать на агентов договорные обязательства ПОД/ФТ.

[102] В определении термина «агент» для целей СР IV, представленного в глоссарии Методологии ФАТФ, сказано, что агенты работают «*под руководством или по договору с официально зарегистрированной или имеющей официальную лицензию компанией по переводу денежных средств»*. Поэтому агент обычно считается лицом, подчиненным принципалу, т.е. кредитно-финансовому учреждению.

ответственность за соблюдение правовых и регуляторных обязательств лежит на кредитно-финансовом учреждении-эмитенте.

Проблема с разделением ответственности на коммерческую и юридическую ответственность усугубляется в тех случаях, когда менеджер программ банковских карт и банк-эмитент находятся в разных юрисдикциях. Например, в случае, если менеджер программ банковских карт расположен в юрисдикции с жесткими регуляторными требованиями (которые, тем не менее, к менеджеру программ банковских карт не применяются), такие жесткие требования можно обойти, сотрудничая с банком, расположенным в юрисдикции, в которой применяются менее строгие стандарты ПОД/ФТ или надзорные требования.

182. Еще одной проблемой подобного рода является регулирование выхода на рынок. Поскольку в настоящий момент большинство менеджеров программ банковских карт регулированию и надзору не подлежат, требования к выходу на рынок (например, проверка на профессиональную пригодность и добросовестность надзорными органами) к ним не применяются. Поэтому учреждения-эмитенты определяют законность намерений агента/менеджера программ самостоятельно. В результате анализа конкретных примеров было обнаружено, что некоторые учреждения не сумели определить незаконность намерений своих менеджеров программ банковских карт или даже намеренно шли на сговор с менеджерами программ банковских карт, действующих незаконно (см. раздел 4 «Типологии» (*примеры 22 и 28*) выше).

183. Как следствие, некоторые юрисдикции рассматривают возможность применения юридически обязательных требований ПОД/ФТ к менеджерам программ банковских карт и иным третьим сторонам. Полностью ни одна такая инициатива пока что реализована не была. Наиболее близко к осуществлению таких намерений приблизились США. Федеральное агентство по борьбе с финансовыми преступлениями США разработало соответствующее «Уведомление о предполагаемом пересмотре правил» (УППП), которое было вынесено на общественные слушания 28 июня 2010 года.[103]

В «Уведомлении о предполагаемом пересмотре правил» указанное Федеральное агентство предлагает использовать новую категорию компаний по предоставлению денежных услуг (КПДУ) – «провайдер предоплаченного доступа». О провайдерах предоплаченного доступа Федеральное агентство по борьбе с финансовыми преступлениями США говорит следующее:

«В большинстве случаев данный термин будет применяться к любому лицу, осуществляющему надзор и контроль за использованием какой-либо предоплаченной программы. Применимость данного термина к тому или иному участнику транзакций, осуществляющихся в рамках соответствующей программы, определяется на основе конкретных фактов и обстоятельств; мы не «закрепляем» данный термин за той или иной функцией. Мы признаем вероятность возникновения ситуаций, в которых ни одна из сторон не будет осуществлять единоличный контроль. Тем не менее, мы действительно считаем, что при осуществлении транзакций одна из сторон всегда отвечает за

[103] http://edocket.access.gpo.gov/2010/pdf/2010-15194.pdf

принятие решений в большей степени, чем другие стороны. Мы хотели бы четко и недвусмысленно заявить, что лицо, являющееся провайдером предоплаченного доступа, не может быть определено произвольным решением участников программы. Так же, как и при определении категории других КПДУ, провайдер предоплаченного доступа определяется на основе совокупности фактов и обстоятельств, относящихся к осуществляемой деятельности, тогда как какое-либо одно действие или обязанность не само по себе может быть определяющим. Несмотря на то, что представленный ниже список не является исчерпывающим, мы считаем, что указанные в нем виды деятельности позволяют эффективно определить основного участника:

- *Сторона, от имени которой предоплаченная программа продается покупателям. Например, от имени какой стороны заявлено о выпуске нового продукта? Чье имя используется в печати, в Интернет-объявлениях и на самой карте/устройстве? В соответствии с юридической практикой, действия физического или юридического лица, направленные на то, чтобы представить себя в качестве основного участника, являются одним из важнейших признаков основного участника.*
- *Сторона, которую «здравомыслящий человек» посчитал бы основным участником серии транзакций – основное лицо, принимающее решения.*
- *Сторона, которую банк-эмитент считает своим основным представителем по защите своих сетевых отношений и обеспечению целостности своего бренда.*
- *Сторона, определяющая методы дистрибуции и стратегии сбыта.*
- *Сторона, чьи опыт и знания в области предоплаченных продуктов признаются другими сторонами, в частности, банком-эмитентом, в качестве важнейшего средства, позволяющего создавать успешные программы за счет привлечения наиболее подходящих сторон.*

На примере вышеуказанных характеристик мы бы хотели показать, что единого определяющего фактора не существует: провайдер предоплаченного доступа не обязан осуществлять или воздерживаться от осуществления какого-либо одного вида деятельности. Определить, что то или иное лицо является провайдером предоплаченного доступа, возможно лишь на основе целого ряда, совокупности фактов и обстоятельств».

Так как провайдеры предоплаченного доступа представляют собой одну из категорий КПДУ, они обязаны зарегистрироваться в Федеральном агентстве по борьбе с финансовыми преступлениями США. В соответствии с УППП, такие провайдеры обязаны внедрить и использовать программы ПОД (в т.ч. обучение персонала), обеспечить сбор данных, необходимых для установления личности клиентов, вести учет транзакций и хранить соответствующие данные в течение пяти лет, а также предоставлять ОПТ и ОПД. Федеральное агентство по борьбе с финансовыми преступлениями США также предлагает наложить вышеуказанные обязательства и на «продавцов» предоплаченного доступа, однако при этом их не следует считать КПДУ и, соответственно, не требовать от них регистрации в Федеральном агентстве по борьбе с финансовыми преступлениями США.

Новые обязательства провайдеров и продавцов предоплаченного доступа никак не влияют на правовую ответственность банков или кредитно-финансовых учреждений, связанных с такими провайдерами и продавцами: их обязательства ПОД остаются неизменными.

b) Продавцы платежных инструментов с предоплаченными денежными средствами

184. Некоторые провайдеры услуг НСП используют для продажи своего продукта клиентам сеть партнеров (например, предприятия розничной торговли, аптеки и т. д.). В одних юрисдикциях такие партнеры рассматриваются как агенты, действующие от имени провайдера услуг НСП, а в других — как обычные получатели платежей.

США

В описанном выше уведомлении о предлагаемых правилах (NPRM)[104] Федеральное агентство по борьбе с финансовыми преступлениями (FinCEN) предложило возложить обязательства в области ПОД/ФТ не только на банк-эмитент и «поставщиков предоплаченного доступа», но и на продавцов предоплаченных продуктов:

«Мы также принимаем во внимание тот факт, что очень важную роль среди всех типовых партнеров играет продавец. Именно продавец имеет дело с покупателями и получает информацию, недоступную для остальных участников операционной цепочки. По этой причине мы считаем, что из всех задействованных в программе сторон второе по важности место занимает продавец. (…) У продавца уникальная позиция — он наблюдает первый этап формирования отношений предоплаты и напрямую взаимодействует с покупателем, который может быть или не быть конечным пользователем покупаемой карты. Предъявляемые к этой стороне требования о хранении данных в течение пяти лет и сообщении о подозрительной активности также служат системе охраны правопорядка.

(…)

Продавец предоплаченного доступа — это сторона, которая больше всего контактирует с покупателями, а значит, в отличие от других участников операционной цепочки, является ценным ресурсом для получения информации в точках продаж. Как правило, в качестве продавца выступает предприятие розничной торговли общего профиля, предлагающее всю линейку продуктов через хозяйственное подразделение, например, аптеку, магазин шаговой доступности, супермаркет, магазин уцененных товаров или любую другую торговую точку. Именно потому, что эта сторона лично взаимодействует с покупателем и имеет возможность фиксировать уникальную информацию в ходе осуществления сделок, мы считаем, что продавец должен прямо подчиняться стандартам.

Поскольку роль продавца носит дополнительный характер и не эквивалентна полномочиям и первенству провайдера предоплаченного доступа, мы предпочитаем не требовать регистрации в FinCEN. Мы считаем, что в целом продавец действует как представитель провайдера, и такая трактовка соответствует определению других агентов в правилах MSB.

В то же время наличие агентов не освобождает продавца от соблюдения других обязательств, накладываемых в соответствии с данным предлагаемым правилом: (1) поддержка эффективной программы ПОД, (2) сообщение о подозрительных операциях или действиях и (3) учет идентификационной информации и переменных данных клиентов».

185. Так в Австралии, кроме выпуска предоплаченных карт, одной из услуг, при оказании которых провайдеры становятся субъектами первичного финансового мониторинга по австралийскому закону о ПОД/ФТ и принимают на себя ряд важных обязательств, считается деятельность по «увеличению денежной стоимости» определенных карт с хранимой стоимостью[104] (т. е. загрузка и перезагрузка средств на карты). Сюда входит требование о наличии программы ПОД/ФТ, идентификация и надлежащая проверка клиентов, учет и обязательства по отчетности.

186. Другие юрисдикции не разделяют описанную выше точку зрения, т. е. то, что действующий подход к агентам не соответствует стандартам, и не поддерживают идею о подчинении агентов требованиям ПОД. В качестве альтернативы было предложено подкрепить или разъяснить требования к соглашениям финансовых учреждений об аутсорсинге или посредничестве, особенно в том, что касается обязательств в области ПОД/ФТ. Во многих юрисдикциях действует законодательство о требованиях к договорам аутсорсинга, но в настоящее время в 40+9 рекомендациях ФАТФ это не отображено.

«Гибридные» провайдеры услуг

[104] См. выше, пар. 182.

[104] Австралийский закон о ПОД/ФТ, табл. 1, п. 23.

187. Некоторые нефинансовые коммерческие компании занялись оказанием услуг НСП (например, телекоммуникационные компании предоставляют услуги мобильных платежей). Такие «гибридные» провайдеры платежных сервисов могут создавать определенные сложности для действующих режимов регулирования, поскольку в связи с осуществлением финансовой деятельности во многих юрисдикциях они либо исключаются из рынка (поскольку подобной деятельностью могут заниматься только кредитные организации)[105], либо регламентируются законоположениями, регулирующими все их специализации, а не только финансовую деятельность. Кроме того, если гибридным провайдером является большая компания, то во многих юрисдикциях использование законодательных освобождений будет невозможно.

188. Такие препятствия могут либо подтолкнуть заинтересованных гибридных провайдеров к предоставлению финансовых услуг через отдельное юридическое лицо, ориентированное на финансовые услуги, либо отпугнуть потенциальных кандидатов от выхода на рынок НПС.

Пример ЕС

Новый режим ЕС для выпуска электронных денег с изменениями, внесенными второй директивой об электронных деньгах (EMD), направлен на упрощение доступа к рынку для новых участников, а именно телекоммуникационных компаний и крупных предприятий розничной торговли, желающих выйти на рынок электронных денег. После принятия Директивы о платежных услугах к организациям, работающим с электронными деньгами, больше не будет применяться принцип исключительности. Теперь наряду с выпуском электронных денег они смогут заниматься и любой другой коммерческой деятельностью (ст. 6, пар. 1, п. (e) EMD).

При расчете собственных средств или требований по гарантиям организации, работающей с электронными деньгами, учитываются только те средства, которые относятся к работе с электронными деньгами, а средства, относящиеся к другим сферам деятельности, в расчет не берутся (границы балансовой принадлежности четко обозначаются).

Сообщения о подозрительных транзакциях в трансграничных ситуациях

189. Предоставление трансграничных услуг, свойственное многим бизнес-моделям НПС (в частности большинству провайдеров услуг интернет-платежей), поднимает проблемы сообщения о подозрительных транзакциях и эффективности обеспечения правопорядка. В большинстве юрисдикций провайдеры НСП обязаны сообщать о подозрительных транзакциях только в местное ПФР, даже если связанные с ними лица (клиенты, отправители, получатели) находятся в другой стране. ПФР соответствующей страны будет зависеть от эффективности международного сотрудничества и обмена информацией с ПФР той страны, где находится провайдер НСП. Если такого сотрудничества нет, эффективность режима сообщений о подозрительных транзакциях и обеспечения правопорядка в подозрительных случаях будет незначительной.

190. Если агенты используются для предоставления трансграничных услуг, ситуация аналогична. В большинстве юрисдикций режим сообщения о подозрительных транзакциях на агентов не распространяется. Если они и сообщают о подозрительных транзакциях, то, скорее всего, своим принципалам (т. е. провайдеру услуг НСП) в договорном порядке. Как описано выше, после этого провайдер НСП подает ОПТ в ПФР своей страны, но не обязательно в ПФР той страны, где находится агент.

Правоприменение и надзорная деятельность в отношении иностранных провайдеров

191. Если провайдеры НСП предоставляют свои услуги в других странах только через Интернет (т. е. без физического присутствия в юрисдикции клиента), иностранные органы власти

[105] См. выше главу 5.1.2 («согласно действующим стандартам в отношении традиционных финансовых услуг»), пар. 150.

ограничены в мерах воздействия и обычно вынуждены полагаться на аналогичные органы той юрисдикции, где находится провайдер.

192. Однако некоторые национальные органы власти успешно приняли меры воздействия против иностранных провайдеров с помощью средств уголовного и административного права собственной страны.

ЕС
В комитете ЕС по борьбе с отмыванием денег и финансированием терроризма (CPMLFT) в настоящее время обсуждается, какая отчетность подразделения финансовой разведки должна оформляться в трансграничных ситуациях, а также вопросы распределения компетенции между органами надзора за ПОД, если согласно Директиве о платежных услугах платежная организация пользуется услугами агентов для продажи услуг в государстве-члене ЕС, отличном от страны ее учреждения. Если возникла эта дискуссия в связи с агентами по услугам денежных переводов, то ее результат повлиял непосредственно на провайдеров НПС, к которым применяются те же положения, что и к агентам.

193. Например, власти США использовали положения уголовного права США для применения санкций к иностранным провайдерам, находящимся на о. Мэн (см. выше **дело 31**) и на островах Карибского (см. выше **дело 33**). Применение национальных санкций стало возможным, поскольку ответчики (т. е. директора и владельцы иностранных провайдеров) либо проживали в США, либо находились на их территории.

194. Немецкие власти издали административные приказы о запрещении продолжения противоправных действий в отношении провайдеров услуг интернет-платежей, находящихся в Юго-Восточной Азии и Центральной Америке. Согласно немецким законам о надзоре, такие меры могли быть приняты только в том случае, если деятельность осуществлялась в Германии. Тем не менее, при соблюдении определенных условий власти рассматривали услуги, оказываемые из-за границы, как имеющие место «в Германии». Что касается предоставления финансовых услуг через Интернет, то такая деятельность будет считаться осуществляемой в Германии, если содержимое веб-сайта ориентировано на немецкий рынок. На это указывают следующие признаки (список не полный): домен веб-сайта (.de), веб-сайт на немецком языке, информация для клиентов, характерная для Германии или немецкого финансового сектора, ссылки на законодательную базу Германии и контактные лица в Германии.

Идентификация держателей дополнительных карт

195. Некоторые провайдеры предоплаченных карт выпускают карты, предназначенные специально для упрощения трансграничных денежных переводов. В подобных бизнес-моделях клиент (владелец) получает основную карту и может передать одну или несколько дополнительных карт (которые также называются «партнерскими» и «картами для переводов») третьим лицам — целевым получателям транзакций по переводу денежных средств. После этого деньги переводятся в два этапа: сначала владелец карты вносит сумму перевода на предоплаченную карту, а затем получатели с помощью своих дополнительных карт могут снять эту сумму через любой банкомат.

196. В некоторых из таких бизнес-моделей устанавливается личность только держателя основной карты. Держатели дополнительных карт часто остаются неизвестными для эмитента.

197. В отчете о взаимной оценке по Новой Зеландии за 2009 г. одна такая бизнес-модель и соответствующая надзорная практика описаны подробно:

ОВО по Новой Зеландии за 2009 г.

Согласно ОВО на момент проведения оценки, при наличии трех или более «держателей средств» (т. е. держателей счета или карты) финансовые учреждения в Новой Зеландии обычно «обязаны проверять только держателей основных карт (т. е. тех, кого на соответствующий момент финансовое учреждение справедливо считает ответственными за управление средствами)», в то время как другие держатели средств, которые остаются **неизвестными**, также могут осуществлять операции с этими средствами, хранящимися в таком кредитно-финансовом учреждении. Эта ситуация подверглась критике экспертов и повлияла на квалификационную оценку согласно рекомендации 5 (ОВО по Новой Зеландии за 2009 г., стр. 84, 93).

Однако в том, что касалось **верификации** держателей дополнительных карт, применение упрощенной процедуры НПК, по всей видимости, возражений у экспертов не вызвало: «419. Упрощенная процедура НПК допускается, если предоставленная карта является картой для переводов. В таких случаях проверка личности держателя второй карты не требуется (Пояснения к нормативным требованиям на 2008 г.). Такого типы карты для переводов предлагает только один банк в Новой Зеландии. Власти рекомендуют разработать исключение к положению о картах для переводов, чтобы смягчить риски отмывания денег и финансирования терроризма, которые могут быть связаны с переводами денежных средств, и включить в основания для применения этого исключения ряд условий и ограничений. В такие условия и ограничения входит следующее: *i)* максимальный годовой объем переводов денежных средств и максимальный остаток на карте не более 9999,99 новозеландских доллара; *ii)* соответствующими картами можно пользоваться только через банкоматы международных банков и *системы электронного перевода платежей в торговых точках* (EFTPOS); *iii)* требования полной верификации FTRA и ведения учета применяются только к держателю основной карты (лицу, открывшему счет); *iv)* требования проверки личности и ведения учета применяются к любому другому правомочному держателю карты (который может не быть резидентом Новой Зеландии); и *v)* учреждение, выпустившее карту, обязано осуществлять текущую надлежащую проверку и мониторинг транзакций по соответствующим картам. Власти пришли к заключению, что вышеуказанные ограничения достаточно смягчают риск отмывания денег, чтобы предлагать этот продукт в Новой Зеландии, при условии применения всех мер НПК к держателям основных карт и упрощенной процедуры НПК для держателей дополнительных карт. Заключение было сделано на основе анализа, согласованного с Резервным Банком, при участии должностных лиц Министерства юстиции, Министерства внутренних дел тихоокеанских островов и Управления финансовой разведки. В процессе анализа были рассмотрены материалы, предоставленные полицией Новой Зеландии, APG и ФАТФ, включая типологии и подтверждения недобросовестного использования карт с хранимой стоимостью и продуктов типа туристических карт. Также с несколькими банками были проведены обсуждения о возможных вариантах продуктов и способах управления рисками отмывания денег и финансирования терроризма и собраны выборочные данные по объемам и средней сумме переводов денежных средств. После этого были подготовлены материалы общественных обсуждений, а затем и правительственный документ с обоснованиями ограничений регулирования, направленных на смягчение рисков отмывания денег и финансирования терроризма до допустимых пределов, соответствующих ожидаемой форме и концепции нового Билля о ПОД/ФТ, а также дальнейшему соблюдению в Новой Зеландии рекомендаций ФАТФ».

198. Несмотря на то, что в большинстве случаев устанавливается личность всех держателей счета или карты (т. е. держателей основных и дополнительных карт), остаются поводы для обсуждения: так ли это необходимо, если модель соответствующих карт определяется как «мало рискованная», а значит, допускает упрощенную процедуру НПК. В то время как полное освобождение от надлежащей проверки держателей основных карт подвергается критике как несоблюдение рекомендации 5[106], остается непонятным, следует ли применять тот же подход к освобождению держателей дополнительных карт (при условии, что держатель основной карты прошел соответствующую проверку личности и верификацию). Это будет зависеть от того, в какой степени держатель дополнительной карты контролирует продукт, а также от того, следует ли считать его клиентом НСП или можно рассматривать как доверительного управляющего или своего рода бенефициара клиента.

6. Заключения и вопросы для дальнейшего рассмотрения

199. Внедрение НСП на рынке увеличилось по сравнению с отчетом за 2006 г. и в будущем эта тенденция сохранится. Все больше и больше НСП предоставляют возможности для перевода денег между любыми странами. В результате увеличилось и количество подтверждений

[106] См. выше главу 5.2 («Освобождение от обязательств в области ПОД»), пар. 162.

недобросовестного использования НСП для отмывания денег и (в некоторой степени) для финансирования терроризма.

200. В будущем появятся новые типы НСП. Из-за объединения и комбинации НСП надзорным и законодательным органам будет гораздо сложнее оценивать уязвимость таких платежных систем для угрозы отмывания денег и финансирования терроризма. В связи с этим для дальнейшего развития НСП необходима оптимальная, гибкая и готовая к будущему система ФАТФ.

201. Помимо оценки рисков (раздел 3) и разработки типологий (раздел 4), в данном отчете исследуется, будут ли и дальше 40+9 рекомендаций ФАТФ обеспечивать адекватную инфраструктуру для работы с новейшими технологическими и нормативными разработками в области НСП.

202. Проектная группа пришла к заключению, что Сорок рекомендаций ФАТФ и Девять специальных рекомендаций обеспечивают достаточно адекватную инфраструктуру для работы с уязвимостями новых способов платежей, несмотря на то, что ФАТФ необходимо рассмотреть некоторые моменты в международных стандартах, требующие доработки или разъяснения. Проектной команде известно о том, что ФАТФ уже приступила к тщательному пересмотру своих стандартов, и некоторые вопросы, поднятые в настоящем документе, уже рассматриваются в этом контексте.

203. Проектная команда пришла к заключению, что ФАТФ желательно пояснить некоторые вопросы, возникшие в связи с НСП. По имеющимся сведениям некоторые из этих вопросов уже рассматриваются в контексте подготовки четвертого этапа оценки.

204. При обсуждении перечисленных ниже вопросов и поиске соответствующего баланса ответственные рабочие группы должны учитывать не только аспекты, связанные с ПОД и ФТ, но и положительный эффект НСП (например, финансовое вовлечение, перевод транзакций из неформального в формальный сектор, стимулирование конкуренции и экономический рост на национальных рынках), а также обоснованные потребности рынка и интересы частного сектора.

В любом случае, принимая политические решения в отношении НСП, необходимо учитывать соотношение затрат и результатов. Ответственным лицам необходимо тщательно изучить, например, следующее:

- оправдывает ли результат ПОД/ФТ потенциальные дополнительные расходы и усилия, которые могут потребоваться от учреждений, а также надзорных органов, ПФР и других организаций;
- существует ли риск того, что определенные меры могут создать крайне неблагоприятные условия для клиентов НСП (например, в отношении стоимости или «удобства» НСП), и могут ли такие возможные неблагоприятные условия побудить клиентов к осуществлению платежей через нерегулируемых провайдеров платежных сервисов.

Политические решения должны быть направлены на поиск правильного баланса между эффективным и всеобъемлющим режимом ПОД/ФТ, обоснованными потребностями рынка и интересами частного сектора.

Вопросы по упрощенной процедуре НПК

1. Должна ли рекомендация 5 предоставлять освобождение от НПК в случаях «малого риска» (рекомендация 5)?

205. Рекомендация 5 гласит, что *«кредитно-финансовые учреждения не имеют права открывать анонимные счета или счета на очевидно вымышленные фамилии».*

206. Кроме того, в рекомендации 5 говорится, что *«кредитно-финансовые учреждения **обязаны применять все меры НПК** (перечисленные в рек. 5), но имеют право **определять объем таких мер в зависимости от степени риска**, определяемой типом клиента, деловыми отношениями или транзакцией. Применяемые меры должны соответствовать всем директивам, изданным компетентными органами. Для более высоких категорий риска кредитно-финансовые учреждения обязаны производить расширенную проверку. В определенных ситуациях, **если риски малы, страны могут разрешить кредитно-финансовым учреждениям применять сокращенные или упрощенные меры**».*

207. Стандарты не включают определение «сокращенных или упрощенных мер НПК», а также не исключают освобождения от данного условия. В настоящее время некоторые юрисдикции полностью освобождают кредитно-финансовые учреждения от мер НПК в обозначенных случаях малого риска. Если в некоторых взаимных оценках такой подход критикуют как несоответствующий рекомендации 5, то есть и другие (включая ряд юрисдикций, организаций, таких как Всемирный банк, и представителей частного сектора), которые придерживаются того мнения, что рекомендация 5 предоставляет (или должна предоставлять) возможности для освобождения от НПК в случаях малого риска.

Секретариат ФАТФ сообщил проектной команде, что ФАТФ планирует предложить некоторые изменения в стандартах, направленные на решение данных вопросов. При этом будут учитываться перечисленные ниже аспекты.

208. Освобождение от верификации:

- совокупные риски продукта или услуги можно смягчать и другими средствами, например, за счет ограничений на остатки счетов и суммы транзакций. Применение жестких ограничений на транзакции или другие функции может отпугнуть потенциальных отмывателей денег даже больше, чем перспектива верификации. Кроме того, интенсивный мониторинг поможет смягчить риск отмывания денег и для продуктов;
- в некоторых юрисдикциях верификация личности клиента затруднена, особенно если большая часть населения не имеет удостоверений личности или других надежных документов.
- верификация способна также накладывать финансовое бремя на кредитно-финансовые учреждения или клиентов (например, если для верификации клиентам нужно проделывать длинный путь в банк или наоборот), что отпугивает как клиентов, так и кредитно-финансовые учреждения и может представлять опасность для экономического успеха отдельных провайдеров НСП.
- целевые исследования показывают, что преступники осуществляли отмывание денег даже при использовании верификации, например, с помощью ворованных или фальшивых документов либо подставных лиц.

209. Освобождение от установления личности:

- в отличие от верификации, установление личности клиента не требует больших затрат или усилий, провайдерам НСП нужно только спросить имя клиента;
- что касается держателей дополнительных карт — можно ли освободить кредитно-финансовые учреждения от установления личности держателей дополнительных карт (например, если держатель основной карты прошел тщательное установление личности и верификацию и используются другие меры и системы, скажем, мониторинг)?

2. Допустима ли упрощенная процедура НПК для бизнес-моделей, не предусматривающих личные контакты? (рекомендации 5 и 8)

210. ФАТФ необходимо разъяснить, квалифицируются ли бизнес-модели, не предусматривающие личные контакты, как «ситуации высокого риска» в контексте рекомендации 5. Поскольку на последнем рабочем совещании эксперты рабочей группы по оценке и внедрению пришли к заключению, что «определенный риск» не приравнивается автоматически к «высокому риску» в контексте рекомендации 5, то было бы хорошо, если бы ФАТФ обеспечила большую ясность по данному вопросу, добавив поправки в стандарты с учетом следующих аспектов:

- выбранная в данном отчете (и отчете за 2006 г.) концепция оценки рисков предполагает, что при расчете категории риска отдельного продукта или услуги необходимо принимать во внимание все факторы риска и все средства их смягчения. Включение продукта в группу высокого риска из-за одного единственного фактора риска (т. е. отсутствия личных контактов) без учета всех остальных факторов риска и средств их смягчения противоречит этой концепции оценки;
- в настоящее время упрощенную процедуру НПК применяют к бизнес-моделям без личных контактов несколько провайдеров НСП, которые могут серьезно пострадать, если эта практика будет объявлена недопустимой. Представители частного сектора указали, что такое решение может поставить под угрозу рентабельность некоторых сервисов НСП.

<u>Вопросы по процедурам работы с агентами</u>

3. Должны ли агенты провайдеров НСП подчиняться стандартам и собственным обязательствам в сфере ПОД/ФТ? (рекомендация 23, SR VI)

211. Агенты в зависимости от типа осуществляемой ими деятельности могут играть очень важную роль в осуществлении и проведении платежных транзакций. По сравнению с более традиционными финансовыми услугами, использование агентов для выполнения функций, связанных с ПОД/ФТ, более распространено среди провайдеров НСП. Такие агенты могут выступать в качестве посредников или средства сопряжения между традиционными финансовыми услугами и более «виртуальными» платежными сервисами. Привлечение агентов также может служить эффективной и недорогой альтернативой открытию филиалов провайдеров услуг НСП, особенно при оказании услуг НСП заграницей.

212. Согласно 40+9 рекомендациям ФАТС, на самих агентов обязательства в области АОД/ФТ не возлагаются. Если некоторые юрисдикции недавно указали, что это может означать несоответствие стандартам, то другие считают действующую практику адекватной и достаточной. ФАТФ следует рассмотреть, должны ли стандарты в более явной форме обозначать вопросы, связанные с эффективным контролем работы агентов, осуществляющих основные операционные функции, либо путем прямого надзора, либо путем непрямого управления со стороны принципала.

При этом необходимо принять во внимание следующие аспекты:

- в целом возложение на агентов обязательств в области ПОД не означает сокращение обязательств в области ПОД самих принципалов;
- сообщение о подозрительных транзакциях: агенты часто являются единственными лицами, которые лично контактируют с клиентами. Таким образом, ценная информация для сообщения о подозрительных транзакциях (например, подозрительное поведение клиента) может быть доступна только агентам. Если агент не несет обязательств по отчетности или должен отчитываться только перед принципалом, такая информация может быть утеряна или поступить с опозданием;

- обязательство по отчетности агентов не означает сокращение или прекращение собственных обязательств кредитно-финансового учреждения в отношении подачи отчетов о подозрительных транзакциях. Кредитно-финансовое учреждение может располагать дополнительной информацией о клиенте и его транзакциях, недоступной агенту, и, таким образом, иметь возможность для выявления подозрительных транзакций, которые агент бы не заметил;

- кроме того, ФАТФ может рассмотреть, в какие органы принципал и (или) агент должны подавать отчеты, если на агента, который находится с принципалом в разных юрисдикциях, возлагаются обязательства по отчетности: в ПФР юрисдикции принципала, в ПФР юрисдикции агента или отчитываться перед обеими юрисдикциями?[107]

- обучение персонала: если на агентов возлагаются обязательства в области ПОД/ФТ, к ним должно также предъявляться требование о соответствующей подготовке персонала. Такую подготовку также может осуществлять принципал;

- расходы на соблюдение требований: возложение на агентов новых обязательств в области ПОД может потребовать от них дополнительных расходов и усилий и сделать услугу менее привлекательной для агентов и (или) клиентов. При этом в бизнес-моделях, где на агентов уже возложены договорные обязательства в области ПОД перед принципалом, возможность существенного увеличения расходов или усилий в случае возложения на таких агентов юридических (а не договорных) обязательств в области ПОД не определена;

- возложение на агентов прямых юридических обязательств в области ПОД/ФТ может стать сильным сдерживающим фактором для выступления в качества агента, затруднить для провайдеров НСП поиск агентов и тем самым привести к сокращению точек доступа для регулируемых и контролируемых провайдеров услуг НСП;

- эффективность надзора: если агенты регулируются и несут обязательства в области ПОД/ФТ, количество объектов, которые должны будут контролировать органы финансового надзора, резко увеличится. Существуют сомнения относительно эффективности такого контроля во всех ситуациях.

- ФАТФ следует также рассмотреть обеспечение провайдеров НСП указаниями о порядке формирования договорных взаимоотношений с агентами и дать надзорными органам возможность следить за тем, чтобы через своих агентов кредитно-финансовые учреждения выполняли обязательства в области ПОД/ФТ. Несмотря на то, что какие-то указания уже были представлены для сферы денежных услуг (например, концепции «знай своего агента», мониторинга и подготовки агентов)[108], остается неясным, считает ли ФАТФ эти указания применимыми и к другим кредитно-финансовым учреждениям (таким как провайдеры НСП).

4. Как следует понимать термин «агент» (рекомендация 9, SR VI)?

213. Главная сложность в отношении термина «агент» — это найти полноценные определения терминам «аутсорсинг», «доверие» и «представление третьей стороной» (как указано в рекомендации 9). По данным проектной группы, этим вопросом в данный момент занимается подгруппа ФАТФ WGEI EGA.

214. Во-вторых, ФАТФ не определяет типы деятельности, которые можно рассматривать как создание агентских взаимоотношений. Например, обменные пункты, используемые в бизнес-моделях цифровых денег, могут утверждать, что являются независимыми организациями, торгующими электронной валютой. Продавцы предоплаченных средств (например, компании розничной торговли, продающие предоплаченные карты или денежные сертификаты) могут

[107] Например, на о. Джерси было издано указание о том, что агенты обязаны подавать отчеты в оба ПФР.

[108] Документ ФАТФ «Подход, основанный на оценке риска: указания для сферы денежных услуг» (Risk Based Approach: Guidance for Money Service Businesses), июль 2009 г.

утверждать, что выступают только в качестве продавцов, действующих за пределами финансового сектора.

Другие вопросы

5. Следует ли расшить контекст SR IX, так чтобы он включал «электронные деньги» или «карты с хранимой стоимостью» и в частности предоплаченные карты? (SR IX)

215. SR IX гласит, что «в странах должны действовать меры по выявлению физических трансграничных перевозок **валюты и оборотные документы на предъявителя**, включая систему декларирования и другие обязанности по предоставлению информации».

216. В отчете за 2006 г. трансграничное перемещение предоплаченных карт определялось как потенциальный риск отмывания денег. Проектная группа по-прежнему видит в нем значительный потенциальный риск, несмотря на то, что поиск прецедентов показал только несколько случаев использования такой типологии в прошлом.

217. В целях контроля и противодействия трансграничному перемещению продуктов с хранимой стоимостью таможенным органам следует использовать инструменты, реализуемые для трансграничного перемещения денег и оборотных документов на предъявителя в соответствии SR IX, такие как декларирование или система предоставления информации и возможность конфискации средств. Однако в большинстве юрисдикций такие инструменты (происходящие из SR IX) применимы только к валюте и оборотным документам на предъявителя, а это означает, что предоплаченные карты декларировать при пересечении границы не нужно.[109]

218. Большинство юрисдикций не классифицируют предоплаченные карты, а также иные средства «с хранимой стоимостью» или «электронные деньги» как денежные средства или оборотные документы на предъявителя в контексте SR IX. Таким образом, для обеспечения возможности подвергать такие карты трансграничному контролю необходимо расширить контекст SR IX (и, соответственно, национальное таможенное законодательство), включив в него такие карты (либо оставить текст SR IX без изменений, но расширить определение либо «денег», либо «электронных денег», включив в него карты с хранимой стоимостью или электронные деньги). Рассматривая расширение контекста SR IX, необходимо принять во внимание перечисленные ниже аспекты.

- В настоящее время существуют разные мнения о том, должны ли предоплаченные карты подпадать под область действия SR IX. Если одни юрисдикции подчеркивают, что такие карты во многих отношениях подобны наличным деньгам, то другие считают их типом дебетовой или кредитной карты, не включенным в область действия SR IX специально.
    - Предоплаченные карты подобны деньгам в том отношении, что они анонимны, имеют определенную стоимость и могут широко применяться для покупки товаров и услуг. Карты оплачиваются заблаговременно (нет кредитной системы) и могут перевозиться через границу.
    - С другой стороны, предоплаченные карты используются аналогично дебетовым и кредитным картам, которые, безусловно, не подпадают под SR IX. Стоимость предоплаченных карт обычно хранится не на самих картах, а на сервере, так что сама карта служит только средством доступа к фондам.

[109] Всего несколько юрисдикций применяют эти правила к предоплаченным картам. Например, по разделу 12a Административного акта Германии о таможне (Zollverwaltungsgesetz) средства трансграничного контроля применяются к «наличности и эквивалентным средствам платежей», включая «чеки, векселя, драгоценные металлы и камни, электронные деньги» (раздел 1, пар. 3a, Zollverwaltungsgesetz).

- Далее, нужно изучить, действительны ли причины, по которым кредитные и дебетовые карты исключили из области действия SR IX, для предоплаченных карт.
- Эффективность: в настоящее время сохраняются технические сложности с верификацией предоплаченных карт. Неясно, как сотрудники таможни будут определять фактическую стоимость, которая хранится на карте. Потребуется ли установка устройств для чтения карт и будут ли они работать со всеми техническими стандартами различных провайдеров? Однако технические сложности можно преодолеть, если заложить правовые основы для трансграничного контроля предоплаченных карт.
- Если разрешить перевозку предоплаченных карт через границу при условии минимального остатка или отсутствия средств на таких картах и внесении средств (или «активации») после прибытия в место назначения, это также может повлиять на эффективность режима трансграничного декларирования таких карт.

6. Должна ли рекомендация 10 включать IP-адреса для транзакций, осуществляемых с персональных компьютеров?

219. В настоящее время рекомендация 10 не включает прямые требования о сохранении IP-адресов персональных компьютеров, через которые могут осуществляться платежные транзакции. С одной стороны, большинство провайдеров НСП делают это в собственных интересах, а с другой правоохранительные органы уже сообщали о провайдерах, которые не сохраняют IP-адреса своих клиентов или удаляют их слишком быстро (т. е. до окончания пятилетнего периода, предложенного в рекомендации 10). ФАТФ следует принять во внимание эту проблему и рассмотреть возможность добавления IP-адреса в список примеров «необходимых учетных данных по транзакциям», критерий 10.1 Методологии.

7. Актуализация данного исследования

220. С учетом постоянного развития сектора НСП, технического развития и соответствующей реакции законодателей и ответственных органов, проектная группа предлагает актуализировать данное исследование по истечении соответствующего периода времени (двух лет). Возможно, в условиях будущего развития определенных секторов и будущих прецедентов вместо этого будет целесообразно опубликовать отдельные типологические отчеты по единичным категориям НСП (например, типологический отчет по предоплаченным картам).