



**ФАТФ – ГАФИ**

**Неофициальный перевод**

**ГРУППА РАЗРАБОТКИ ФИНАНСОВЫХ МЕР  
БОРЬБЫ С ОТМЫВАНИЕМ ДЕНЕГ**

**ОТЧЕТ О НОВЫХ СПОСОБАХ ПЛАТЕЖЕЙ**

**13 октября 2006 года**

© 2006 ФАТФ/ОЭСР

Без права переиздания. Воспроизведение или перевод данной публикации возможны только с предварительного письменного разрешения.

Заявление для получения данного разрешения необходимо подать по адресу:

FATF Secretariat, 2 rue André-Pascal, 75775 Paris Cedex 16, France.

Факс: +33 1 44 30 61 37 или по e-mail: [Contact@fatf-gafi.org](mailto:Contact@fatf-gafi.org)

## **Краткое содержание**

Во всем мире появляются новые и инновационные методы для выполнения электронных международных денежных переводов. Эти новые платежные инструменты возникают на основе расширения сферы действия существующих платежных систем, а также появляются новые методы платежей, существенно отличающиеся от традиционных транзакций. Увеличение количества новых методов платежей касается проблем отмывания денег и финансирования терроризма, так как преступники могут быстро освоить использование новых возможностей.

В настоящем исследовании анализируется использование предоплаченных карт, систем платежей через Интернет, оплаты через мобильную связь и обезличенной покупки драгоценных металлов с целью: 1) определить основные направления в применении новых технологий платежей; 2) оценить угрозу отмывания денег и финансирования терроризма; 3) определить, рассматривают ли в достаточной степени 40 рекомендаций и 9 специальных рекомендаций Группы разработки финансовых мер борьбы с отмыванием денег (40+9) любую возможную угрозу.

В исследовании выявлено, что каждый из проанализированных методов платежей соответствует обоснованной потребности рынка, несмотря на то, что существует потенциальная вероятность отмывания денег и финансирования терроризма. Как правило, оффшорные провайдеры новых методов платежей представляют дополнительные риски отмывания денег и финансирования терроризма по сравнению с поставщиками услуг, действующими в пределах одной юрисдикции.

И хотя считается, что программа рекомендаций 40+9 ФАТФ обеспечивает необходимое руководство по предотвращению вероятного незаконного использования данных новых методов платежей, исследование предлагает дополнительно изучить влияние, которое могут иметь данные используемые технологии на международные и государственные системы в целях обеспечения их соответствия программе рекомендаций 40+9 ФАТФ.

## СОДЕРЖАНИЕ

Краткое содержание.....	i
1. Введение.....	1
2. Вводная информация.....	2
Традиционные и нетрадиционные розничные платежи.....	3
Предоплаченные карты.....	4
Электронный кошелек.....	5
Мобильные платежи.....	6
Услуги платежей через Интернет.....	7
Обезличенные драгоценные металлы.....	9
3. Оценка рисков новых систем платежей, типологии и ситуационные анализы.....	10
Факторы рисков методов платежей.....	10
Предоплаченная карта: открытая система.....	11
Предоплаченная карта: закрытая система.....	13
Электронный кошелек.....	14
Мобильные платежи.....	14
Услуги платежей через Интернет.....	15
Обезличенные драгоценные металлы.....	16
Предоставление услуг новых методов платежей за границей.....	17
Предложение Германии о системе раннего предупреждения.....	17
Риски отмывания денег и финансирования терроризма при использовании новых методов платежей.....	18
5. Применение рекомендаций и специальных рекомендаций ФАТФ; и выбранные нормативные подходы.....	19
6. Результаты ответов и анализ анкеты о новых методах платежей.....	22
7. Выводы и задачи для дальнейшего изучения.....	25
Приложение А. Описание сетей традиционных кредитных и дебетовых карт.....	26
Приложение Б. Дополнительные результаты и анализ анкеты о новых методах платежей.....	30

## 1. Введение

Инновации в области платежей, использующие Интернет, радиотехнические устройства и даже установившиеся платежные системы, появляются во всем мире. Эти новые методы платежей могут предлагаться как национальными, так и иностранными провайдерами. Лишь небольшое количество новых платежных методов функционирует и используется в разных странах и по всему миру, область работы большинства из них ограничена или же используется в определенных регионах или для определенных типов транзакций, касающихся покупки товаров и услуг. Некоторые новые методы платежей работают внутри страны, а в отдельных случаях осуществляют международные переводы средств между физическими лицами.

В настоящем исследовании анализируются предоплаченные карты, системы оплаты через Интернет, мобильные платежи и покупка обезличенных драгоценных металлов для того, чтобы 1) определить основные направления в применении новых технологий платежей; 2) оценить угрозу отмывания денег и финансирования терроризма; 3) определить, рассматривают ли в достаточной степени 40 рекомендаций и 9 специальных рекомендаций Группы разработки финансовых мер борьбы с отмыванием денег (40+9) любую возможную угрозу.

Данный отчет дополняет обзор новых методов платежей, который был сделан членами ФАТФ в 1996-1997гг<sup>1</sup>. Большинство специальных платежных инструментов, описанных в данном отчете, еще не использовались во время проведения предыдущего исследования ФАТФ, когда век Интернета только начинался. Поэтому в предыдущем исследовании новых методов платежей ФАТФ был сделан вывод: «Досрочно приводятся предписывающие методы решения теоретических проблем»<sup>2</sup>. Многие проблемы десятилетней давности, однако, больше не являются чисто теоретическими.

Позднее, в 2004-2005гг. в разработке ФАТФ о типологиях отмывания денег участники вновь рассмотрели новые методы платежей как часть альтернативных систем денежных переводов (ARS) проекта по типологиям отмывания денег<sup>3</sup>. Отчет по альтернативным системам денежных переводов сообщал: «Данное исследование очень кратко затрагивает возникновение новых методов платежей, включающих электронные деньги. Хотя многие из этих систем могут считаться альтернативными системами денежных переводов, их характеристики настолько нестандартны, что необходимо провести отдельное исследование». Некоторые из платежных инструментов и систем, определенных в том отчете, рассмотрены более тщательно в настоящем исследовании.

Исследование, лежащее в основе данного отчета, началось с составления анкеты, в которой мы постарались определить новые методы платежей, появляющиеся во всем мире, и оценить размер данного рынка; выяснить, подлежат ли эти методы платежей нормативно-правовому регулированию, контролю и лицензированию; существует ли вероятность отмывания денег и финансирования терроризма при использовании этих новых методов платежей; и существуют ли обоснованные случаи правоприменительных действий. На вопросы анкеты ответили тридцать восемь юрисдикций.

В общем, результаты изучения анкеты показали, что определение новых методов платежей не всегда является простой задачей. Как следствие, данные результаты могут не отражать реальное функционирование новых платежных методов по всему миру, а только их выявленную работу в юрисдикциях, которые дали ответ в анкете. Полезным дополнением к данному отчету являются периодические обзоры новых методов платежей, проводимые Комитетом по платежным и расчетным системам Банка международных расчетов. Однако данные обзоры по развитию рынка платежей не нацелены на проблему отмывания денег или противодействие финансированию

---

1. Первое формальное исследование ФАТФ новых методов платежей, обсуждаемых в данном исследовании, было сделано в *Отчете по типологиям отмывания денег*, февраль 1997г., Раздел V и Приложение I. См.: <http://www.fatf-gafi.org/findDocument/0.2350.en.32250379.32237235.1.32247552.1.1.1.00.html>.

2. Февраль 1997г., *Отчет по типологиям отмывания денег*, с.14. Данные выводы были в последствии обновлены и обычно повторно вписывались в два последующих годовых отчета ФАТФ по типологиям отмывания денег от 10 февраля 1999г. и от 1 февраля 2001г.

3. 10 июня 2005г., Раздел I. См.: <http://www.fatf-gati.org/dataoecd/16/8/35003256.pdf>

4. Комитет по платежным и расчетным системам, под руководством Банка международных расчетов, регулярно публикует отчеты, анализирующие развитие национальных и международных систем платежей, клиринга и расчетов. См. «Обзор развития систем электронных денег, мобильных платежей и платежей через Интернет». Публикации Комитета по платежным и расчетным системам, № 62, март 2004 г. на сайте: <http://www.bis.org/publ/cpss62.htm>. Более новую статистическую информацию по платежным и расчетным системам (включая обзор некоторых новых методов платежей), см. Комитет по платежным и расчетным системам (CPSS), «Статистические данные по платежным и расчетным системам в некоторых странах. – Данные за 2004год.» Банк международных расчетов (BIS), Комитет по платежным и расчетным системам (CPSS) #74, Март 2004г., <http://www.bis.org/publ/cpss74.htm>

терроризма, хотя они используют новые методы платежей, а именно в этом и заключается цель настоящего исследования<sup>5</sup>.

Исполнительная группа, которая включает представителей из Азии, стран-членов Европейского союза и Соединенных Штатов, провела дополнительное первичное исследование, консультируясь с экспертами из государственного и частного секторов. На совещании экспертов, посвященном типологиям отмывания денег и финансированию терроризма, в 2005-2006гг. в Рио-де-Жанейро, исполнительная группа прослушала выступления представителя MasterCard Джошуа Пейреза (Joshua Peirez) и представителя PayPal Алена Лава (Allen Love), которые описали платежные инструменты их компаний и рынки, на которых они работают. Висент С. Аквино (Vicente S. Aquino), исполнительный директор секретариата филиппинского совета по противодействию отмыванию денег описал системы мобильных платежей своей страны; Шери Данлоп (Sheri Dunlop), представитель секретной службы министерства финансов Соединенных Штатов, представила исследование случая отмывания денег с использованием обезличенных драгоценных металлов. В другое время участники основной исполнительной группы встретились с представителями компаний Visa и American Express и фирм по управлению системами программ предоплаченных карт в Соединенных Штатах<sup>6</sup>. И, в заключении, члены исполнительной группы рассмотрели ряд статей в прессе и отчетов государственного сектора, связанных с этим вопросом. Данный отчет включает доклады экспертов по платежным системам, специалистов по противодействию отмыванию денег и законодательных экспертов из многих стран. Во многих случаях определения и терминология, используемые для описания подобных платежных систем или платежных операций, различаются в разных странах. Для обеспечения ясности и согласованности в рамках данного отчета, члены рабочей группы выбрали для использования, насколько это возможно, определения, применяемые в платежных системах Комиссии по платежным и расчетным системам<sup>7</sup>. В случае, когда термины и определения, используемые в данном отчете, отличаются от этого источника, различие подчеркивается и объясняется.

Отчет разделен на шесть разделов. Разделы 1 и 2 дают краткое содержание и короткое вступление. В разделе три описывается, каким образом работают и используются новые методы платежей, рассматриваемые в данном отчете<sup>8</sup>. В разделе четыре представлена таблица рисков отмывания денег и финансирования терроризма, составленная исполнительной группой для оценки потенциальных рисков отмывания денег и финансирования терроризма по каждому новому методу платежей. В разделе пять описывается, как Сорок рекомендаций и девять специальных рекомендаций ФАТФ применяются для новых методов платежей, и представлено нормативно-правовое регулирование в выборочных юрисдикциях. В Разделе шесть подводятся итоги 38 ответов анкеты о новых методах платежей ФАТФ, подготовленные исполнительной группой<sup>9</sup>. В разделе семь сделаны выводы и выделяются области для дальнейшего рассмотрения ФАТФ.

## **2. Вводная информация**

Возникновение новых платежных систем обусловлено рядом факторов, специфических для каждой страны. К ним относятся основная экономическая обстановка, технология работы, предпочтения, фактические и планируемые издержки, а также действующие нормативные акты, принципы политики и правила государственных и частных организаций, оказывающих значительное влияние на развитие платежных систем. Однако основной тенденцией во всех странах является переход от расчетов бумажными деньгами к электронным платежам.

Переход от платежей бумажными деньгами к стандартизированной технологии электронных транзакций повлек за собой разрушение платежной системы в различных сегментах коммерческой деятельности. Техническое и программное обеспечение, средства связи, системное руководство, бухгалтерия, маркетинг и продажи – все это стало различными направлениями деятельности, где применяются определенные платежные системы. Данная сегментация рынка, а также возникшая в

---

5. Другим авторитетным источником информации по развитию и состоянию рынка новых методов платежей является сайт организации по наблюдению за электронными платежными системами (ePSO), которой руководит Европейский центральный банк: [www.e-psy.info](http://www.e-psy.info)

6. Системы NetSpend, Green Dot и Wild Card (сейчас электронные денежные средства)

7. См. Комитет по платежным и расчетным системам «Словарь терминов, используемых в платежных и расчетных системах», Банк международных расчетов (BIS), март 2003г. на сайте: <http://www.bis.org/publ/cpsy00b.htm>

8. Подробное представление традиционных методов кредитного и дебетового платежей (на которых основаны большинство новых методов платежей) содержится в Приложении А.

9. Подробное обобщение ответов в формулярах можно посмотреть в Приложении Б.

результате нее специализация, привели к возникновению небанковских организаций, являющихся внешними поставщиками услуг для банковского сектора, а иногда и конкурентами на рынке межбанковских расчетов<sup>10</sup>.

Несмотря на то, что для конечных пользователей банки остаются основными поставщиками большинства розничных платежных средств и услуг, в настоящее время осуществление платежей предлагает большое количество обслуживающих организаций. Переход от платежей бумажными деньгами к электронным транзакциям предоставил возможность небанковским обслуживающим организациям создать собственные платежные инструменты и снабдить их дополнительными продуктами для работы на нишевых рынках.

В настоящее время небанковские организации работают как порталы для оплаты через Интернет, осуществляя перевод платежей между плательщиками, получателями платежей и организациями, где у них открыты счета. Небанковские посредники также выполняют перевод платежей между покупателями и продавцами, которые заключают сделки через электронные розничные магазины Интернета и через онлайн сайты аукционов. Фактически небанковские организации охватывают всю индустрию платежей, выполняют обработку транзакций, обслуживание баз данных и даже работают в качестве поставщиков ценностей в системах электронных денег. В результате этого «схема оказания прямых услуг розничных платежей конечным пользователям небанковскими организациями и предоставление связанных с ними вспомогательных услуг для пользователей и провайдеров платежей является менее ясной, чем в прошлом»<sup>11</sup>.

### **Традиционные и нетрадиционные розничные платежи**

Традиционными розничными платежами обычно являются потребительские платежи на небольшие суммы, которые не требуют немедленного расчета<sup>12</sup>. Традиционные электронные платежи включают банковские платежи за продукты и услуги и денежные переводы, которые выполняются небанковскими посредниками, такими, как Western Union, которые обычно работают как кредитные переводы, но не зависят напрямую от системы перевода денежных средств между банковскими счетами.

ФАТФ определяет систему перевода денег или ценностей как «финансовую услугу, которая принимает наличные деньги, чеки, другие денежные инструменты или иные средства сбережений в одном месте и выплачивает соответствующую сумму денежной наличностью или в иной форме бенефициару в другом месте с помощью передачи информации, сообщения, перевода или безналичной сети, к которой принадлежит система перевода денег/ценностей»<sup>13</sup>.

Дополнением к этим традиционным розничным платежам являются более новые, инновационные платежные продукты, или нетрадиционные розничные платежи. В настоящем отчете мы считаем данные типы платежей «новыми методами платежей», хотя часто международные специалисты по платежным системам относят их к «электронным деньгам». Новые методы платежей включают множество инновационных продуктов, которые используют новые способы осуществления платежей с помощью традиционных розничных электронных платежных систем или через расширение сферы их действия. Новые методы платежей также включают продукты, которые не основываются на традиционных платежных системах, для перевода ценностей между физическими лицами или организациями<sup>14</sup>. В настоящем отчете рассматриваются следующие новые методы платежей: предоплаченные карты, электронные кошельки, мобильные платежи, услуги оплаты через Интернет и обезличенные драгоценные металлы. Таблица 1, представленная ниже, показывает схематичное распределение новых методов платежей между теми, которые являются расширением сферы действия традиционных платежных инструментов, и теми, которые являются непосредственно новыми методами платежей.

---

10. Клиринговые и расчетные схемы для розничных платежей в выбранных странах, Комитет по платежным и расчетным системам, Банк международных расчетов, сентябрь 2000 (CPSS #40)

11. Результаты политики для центральных банков по розничным платежам, Комитет по платежным и расчетным системам, Банк международных расчетов, март 2003 (CPSS #52)

12. Бумажные неденежные розничные платежные инструменты включают чеки, переводные векселя, кассовые чеки, платежные поручения и другие банковские тратты. Электронные неденежные розничные платежные инструменты включают кредитные и дебетовые карты, а также кредитные переводы и прямой дебет, выполняемые через такие системы, как электронная расчетная палата (ACH). Подробное описание традиционных систем кредитных и дебетовых карт см. в Приложении А.

13. Пояснение к специальной рекомендации VI ФАТФ: альтернативный перевод денежных средств, февраль 2003г.

14. В данном исследовании мы исключили из рассмотрения любые нетрадиционные методы клиринговых и расчетных платежей по бумажным чекам или банковским траттам через использование электронной информации или электронных изображений чеков, включая их конверсию в систему электронных платежей через системы электронной расчетной палаты.

<b>НОВЫЕ МЕТОДЫ ПЛАТЕЖЕЙ</b>	
Расширение сферы действия традиционных розничных электронных платежных систем	Новые нетрадиционные розничные электронные платежные системы
Предоплаченные платежные карты	Электронный кошелек
Платежи через Интернет на основе банковских счетов <sup>15</sup> (не рассматриваются в данном отчете)	Платежи через Интернет, не основанные напрямую на банковском счете
Мобильные платежи на основе банковских счетов	Мобильные платежи, не основанные напрямую на банковских счетах
	Обезличенные драгоценные металлы

**Таблица 1**

## **Предоплаченные карты**

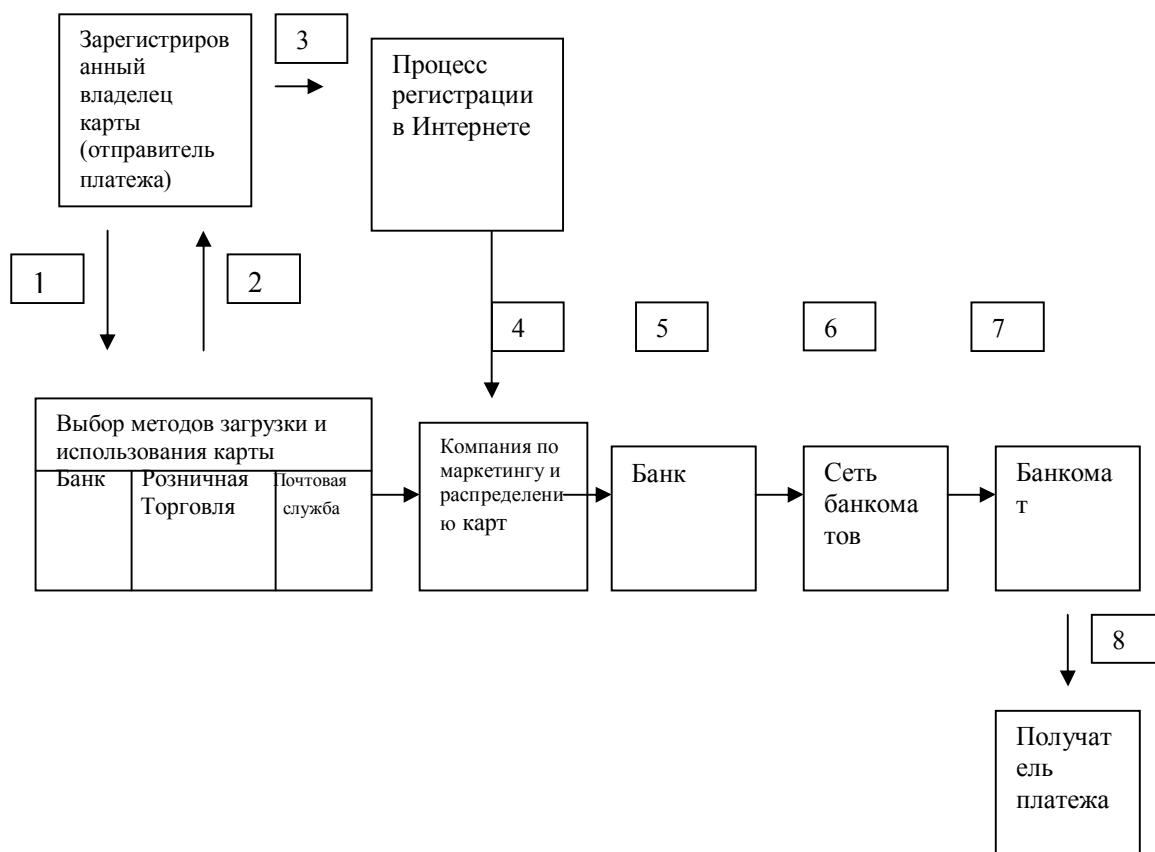
Предоплаченные платежные карты предоставляют доступ к денежным средствам, которые предварительно внесены держателем карты. Хотя существуют разные типы предоплаченных карт, которые используются различным образом, они, как правило, функционируют таким же образом, как дебетовая карта, и в основном основываются на доступе к счету. Для каждой выпущенной карты может быть открыт отдельный счет, или же наоборот, может существовать единый счет, на котором находятся предварительно внесенные средства для всех выпущенных карт. Осуществлять выпуск карт и открытие счетов могут кредитные учреждения или небанковские организации; единые счета, как правило, открываются эмитентом в банке.

Предоплаченные карты могут выпускаться для ограниченных или многочисленных целей. Предоплаченные карты с ограниченными целями использования, или *закрытой системой*, могут быть использованы только в четко определенных целях, и их использование часто ограничено отдельными торговыми точками или отдельными услугами. Примерами таких карт могут быть торговые подарочные карты, предоплаченные услуги связи дальнего действия и карты массовой системы распространения. Данные карты также могут быть ограничены суммой, первоначально внесенной на карту (непополняемая карта), или же владелец карты может вносить дополнительные суммы (в пределах установленного лимита) и повторно использовать карту (пополняемая карта). Эмитент карты или ее обслуживающая компания обычно работает в сети, в которой могут быть использованы карты. Стоимость карт обычно соответствует сумме предоплаченного счета, открытому эмитентом или обслуживающей компанией. Транзакции проводятся таким же образом, как и транзакции, выполняемые по кредитным и дебетовым картам. Предоплаченные карты многоцелевого использования, или *открытой системой*, могут быть использованы во многих местах для широкого ряда услуг. Данные карты можно использовать в пределах одного государства или на международном уровне, но иногда их действие может быть ограничено определенным географическим районом. Многоцелевые карты могут быть использованы лицом, купившим карту, или же кем-либо другим. Примерами таких карт являются зарплатные карты и расходные карты широкого пользования для физических лиц, которые не требуют открытия счета в банке или наличия кредитной карты. Эти карты обычно связаны с карточной платежной системой, такой, как Visa или MasterCard, которая позволяет использовать их таким же образом, как дебетовые карты, для покупок или получения наличных через банкоматы (АТМ). Некоторые эмитенты не требуют от владельца карты иметь депозитный счет. Данные карты распространяются торговыми предприятиями, депозитарными финансовыми учреждениями и системами перевода денег/ценностей для различных целей. Большинство данных карт пополняемые.

---

15. Выражение «банковский счет», используемое в данной таблице, относится к счетам, открытым в финансовых учреждениях, выполняющих требования о противодействии отмыванию денег.





о  
**Рисунок 1.** Процесс выпуска prepaid магнитной карты открытой системы различается в зависимости от эмитента. Вышеуказанные этапы (1), (2) и (3) могут проходить в любом порядке. На этих трех этапах физическое лицо проходит процедуру регистрации для prepaid карты, готовит деньги для карточного счета и получает карту. Этапом (4) является передача регистрационной информации обслуживающей организации. Если на карте есть знак обслуживания банковской ассоциацией (как, например, у карт Visa и MasterCard), обслуживающая организация должна заключить договор с банком (5) для получения доступа во всемирную сеть банкоматов (6). Отдельные банкоматы (7) соединяются с местными системами, а часто и всемирными системами, позволяя физическим лицам в одной стране (8) получить денежные средства, внесенные в другой стране (9).

## Электронный кошелек

Электронный кошелек, или e-purse (называемый также «карточка с заложенным лимитом средств», так как денежные средства положены на карту), электронно prepaid в валюте, в которой открыта карта с кристаллами интегральной схемы (именуемая смарт-карта или чип-карта). В отличие от карты с магнитной полоской, которая содержит информацию о счете, электронный кошелек на самом деле хранит денежные средства в памяти чипа карты. Пользователь буквально носит с собой на карте эти денежные средства (отсюда и название «электронный кошелек»).

В некоторых программах электронного кошелька деньги могут быть переведены напрямую с карты к участвующей торговой организации или другому физическому лицу без транзакции, проводимой через счет организации-посредника. Такая идентифицирующая информация может ограничить сумму, разрешенную для таких транзакций. Для получения денежных средств,

---

16. Данное определение немного дополняет термин «электронный кошелек», обычно используемый Комиссией по платежным и расчетным системам, и включает в себя также термин «электронные деньги». В данном отчете, под термином «электронный кошелек» понимается «пополняемая многоцелевая prepaid карта, которая может быть использована для совершения небольших розничных покупок или других платежей вместо денег», где денежные средства электронно положены на карту в валюте чип-карты.

оплаченных через электронный кошелек, тем не менее, торговое предприятие или физическое лицо должно снять денежные средства со счета, открытого провайдером электронного кошелька или организацией, выпускающей электронный кошелек. Как только денежные средства поступят на карту, для осуществления платежа не требуется никакого онлайн подключения или идентификации личности владельца карты. Основной функцией электронного кошелька является замена наличных денег в повседневных ситуациях. В настоящее время электронные кошельки используются, в основном, для осуществления микроплатежей, например, за общественный транспорт, штрафы за нарушение правил парковки или в торговых аппаратах.

За последние десять лет развитие и использование электронных кошельков на основе карт значительно снизилось, поэтому сейчас работает только несколько систем электронных кошельков. К тому же эти немногие оставшиеся системы электронных кошельков обычно не взаимодействуют между собой, несмотря на размер рынка, на котором они функционируют. Только одна система, German GeldKarte, которая работает в пограничной области между Германией и Люксембургом (см. Рисунок 2), может использоваться в разных государственных юрисдикциях. Кроме того, электронные кошельки обычно имеют ограниченный объем для хранения денежных средств (например, предельная сумма немецкой GeldKarte составляет 200 евро).



**Рисунок 2**

### **Мобильные платежи**

Мобильные платежи обычно связаны с использованием мобильных телефонов и беспроводных способов связи для оплаты товаров и услуг. Платежи принимаются от прибора мобильного средства связи, используя голосовую команду, протоколы текстовых сообщений (такие как систему обмена краткими/одиночными сообщениями, или SMS) или протоколы беспроводного доступа (WAP), которые позволяют получить доступ в Интернет с телефона. Авторизация часто происходит путем ввода уникального личного идентификационного номера (PIN), связанного с пользователем или мобильным средством. Прием мобильных платежей различается в разных странах. Использование мобильных телефонов как способов приема платежей широко распространено в Юго-Восточной Азии и некоторых европейских странах<sup>17</sup>.

Большинство услуг мобильных платежей просто используют телефон как средство доступа для приема и подтверждения транзакций с существующих банковских счетов или карт оплаты<sup>18</sup>. Это эквивалентно использованию Интернета для приема прямого дебета или кредитного перевода с банковского счета, или транзакции по кредитной или дебетовой карте. Это расширенное использование традиционных методов платежей.

Новые способы мобильных платежей: Когда услуги по мобильным платежам не основаны на определенном счете банка или платежной карты, телефонный оператор действует как посредник платежа, выполняя авторизацию, клиринг и расчет по платежу<sup>19</sup>. Телефонные компании, участвующие в этих действиях, могут не контролироваться центральным банком страны или иным регулирующим банковским органом, но могут выполнять правила противодействия отмыванию денег и финансированию терроризма.

Телефонный оператор может также разрешить владельцу телефона проводить некоторые транзакции через телефонный счет (с оплатой по факту) или разрешить владельцу телефона вносить деньги на счет, открытый телефонным оператором или другим провайдером услуг в целях осуществления платежей (предоплаченный). Предоплаченные счета мобильных платежей

---

17. См. Комитет по платежным и расчетным системам «Результаты политики для центральных банков по розничным платежам», Комитет по платежным и расчетным системам, Банк международных расчетов, март 2003 (CPSS #52) на сайте: <http://www.bis.org/publ/cpss52.htm>

18. См. Комитет по платежным и расчетным системам «Обзоры развития электронных денег и платежей через мобильные телефоны и Интернет», Комитет по платежным и расчетным системам, Банк международных расчетов, март 2004 (CPSS #62) на сайте: <http://www.bis.org/publ/cpss62.htm>

19. Телефонные компании, предлагающие услуги мобильных платежей, для расчетов по платежам проводят транзакции, выполняемые через их системы по обычным банковским каналам.

функционируют таким же образом, как предоплаченная карта или электронный кошелек. Когда телефон применяется таким же образом, как предоплаченная карта, владелец телефона использует телефон как средство доступа к платежной системе для авторизации списания суммы с предоплаченного счета. Когда телефон функционирует как электронный кошелек, предоплаченная сумма хранится на индивидуальном модуле подписчика или SIM-карте внутри телефона.

Мобильные платежи по типу предоплаченной карты или с оплатой по факту более широко используются, чем платежи по типу электронного кошелька. В случае предоплаченных мобильных платежей, телефонные провайдеры часто предлагают эту услугу во взаимодействии с банком. Например, на Филиппинах услуги мобильных платежей предлагают две телефонные компании - Globe Telecom и Smart Communications. Услуга Smart Money от Smart Communications сотрудничает совместно с банком Banko de Oro. Пользователи Smart Money выполняют транзакции и переводы денежных средств через свои мобильные телефоны, они проводятся через предоплаченные счета, открытые в Banko de Oro. Пользователи Smart Money также могут выполнять международные переводы денег, если у их близких есть предоплаченная карта MasterCard, связанная со счетом Smart Money, которая может быть использована для снятия наличных в банкомате.

Globe Telecom работает как посредник по переводу денежных средств с использованием системы G-cash и функционирует без участия банка. Таким образом, клиенты Globe не могут снять средства с предоплаченных счетов в банкомате, а могут получить их только в кассах участвующих в проекте организаций. На Рисунке 3 представлена схема перевода денег от одного клиента Globe Telecom к другому с использованием SMS. Системы G-cash и Smart Money подчиняются правилам противодействия отмыванию денег и финансированию терроризма (включая предоставление информации о подозрительных переводах), а также обязательному надзору.

<b>500 1234</b> <b>28829175880309</b>	<b>От:</b> <b>2882</b> <b>Вы получили 500 по системе G-cash от Авроры Сантос 08.12.04 в 10ч 30 мин.</b> <b>Контр.номер: # 13134</b>	<b>От:</b> <b>2882</b> <b>Вы отправили Джулии Сантос 500 по системе G-cash 08.12.04 в 10ч 30 мин.</b> <b>Контр.номер: # 13134</b>
<b>OK</b> <span style="float: right;"><b>Back</b></span>	<b>OK</b> <span style="float: right;"><b>Back</b></span>	<b>OK</b> <span style="float: right;"><b>Back</b></span>
Отправитель вводит сумму и Pin-код, затем отправляет сообщение на мобильный номер получателя.	Отправителю и получателю платежа приходят SMS сообщения с соответствующим контрольным номером операции.	
Источник: Gartner Research (февраль 2005г.)		

**Рисунок 3. Схема перевода денег по системе G-cash с телефона на телефон**

### **Услуги оплаты через Интернет**

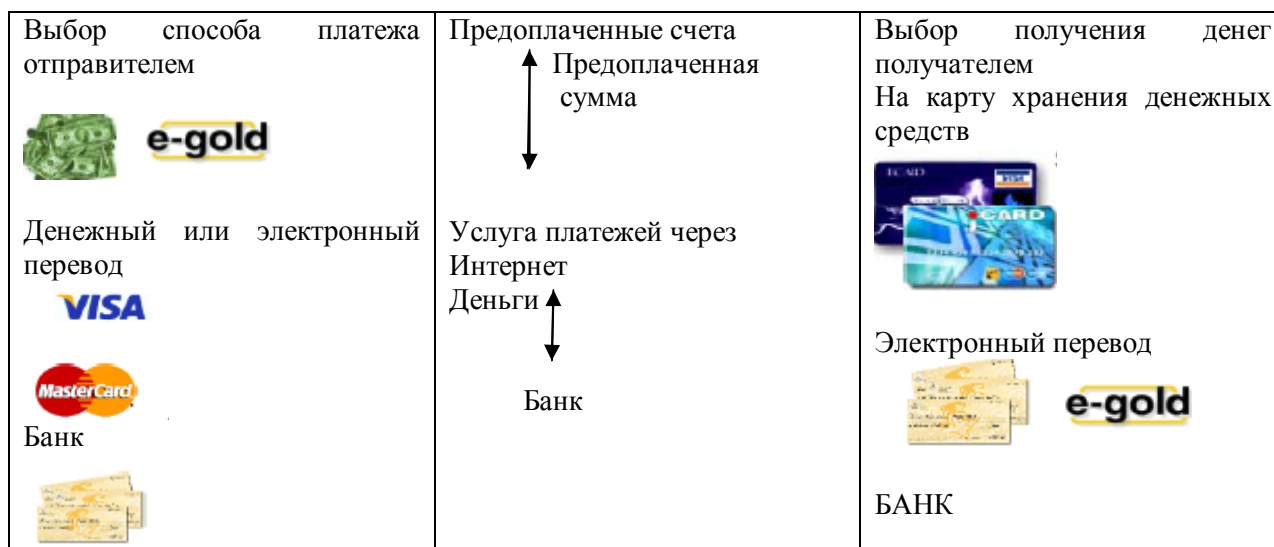
Выражение «оплата услуг через Интернет» обычно применяется для: (i) оплаты услуг, которая проходит через банковский счет и использует Интернет как средство перемещения денежных средств на банковский счет или со счета; и (ii) оплаты услуг, осуществляемой небанковскими организациями, работающими только в Интернете и связанных только косвенно с банковским счетом.

В обычном случае оплата услуг через Интернет относится к традиционным методам платежей, где Интернет является только инновационным каналом для обмена информацией, которая необходима для перевода денежных средств с одного счета на другой и которая позволяет клиентам получать доступ к своим банковским счетам, не выходя из дома, 24 часа в сутки.

Когда оплата услуг через Интернет не связана напрямую с банковским счетом, например, система PayPal, физические лица могут переводить денежные средства, делать покупки в сети или участвовать в онлайн аукционах, используя предоплаченный счет; однако провайдер по оплате услуг может не выполнять правила противодействия отмыванию денег и финансированию терроризма, которые применяются для банков. Обычно провайдер услуг не имеет прямых отношений с клиентом. В зависимости от доступности услуг оплаты через Интернет, данная

деятельность также может включать осуществление платежей и переводов денежных средств за пределами государства.

Некоторые небанковские услуги оплаты через Интернет позволяют клиентам иметь счета у провайдера услуг по оплате, тогда как другие предлагают только услуги по получению и отправке платежей физических лиц с использованием существующего банковского счета или предоплаченной карты клиента. Когда небанковские услуги оплаты через Интернет предлагают клиентам открыть у них счета, они могут объединить данные денежные средства клиентов в единый счет в банке. Данный счет может быть открыт на имя провайдера. В этом случае банк, где открыт счет провайдера услуг, может не иметь прямых отношений с индивидуальными клиентами провайдера услуг.



**Рисунок 4**

Хотя в определенных странах существует ограниченное количество одинаковых продуктов, система PayPal является самым широко используемым небанковским новым методом платежей, использующим Интернет. В основном PayPal работает как посредник по осуществлению платежей между физическими лицами и организациями, которые хотят вести торговую деятельность между собой или переводить денежные средства через Интернет. PayPal функционирует, разрешая физическому лицу открыть предоплаченный счет на свое имя в системе PayPal, куда вносятся деньги с кредитной или дебетовой карты или с банковского счета с помощью кредитного перевода. Используя эти предоплаченные денежные средства, пользователи могут покупать товары или переводить деньги другим владельцам счетов в системе PayPal. Платеж или перевод денег проходит как бухгалтерская транзакция между счетами в системе PayPal. Когда физическое лицо хочет получить доступ к своим денежным средствам на счете в системе PayPal, он дает распоряжение в PayPal кредитовать его кредитную или дебетовую карту или банковский счет через кредитные перевод или даже бумажный счет.





Провайдеры услуг будут различаться по методам платежей, которые они будут принимать для осуществления денежных переводов, и методам платежей, которые они будут использовать для выдачи средств получателю. Вышеуказанный Рисунок 4 показывает, как физическое лицо может использовать кредитную карту, выпущенную банком, или другие традиционные методы платежей для оплаты счета на основе транзакции через Интернет, и, следовательно, делать покупки или переводить все или часть предоплаченных денежных средств другому владельцу счета через бухгалтерскую проводку провайдера услуг. Затем получатель может использовать данные денежные средства для проведения дополнительных транзакций или же для снятия денег традиционным розничным методом платежей. Услуги по переводу денежных средств онлайн используют собственные условия, касающиеся того, в какой форме они будут получать платеж от отправителя, и какие формы выплаты они предоставляют получателям.

## Обезличенные драгоценные металлы<sup>20</sup>

Обезличенные драгоценные металлы – это относительная новая онлайн система MVT, которая осуществляет обмен опционами или правами на покупку некоторого количества драгоценных металлов по определенной цене. Данные производные финансовые инструменты могут быть обменены, как традиционные товарные производные инструменты или производные ценные бумаги между владельцами счетов в системе обезличенных драгоценных металлов.

Клиент покупает некоторое количество фондов виртуальных драгоценных металлов по текущей цене металла на мировой товарной бирже. Как только покупатель приобрел некое количество обезличенных драгоценных металлов, эти вклады или часть их могут быть переведены другому физическому лицу или продавцу для обмена на товары или услуги.

Самым старым и хорошо известным дилером обезличенных драгоценных металлов является e-gold LTD., которое сообщает, что имеет почти 2 миллиона счетов<sup>21</sup>. Согласно информации, предоставленной компанией e-gold и другими дилерами обезличенных драгоценных металлов, смысл использования данного вида средств сбережений заключается в упрощении проведения сетевых транзакций без учета стоимости основных валют и доступа на мировые биржи. Транзакции с обезличенными драгоценными металлами имеют незамедлительный окончательный характер, что может быть интересным онлайн продавцам, которые должны выплачивать большую комиссию за перевод между кредитными картами из-за высокого риска мошенничества. Некоторые дилеры обезличенных драгоценных металлов также позволяют пользователям иметь анонимные счета. Эти характеристики касаются федеральных правоохранительных органов США. Процедура проведения транзакций, связанных с переводом виртуальных сбережений драгоценных металлов между владельцами счетов, может привлечь к участию двух отдельных провайдеров услуг: дилера обезличенных драгоценных металлов, который обслуживает счета, содержащие сбережения драгоценных металлов, и биржевую службу по обезличенным драгоценным металлам, которая действует в качестве брокера обезличенных драгоценных металлов, которые покупают или продают дилеры. Некоторые дилеры работают напрямую с владельцами счетов. По завершению транзакции, владелец счета, продающий обезличенные драгоценные металлы, передает покупателю право собственности на свои виртуальные сбережения драгоценных металлов, и может получить вырученные деньги от продажи с помощью различных традиционных и нетрадиционных методов платежей (См. Рисунок 5).

Клиент открывает счет онлайн у дилера обезличенных драгоценных металлов		Сбережения переводятся в фондовую службу по обезличенным драгоценным металлам		Фондовая служба покупает и продает обезличенные драгоценные металлы со счета клиента, открытого у дилера
Клиент может передать право собственности на обезличенные драгоценные металлы новому собственнику, который может продавать		Вырученные деньги от продажи обезличенных драгоценных металлов могут быть получены множеством разных способов		

**Рисунок 5.** Продажа и покупка обезличенных драгоценных металлов обычно привлекает к работе две отдельные категории провайдеров услуг: фондовую биржу обезличенных драгоценных металлов и дилера обезличенных драгоценных металлов.

20. Эмитенты обезличенных драгоценных металлов используют термин «цифровая валюта» для описания договора о товарообмене, который они выполняют. Так как данный общепотребительный экономический термин возможно спутать с терминами «электронный кошелек» и «электронные деньги», в данном отчете мы используем термин «обезличенные драгоценные металлы».

21. E-dinar является отделением компании e-gold, связанным с мусульманским монетным двором, частной организацией, работающей для восстановления оборота золотой и серебряной валюты, описанной в Коране, золотого динара и серебряного дирхама. См. [www.e-dinar.com](http://www.e-dinar.com)

### 3. Оценка рисков новых систем платежей, типологии и ситуационные анализы

Потенциальные риски отмывания денег и финансирования терроризма, которые несут новые методы платежей, могут отличаться у разных провайдеров услуг, так как не существует единого стандарта применения закона или нормативно-правового регулирования о противодействии отмыванию денег и финансированию терроризма. Для определения высокой и низкой степеней рисков отмывания денег и финансирования терроризма при использовании новых методов платежей, исполнительная группа разработала модель оценки рисков (Таблица 1). Эта модель определяет критерии основных рисков, применяет данные критерии к наличным деньгам, представляющим пример очень высокой степени риска, и приводит основные варианты высокой и низкой степени риска при использовании новых методов платежей<sup>22</sup>. Затем каждый новый метод платежей оценивается индивидуально по критериям риска отмывания денег и финансирования терроризма, и приводятся возможные ситуационные анализы и типологии. Оценки рисков отдельных новых способов платежей представлены в Таблице 2.

Для точной оценки риска отмывания денег и финансирования терроризма новых методов платежей были проанализированы все факторы риска, касающиеся потребностей целевого рынка, а также действующие законы, нормативно-правовые акты, правила и методики по снижению степени рисков. Принимая в расчет все эти факторы, отдельный новый метод платежей может быть эффективным для всех законных целей, и в то же время оказываться неэффективным или, как минимум, неподходящим, для незаконных целей<sup>23</sup>.

Немногие страны определили криминальные случаи или типологии, указывающие непосредственную связь отмывания денег и финансирования терроризма с новыми методами платежей. И хотя это указывает на то, что новые методы платежей мало используются криминальными структурами и террористами, это также может указывать на ограниченную осведомленность об этих новых методах платежей внутри группы противодействия отмыванию денег и финансированию терроризма. Поэтому следующие типологии не должны считаться исключительными для какой-либо юрисдикции.

<b>Факторы рисков методов платежей</b>			
<b>Критерий</b>	<b>Наличные деньги</b>	<b>Новые методы платежей с высоким риском</b>	<b>Новые методы платежей с низким риском</b>
<b>Установление личности</b>	Анонимно	Анонимные счета, не требующие установления личности или проверки документов	Методы платежа, которые проводят проверку всех документов, удостоверяющих личность клиента
<b>Лимиты сумм</b>	Не ограничено	Любой метод анонимного платежа, без ограничений суммы вложений или перевода	Установлены определенные лимиты на размер сбережений и сумм транзакций <sup>24</sup>
<b>Методы вложения денег</b>	Анонимно, без посредников, без записи транзакции	Используя анонимный источник вложения средств (например, наличные деньги или денежный перевод) для оплаты или получения денежных средств со счета нового метода платежей, который также может быть использован анонимно для	Использование методов вложения, оплаты и перевода денежных средств, которые требуют проверки личности клиента, а также проводятся регистрационные записи транзакции по каждому переводу денежных средств.

22. Наличные денежные средства часто являются идеальным способом перевода денег для криминальной деятельности, потому что этот способ анонимен, не оставляет следов, не требует участия посредников, широко применяется и подходит для немедленного расчета. Риски отмывания денег или финансирования терроризма новых методов платежей, обсуждаемые в данном отчете, могут быть оценены по их сходству с наличным использованием денег. Основной проблемой наличных денежных средств для отмывателей денег является их объем, что создает трудности при перемещении денежных средств через границу. Преступники, используя вместо наличных денег альтернативные методы платежей, включая новые методы платежей, могут решить проблему с перемещением большого количества наличности, но могут встретить другие ограничения.

23. На практике ни одна единая категория критерия риска отмывания денег и финансирования терроризма не может определить соответствующий риск отмывания денег и финансирования терроризма отдельного нового метода платежей. В дополнение к оценке новых методов платежей, анализируемых в данном отчете, представленная модель оценки рисков может быть полезной основой для анализа уровня рисков, связанного с другими платежными системами или коммерческой деятельностью.

24. Предельная сумма счета может не иметь значения, когда полностью проверяется личность клиента и ведутся записи транзакций, в других случаях предельные значения сумм могут быть необходимы.

		перевода денежных средств анонимному получателю.	
<b>Географические пределы</b>	Некоторые виды валюты применяется более широко, чем другие	Методы платежей могут использоваться для отправки/получения денежных средств за границу.	Методы платежей могут использоваться для отправки/получения денежных средств только внутри одного государства
<b>Ограничения использования</b>	Не ограничено	Платежный инструмент может использоваться только для доступа к наличным деньгам или для обмена на наличные деньги	Платежный инструмент может использоваться только для оплаты товаров и услуг

Таблица 2

### Предоплаченные карты: открытая система

**Определение.** Предоплаченные карты с открытой системой могут использоваться для осуществления анонимных переводов денежных средств через границу (См. Рисунок 6). Когда карты выпускаются без открытия банковского счета, а заявления принимаются онлайн, по факсу, в розничных точках или в отделениях оплаты чеков, недостаточная информация о клиенте в заявлении может увеличить потенциальный риск отмывания денег или финансирования терроризма. Этот риск может быть уменьшен введением лимитов на сумму на счете и размер транзакций. Некоторые провайдеры услуг связывают процесс идентификации личности клиента с суммой, находящейся на счете, а также частотой и размером проводимых транзакций по счету. И хотя предоплаченные карты имеют индивидуальный номер счета, и по ним ведется электронная запись транзакций, без точной идентификации личности владельца карты только записи транзакций правоохранительным органам может быть недостаточно для поиска владельца карты. В зависимости от юрисдикции, оффшорные эмитенты карт создают дополнительные риски отмывания денег и финансирования терроризма.

**Лимиты сумм.** Программы предоплаченных карт с открытой системой часто нацелены на четкие рыночные сегменты (например, детей, подростков, проживающих вдали от дома, взрослых, не имеющих банковского счета, взрослых, не имеющих право на получение кредитной карты). Каждый рыночный сегмент имеет четкие потребности, которые могут быть отражены в установленных банком-эмитентом лимитах сумм карты и ее пополнения. Эти лимиты включают размер суммы, которая может находиться на банковском счете, размер суммы, могущей быть предоплаченной за один раз, а также частоту пополнения счета или снятия наличных. Чем больше денег может быть перемещено со счета карты за один раз или с помощью несколько переводов в банкоматах, тем выше будет риск, относящийся к другим критериям риска.

**Метод внесения денежных средств.** Предоплаченные карты снимают деньги с предварительно оплаченного счета, который можно пополнить различными способами. Банк, выпускающий карту, и его партнеры определяют методы, какими могут пополняться счета карты. Некоторые методы, например, кредитные переводы с банковского счета или кредитной карты, включают источники платежей, которые: (i) независимо проверяют личность держателя карты; (ii) ведут запись перевода денежных средств на предоплаченную карту; и (iii) обычно выполняют политику и методику противодействия отмыванию денег, которая включает мониторинг транзакций по подозрительной деятельности. Другие методы пополнения счета, такие, как наличные и почтовые переводы, анонимны и не фиксируются в документах, что увеличивает потенциальный риск отмывания денег и финансирования терроризма независимо от других критериев риска.

**Географические пределы.** Предоплаченные карты с открытой системой, которые обеспечивают доступ к получению наличных денег через сети банкоматов, увеличивают потенциальный риск отмывания денег и финансирования терроризма независимо от других критериев риска и уменьшения риска. Однако доступ к получению наличных средств через банкоматы обычно требует введения личного идентификационного номера (PIN), который должен быть заранее установлен организацией, выпускающей карту. Однако требование введения PIN без записи транзакции не может предоставить информацию, необходимую для точного определения личности получателя.

**Ограничения использования.** Предоплаченные карты с открытой системой могут иметь ограничения в использовании. Материальные карты могут быть ограничены для использования в определенных точках продаж, позволяя только расплачиваться за товары и услуги и запрещая снятие наличных денег через банкоматы. Виртуальные карты разрешают владельцу карты использовать номер счета только для совершения транзакций по телефону или онлайн; при этом материальной карты для получения наличных денег через банкомат не существуют. Однако большинство предоплаченных карт с открытой системой являются материальными картами, что упрощает доступ к точкам продаж и банкоматам. В некоторых странах материальные карты могут также использоваться для снятия наличных денег в розничных сетях, когда продавцу выплачивается большая сумма, чем цена товара, и разница между ценой товара и уплаченной суммой возвращается владельцу карты наличными деньгами. По причинам, обсуждаемым выше, карты, которые могут предоставить доступ к наличным средствам через банкоматы, на глобальном

уровне могут увеличить потенциальный риск отмывания денег и финансирования терроризма независимо от других критериев риска.

**Типология.** Перевод незаконными способами из одной страны в другую с использованием дебетовых карт, связанных с личными банковскими счетами и сетями банкоматов, является традиционным методом отмывания денег. Факты отмывания денег были зафиксированы даже в случае существования программы по идентификации личности клиента в момент открытия банковского счета. Это может произойти, если клиент использует фальшивые документы, устанавливающие его личность. Некоторые предоплаченные карты с открытой системой предлагают доступ к банкоматам, не требуя при этом от владельца карты открытия счета в банке или без проверки его личности, создавая потенциальный риск более широкого использования данной типологии.

#### **Ситуационный анализ**

А. В 2001 году согласно сообщению о подозрительной деятельности (СПД), проведенный в Соединенных Штатах, сообщил о приобретении более 300 предоплаченных карт одним физическим лицом, которое использовало их для перевода почти 2 миллионов \$ в Колумбию. Больше общественности не было предоставлено никакой информации по этому случаю.

Б. В 2001 году оперативная группа Эль Дорадо в Нью-Йорке установила значительную тенденцию увеличения количества физических лиц, которые использовали банкоматы как средство отмывания денег через снятие денег со счета в других странах. В результате расследования было составлено более 50 отчетов о подозрительной деятельности, включающие оформленные депозитные счета наличных денег в Нью-Йорке и последующее снятие наличных через банкоматы в Колумбии, Мексике, Перу, Эквадоре и Панаме. Подобное исследование, проведенное Сетью по расследованию финансовых преступлений (органом Министерства финансов США) за четырехлетний период выявило, что обычно снятие денежных средств происходит в Колумбии, Венесуэле, Мексике, Аргентине и Бразилии. В большинстве всех отчетов по подозрительной деятельности банки описывают подозреваемые нарушения как связанные с отмыванием денег.

В. В 2004 году налоговые эксперты Германии выявили случай отмывания денег с использованием предоплаченных карт. Два участника криминального мошенничества/схемы присвоения денег незаконным путем перевели часть своих средств криминального происхождения в предоплаченные карты. Они использовали денежные средства на карте для получения наличных денег (только на территории своего государства, а не за границей) и оплаты за товары. Счета карт открывались только на короткий период (от 6 до 24 месяцев), затем они закрывались и открывались новые счета. Таким образом, было скрыто и использовано более 350 000 евро.

---

25. Созданная в 1992 году в целях борьбы с отмыванием денег в Нью-Йорке оперативная группа Эль Дорадо стала одной из самых успешных оперативных групп по борьбе с отмыванием денег. Группой управляет федеральный правоохранительный орган по контролю за соблюдением иммиграционного и таможенного законодательства, и в ее состав входят представители 29 федеральных, штатных и местных правоохранительных органов.



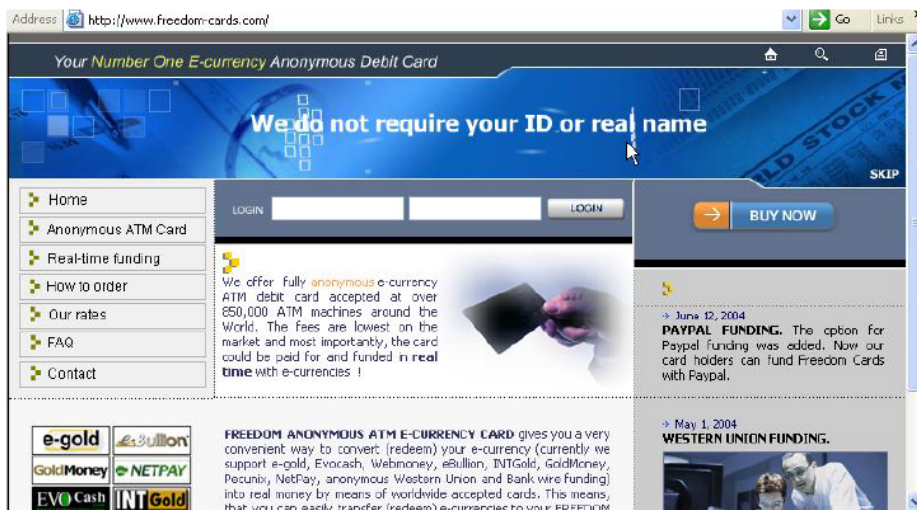


Рисунок 6

### Предоплаченные карты: закрытая система

**Определение.** Анонимные предоплаченные карты с закрытой системой могут быть перепроданы для получения наличных денег, что упрощает отмывание денег и финансирование терроризма. Этот риск, тем не менее, сокращается, введением ограничения на товары и услуги, которые могут быть оплачены данной картой, а также географическими пределами принятия карты.

**Лимиты сумм.** Предоплаченная карта с закрытой системой и большой суммой денег на счете, которая может быть перепродана, является подходящей заменой наличным деньгам для перемещения денежных средств через границы. Чем больше лимит предельной суммы предоплаченной карты закрытой системы, тем выше потенциальный риск отмывания денег и финансирования терроризма независимо от других критериев риска и сокращения риска.

**Метод внесения денежных средств.** Как и предоплаченные карты с открытой системой, на карты с закрытой системой поступают деньги с предоплаченного счета, который может пополняться различными способами, определяемыми организацией, продающей карту.

**Географические пределы.** Потенциальная перепродажа предоплаченной карты с закрытой системой зависит от доступности рынка перепродажи и уровня спроса на карту. Чем больше географическая зона, в которой принимается карта, тем выше потенциальная возможность ее перепродажи, что может увеличить возможный риск ее использования как средства отмывания денег или финансирования терроризма.

**Ограничения использования.** Карты хранения денежных средств с закрытой системой по определению ограничены в их возможном использовании. Обычно эти карты могут быть использованы только для покупки товаров или услуг, продаваемых эмитентом карты. Как отмечено выше, чем больше доступность рынка перепродажи и уровень спроса на карту, тем больше потенциальная возможность ее использования для отмывания денег и финансирования терроризма. В отличие от предоплаченных карт с открытой системой, карты с закрытой системой не могут быть использованы для получения наличных денег в банкоматах, хотя потенциально они могут быть перепроданы для получения наличных средств и куплены для получения наличных денег.

**Типология.** Оптовое распространение предоплаченных телефонных карт для звонков на большие расстояния, является, согласно Федеральному бюро расследований США, капиталоемкой отраслью промышленности с прибылью 4 миллиарда долларов в год, которая может обеспечить прикрытие отмыванию денег. На уровне розничной торговли, предоплаченные карты с закрытой системой могут потенциально покупаться анонимно в больших количествах для получения наличных денег, перевозиться за границу и перепродаваться. В отличие от валюты, сумма, находящаяся на предоплаченных картах, не выясняется таможенными и пограничными органами, хотя количество карт может декларироваться.

### **Ситуационный анализ**

А. В 2001 году Сеть по расследованию финансовых преступлений сообщила, что было заявлено более 160 отчетов по подозрительной деятельности с использованием телефонных карт с долларовыми суммами, которые варьировались от 300 000 \$ до 50 миллионов \$. В 2005 году ФБР сообщило, что обзор базы данных отчетов о подозрительной деятельности выявил, что финансовые организации все чаще сообщают о подозрительной деятельности, связанной с индустрией предоплаченных телефонных карт.

Б. В 2005 году Орган по контролю за соблюдением иммиграционного и таможенного законодательства США начал расследование в отношении служащего государственного органа в штате Огайо, продающего фальсифицированные водительские права и удостоверения личности в обмен на предоплаченные телефонные карты<sup>27</sup>.

### **Электронный кошелек**

**Определение.** Владелец карты с электронным кошельком, связанным с банковским счетом, идентифицируется в процессе открытия счета. Однако есть другие программы чип-карт, не связанных с банковским счетом, которые могут не требовать установления личности клиента и не предусматривают записи транзакций. Независимо от других факторов риска и методов уменьшения рисков, недостаточная информация об установлении личности клиента может увеличить потенциальный риск отмывания денег и финансирования терроризма.

**Лимиты сумм.** Хотя технология чип-карты не запрещает электронным кошелькам иметь неограниченные суммы денег, текущие программы карт обычно используются для транзакций с небольшой стоимостью и, таким образом, имеют низкие лимиты предельной суммы. Немецкая GeldKarte, например, имеет лимит в 200 евро.

**Метод внесения и получения денежных средств.** Электронные кошельки, связанные с банковским счетом, могут работать только с денежными средствами, внесенными на счет. Некоторые программы электронных кошельков также разрешают осуществлять переводы средств с карты на карту. Электронный кошелек, не связанный с банковским счетом, может иметь возможность пополняться наличными деньгами. Независимо от любого метода снижения риска, карта с высоким лимитом денежных средств, анонимные переводы с карты на карту, и наличные деньги в качестве выбора пополнения счета и снятия наличных могут представлять значительный риск отмывания денег и финансирования терроризма.

**Географические пределы.** Недостаточные возможности международной системы, связанной с любой программой электронных кошельков, значительно уменьшает риск отмывания денег и финансирования терроризма для этих платежных инструментов.

**Ограничения использования и получения денежных средств.** Электронные кошельки обычно ограничиваются розничными транзакциями с небольшой стоимостью, хотя некоторые программы позволяют осуществлять переводы с карты на карту и с карты в наличные деньги.

**Типология.** В настоящее время не выявлено типологий отмывания денег и финансирования терроризма, связанных с использованием электронных кошельков.

**Ситуационный анализ.** В настоящее время не выявлено случаев отмывания денег и финансирования терроризма, связанных с использованием электронных кошельков.

### **Мобильные платежи**

**Определение.** Большинство мобильных платежных систем используют мобильный телефон как средство доступа к банковскому счету или кредитной карте. Эти системы проводят идентификацию личности клиента при открытии основного счета в банке или оформлении кредитной карты. Подобная методика идентификации личности клиента происходит, когда счет для мобильных платежей открывает телефонный провайдер услуг, а не финансовое учреждение, он же предоставляет кредит владельцу счета. Если услуга

---

26. Министерство финансов, Сеть по расследованию финансовых преступлений, бюллетень отчета о подозрительной деятельности, июль 2001г.

27. Орган по контролю за соблюдением иммиграционного и таможенного законодательства США, пресс-релиз, Орган по контролю за соблюдением иммиграционного и таможенного законодательства задерживает 9 участников схемы выдачи фальсифицированных водительских удостоверений в штате Огайо, см. на сайте: <http://ice.gov/graphics/new/newsreleases/articles/drivers022405.htm>

мобильного телефона предоплачена и средства, используемые для осуществления мобильных платежей, также предоплачены, провайдер услуг может не нуждаться в полной идентификации личности клиента из-за отсутствия кредитного риска.

**Лимиты сумм.** Когда мобильные телефоны являются средством доступа к основным счетам в банке и кредитной карты, установление лимитов суммы может не являться необходимым. На Филиппинах компания Globe Telecommunication требует предварительной оплаты за транзакции по программе мобильных платежей G-cash и устанавливает максимальную сумму для транзакции в размере 10 000 песо (182 \$, 145 €), максимальную сумму транзакций в день в размере 40 000 песо (728 \$, 580 €), и размер максимального перевода в месяц в 100 000 песо (1 825 \$, 1455 €).

**Метод внесения денежных средств.** Программы мобильных платежей, которые работают с предоплаченного счета, могут оплачиваться различным образом. Источники платежей, которые независимо проверяют личность собственника телефона и ведут запись перевода денежных средств на счет мобильных платежей, представляют низкий риск. Использование наличных денег для пополнения счета мобильных платежей, независимо от других факторов риска и стратегий снижения рисков, могут представлять некоторый ограниченный риск отмыывания денег и финансирования терроризма.

**Географические пределы.** Системы мобильных платежей в настоящее время не упрощают проведение международных транзакций ввиду несовместимости систем. Попытка создания в 2006 году совместного предприятия (SIMPAY) из нескольких европейских провайдеров телефонных услуг не увенчалась успехом.

**Ограничения использования.** Платежи могут быть получены только участвующей торговой организацией или организацией, сотрудничающей с провайдером.

**Типология.** В настоящее время не выявлено типологий отмыывания денег и финансирования терроризма, связанных с использованием систем мобильных платежей.

**Ситуационный анализ.** В настоящее время не выявлено случаев отмыывания денег и финансирования терроризма, связанных с использованием систем мобильных платежей.

## **Системы оплаты через Интернет**

**Определение.** Системы оплаты через Интернет могут разрешать иметь анонимные счета.

**Лимиты сумм.** Индивидуальные провайдеры услуг обычно определяют пределы суммы на счете или размера транзакции, что влияет на связанный с этим риск отмыывания денег и финансирования терроризма.

**Метод внесения денежных средств.** Системы оплаты через Интернет устанавливают собственные правила в отношении методов платежей, которые они принимают для пополнения счета и методы выплаты денежных переводов получателем. Провайдеры услуг, принимающие наличные деньги, денежные или почтовые переводы с анонимных предоплаченных карт, могут представлять больший риск отмыывания денег и финансирования терроризма, чем провайдеры услуг, которые ограничивают методы внесения денежных средств банковским счетом или кредитной картой.

**Географические пределы.** Оффшорные системы оплаты через Интернет могут упростить проведение транзакций, которые незаконны в юрисдикции плательщика. Услуга платежей онлайн действует как посредник, получая денежные средства, которые предназначены для конечного получателя. В некоторых случаях, когда прямые переводы денежных средств конечному получателю не разрешаются согласно государственным законам юрисдикции, плательщик может переводить денежные средства через оффшорную систему платежей онлайн, работающую по другому правовому режиму.

**Ограничения использования.** Индивидуальные провайдеры услуг определяют пределы использования для своей услуги.

**Типология.** Системы оплаты через Интернет предлагают потенциальную возможность для анонимных международных переводов денежных средств. Риск возрастает, когда провайдер услуги работает оффшорной в юрисдикции со слабым режимом противодействия отмыыванию денег и финансированию терроризма. Даже если соблюдаются меры по надлежащей проверке клиента, общение с клиентом проходит полностью онлайн, что ограничивает возможности проверки его личности провайдерами услуг. Это представляет риск отмыывания денег и финансирования терроризма, связанный с другими критериями риска и методами уменьшения риска.

**Ситуационный анализ.** В настоящее время не выявлено случаев отмыывания денег и финансирования терроризма, связанных с использованием систем оплаты через Интернет.

## **Обезличенные драгоценные металлы**

**Определение.** Дилеры обезличенных драгоценных металлов могут разрешать иметь анонимные счета.

**Лимиты сумм.** На счетах обезличенных драгоценных металлов может не быть определенных лимитов сумм, кроме суммы денежных средств, которая может быть внесена на онлайн счет с использованием традиционных или нетрадиционных платежных систем.

**Метод внесения денежных средств.** Каждый провайдер услуг определяет условия, касающиеся методов платежей, которые он принимает. Способность провайдеры услуги принимать определенные методы платежей также будет ограничена согласием провайдеров этих других платежных систем предоставлять доступ дилерам или брокерам обезличенных драгоценных металлов к своим услугам.

**Географические пределы.** Провайдеры услуг могут работать по всему миру без географических ограничений, хотя естественные границы будут существовать на основе доступа в Интернет. Правительства некоторых стран, таких как Китай и другие, могут также установить ограничения на типы услуг, к которым разрешен доступ их гражданам. Web-хостинг и другие провайдеры услуг могут также установить ограничения на типы web-сайтов и видов деятельности, с которыми они хотят сотрудничать.

**Ограничения использования.** Счета обезличенных драгоценных металлов могут не иметь ограничений в использовании. Каждый провайдер услуг устанавливает свои собственные правила выплаты денежных средств, но эта возможность также зависит от желания провайдеров других платежных систем предоставлять дилерам и брокерам обезличенных драгоценных металлов доступ к своим услугам.

**Типология.** Обезличенные драгоценные металлы предоставляют потенциальную возможность осуществлять международные переводы денежных средств. Риск увеличивается, когда провайдер услуг работает оффшорной в юрисдикции со слабым режимом противодействия отмыванию денег и финансирования терроризма. Даже если соблюдаются меры по надлежащей проверке клиента, общение с клиентом проходит полностью онлайн, что ограничивает возможности проверки его личности провайдерами услуг. Это представляет риск отмывания денег и финансирования терроризма, связанный с другими критериями риска и методами уменьшения риска.

### **Ситуационные анализы**

А. В марте 2004 года мужчина из штата Оклахома признался в организации незаконной финансовой схемы с использованием инвестиционного фонда онлайн. Тысячи людей потеряли около 9 миллионов долларов. Согласно Федеральному бюро расследований США, инвестиционная онлайн схема, E-Biz Ventures, отмывала деньги инвестора через систему e-gold Ltd. Человек, проживающий в Оклахоме и создавший это криминальное предприятие, мог работать с лицами, уклоняющимися от уплаты налогов, и другими преступниками, так как он, по неофициальной информации, «подчеркивал свою связь с e-gold, чтобы вызвать страх своих жертв перед федеральным правительством из-за их желания остаться анонимными».

Б. В октябре 2004 года секретная служба Соединенных Штатов прекратила работу сайта ShadowCrew.com, одного из самых крупных незаконных онлайн центров по торговле украденными документами и платежными картами. Задержан 21 человек, и на сегодняшний день 12 обвиняемых были признаны виновными. На сайте ShadowCrew.com было приблизительно 4000 членов со всего мира, которые были злоумышленными компьютерными хакерами и продавали украденные и подделанные удостоверения личности и номера кредитных и дебетовых карт<sup>29</sup>. Те из задержанных, которые признаны виновными, «признались, что члены ShadowCrew отправляли и получали платежи, осуществляя незаконную торговлю и услуги, с помощью переводов по системе Western Union и путем виртуальной валюты e-gold и Webmoney<sup>30</sup>». Один из них «с прозвищем Voleur – «вор» по-французски – хвастался в чате, что зарабатывает от 40 000 до 100 000 \$ в неделю», получая переводы по системе Western Union от сообщников, которые он отмывал на счетах e-gold за отдельную плату<sup>31</sup>.

---

28. Гроу (Grow), Брайэн (Brian), «Золотая лихорадка» (Gold Rush), Business Week, 9 января 2006 г, см. на сайте: [http://www.businessweek.com/magazine/content/06\\_02/b3966094.htm](http://www.businessweek.com/magazine/content/06_02/b3966094.htm).

29. [http://www.usdoj.gov/opa/pr/2004/October/04\\_crm\\_726.htm](http://www.usdoj.gov/opa/pr/2004/October/04_crm_726.htm).

30. <http://www.usdoj.gov/criminal/cybercrime/mantovaniPlea.htm>.

31. Гроу (Grow). В упомянутой статье.

В. В Эстонии сообщили о случае отмывания незаконных доходов через неавторизованное снятие наличных с банковского счета путем использования обезличенных драгоценных металлов. Информацию по счету получали через использование мошеннических электронных писем, которые нужно было отправить в банк получателя для подтверждения информации. Если получатель письма отвечал на письмо, сообщая информацию по счету, преступники предпринимали незаконное снятие денег со счета. Деньги отмывались в несколько этапов, включая международные переводы через Western Union и Money Gram, и, в основном, WebMoney, службу обезличенных драгоценных металлов.

### **Оффшорное обеспечение новых методов платежей**

Фактором потенциального риска, могущего быть названным общим для многих типов новых методов платежей, является фактор юрисдикции. В некоторых случаях эмитенты или провайдеры услуг новых методов платежей могут находиться в оффшорном финансовом центре, и, таким образом, подчиняться менее строгой системе законов и норм. В дополнении к этому, процессы, связанные с новыми методами платежей, часто проходят через многочисленные юрисдикции, что способствует созданию более сложного продукта. Привлечение многочисленных юрисдикций и проходящее в результате этого разделение цепочки транзакции на различные части затрудняют разработку эффективных стратегий надзора за новыми методами платежей. Когда новые методы платежей работают через Интернет, риск юрисдикции увеличивается из-за потенциальных трудностей в установлении юрисдикции, к которой принадлежит провайдер услуг, где они образованы, какие административные органы контролируют их деятельность и какой режим противодействия отмыванию денег и финансированию терроризма применяется. В этом случае любой из юрисдикций, где новый метод платежей доступен для национальных пользователей, становится очень сложно вмешаться и остановить ведущуюся незаконную деятельность. Основным ключом для решения данной проблемы может стать образование международного сотрудничества административных органов, особенно тех, которые ведут четкий и эффективный обмен информационными системами. В этом отношении хорошим примером может быть Система раннего предупреждения, предложенная Германией на Азиатско-Европейском совещании, которое проходило в Берлине в конце 2003 года и описанная ниже в рамке.

#### **Предложение Германии о системе раннего предупреждения**

Оффшорные эмитенты карт и платежные системы, независимо от того, работают ли они через агента или через Интернет, не всегда выполняют законы той страны, где они пытаются вести свою деятельность. На совещании АЗЕС в Берлине в октябре 2003 года Германия представила на рассмотрение Систему раннего предупреждения и обмена информацией для содействия сотрудничеству и обмену информацией между юрисдикциями по вопросу альтернативных систем перевода денежных средств и нелегального осуществления банковских операций. Эксперты АЗЕС<sup>32</sup> утвердили назначение контактного лица из компетентного правоохранительного или контрольного органа или управления финансовой разведки в каждой стране АЗЕС в целях содействия сотрудничеству, включая обмен информацией и, по возможности, ведения совместных действий государственных и иностранных органов власти для ограничения нелегальных видов деятельности или злоупотребления полномочиями. Эксперты из стран АЗЕС утвердили, что этот вид системы раннего предупреждения поможет предотвратить незаконные международные транзакции одновременно во всех участвующих странах и уполномочит правоохранительные и контрольные органы власти предпринять необходимое совместное действие внутри их юрисдикций. Эксперты поощрили участие в этой программе других стран<sup>33</sup>.

Система раннего предупреждения и обмена информацией позднее была одобрена некоторыми членами группы финансовых мер борьбы с отмыванием денег, которые к ней присоединились, и которым эта система была представлена во время совещания по проблеме отмывания денег Группы финансовых мер борьбы с отмыванием денег в Париже в феврале 2004 года.

И хотя Система раннего предупреждения первоначально была нацелена на противодействие нелегальным банковским операциям, она также может быть очень эффективным средством противодействия злоупотреблению использованием новых методов платежей. Эти новые методы платежей, особенно те, которые используют Интернет, имеют международную структуру, очень похожую на сеть нелегальных банков. Новые методы платежей могут использоваться для денежных переводов по всему миру. Таким образом, система раннего предупреждения является очень полезным и эффективным средством не только ведения совместных действий, направленных против злоупотребления этими новыми методами платежей, но также и для повышения информированности об этих злоупотреблениях не только внутри юрисдикций, но и по всему миру.

32. Аббревиатура АЗЕС означает Азиатско-Европейское совещание, неофициальное собрание для ведения диалога между Европейскими и Азиатскими юрисдикциями. Для дополнительной информации по АЗЕС и его членам см. [www.aseminfoboard.org](http://www.aseminfoboard.org)

33. Окончательные заключения берлинского симпозиума по альтернативным системам перевода денежных средств и незаконных банковских операций 30-31 октября 2003 года, раздел IV.

<b>Риски отмывания денег и финансирования терроризма при использовании новых методов платежей</b>		
<b>Метод платежа</b>	<b>Факторы потенциального риска</b>	<b>Факторы уменьшения действующих и потенциальных рисков</b>
<b>Предоплаченные карты: открытая система</b>	<ul style="list-style-type: none"> <li>- Анонимный владелец карты</li> <li>- Анонимное внесение средств (приход) и анонимный доступ к средствам (уход)</li> <li>- Высокий лимит сумм на карте и/или отсутствие ограничений в количестве карт, которые может приобрести физическое лицо</li> <li>- Доступ к наличным средствам через банкоматы во всем мире</li> <li>- Оффшорные эмитенты могут не соблюдать законы всех юрисдикций</li> </ul>	<ul style="list-style-type: none"> <li>- Проверять личность владельца карты</li> <li>- Средства установления лимитов пополнения денежных средств</li> <li>- Ограничение сумм на карте и/или количества карт, которые может приобрести физическое лицо и/или ограничение суммы транзакции</li> <li>- Ограничение доступа к наличным за границей</li> <li>- Мониторинг транзакций и отчет о подозрительной деятельности</li> <li>- Применение блокировки карты/счета</li> <li>- Ограничение доступа к сети нежелательных торговых организацией и провайдеров/сетей банкоматов</li> </ul>
<b>Предоплаченные карты: закрытая система</b>	<ul style="list-style-type: none"> <li>- Анонимный владелец карты</li> <li>- Анонимное внесение средств</li> <li>- Высокий лимит сумм на карте</li> <li>- Заменяет контрабандный ввоз большого числа наличных денег</li> <li>- Отсутствие ограничений в количестве карт, которые может приобрести физическое лицо</li> </ul>	<ul style="list-style-type: none"> <li>- Проверять личность владельца карты</li> <li>- Ограничение сумм на карте и/или количества карт, которые может приобрести физическое лицо</li> <li>- Средства установления лимитов пополнения денежных средств</li> <li>- Мониторинг транзакций и отчет о подозрительной деятельности</li> <li>- Отсутствие прямого доступа к наличным деньгам через банкоматы</li> <li>- Применение блокировки карты/счета</li> </ul>
<b>Электронный кошелек</b>	<ul style="list-style-type: none"> <li>- Анонимный владелец карты</li> <li>- Анонимное внесение и получение средств</li> <li>- Высокий лимит сумм на карте</li> <li>- Отсутствие записей транзакций</li> </ul>	<ul style="list-style-type: none"> <li>- Проверять личность владельца карты</li> <li>- Отсутствие возможности перевода с карты на карту</li> <li>- Ограничения сумм, которые могут быть потрачены/храниться</li> <li>- Ограниченное функционирование за границей</li> <li>- Ограничение способов внесения денежных средств</li> <li>- Мониторинг транзакций и отчет о подозрительной деятельности</li> <li>- Применение блокировки карты/счета</li> </ul>
<b>Мобильные платежи</b>	<ul style="list-style-type: none"> <li>- Анонимные счета</li> <li>- Анонимное внесение и получение средств</li> <li>- Высокий лимит внесения денежных средств на счет или его отсутствие</li> </ul>	<ul style="list-style-type: none"> <li>- Владальцы счетов определяются, когда телефоны используются как средство доступа к банковскому счету или кредитной карте, или когда телефонная компания проверяет личность собственника телефона</li> <li>- Ограниченное функционирование за границей</li> <li>- Ограничение суммы счета или транзакции</li> <li>- Ограничение способов внесения денежных средств</li> <li>- Мониторинг транзакций и отчет о подозрительной деятельности</li> <li>- Применение блокировки карты/счета</li> <li>- Ограничение доступа к сети</li> </ul>
<b>Обезличенные драгоценные металлы</b>	<ul style="list-style-type: none"> <li>- Анонимные счета</li> <li>- Анонимное внесение и получение средств</li> <li>- Высокий лимит внесения денежных средств на счет или его отсутствие</li> <li>- Оффшорные провайдеры могут не соблюдать законы других юрисдикций</li> </ul>	<ul style="list-style-type: none"> <li>- Проверять личность владельца счета</li> <li>- Вести запись транзакций между отправителем и получателем</li> <li>- Мониторинг транзакций и отчет о подозрительной деятельности</li> <li>- Ограничение способов внесения денежных средств</li> <li>- Применение блокировки счета</li> <li>- Ограничение доступа к услуге</li> </ul>
<b>Системы оплаты через Интернет</b>	<ul style="list-style-type: none"> <li>- Анонимные счета</li> <li>- Анонимное внесение и получение средств (банкоматы)</li> <li>- Высокий лимит внесения денежных средств на счет или его отсутствие</li> <li>- Оффшорные провайдеры могут не соблюдать законы других юрисдикций</li> </ul>	<ul style="list-style-type: none"> <li>- Проверять личность владельца счета</li> <li>- Вести запись транзакций, устанавливающих личность отправителя и получателя</li> <li>- Мониторинг транзакций и отчет о подозрительной деятельности</li> <li>- Ограничение способов внесения денежных средств</li> <li>- Применение блокировки счета</li> <li>- Ограничение доступа к услуге</li> </ul>

Таблица 3

## **5. Применение рекомендаций и специальных рекомендаций ФАТФ; выбранные нормативные подходы<sup>34</sup>**

40 рекомендаций и 9 специальных рекомендаций ФАТФ определяют потенциальные риски отмывания денег и финансирования терроризма, связанные с новыми методами платежей, и обеспечивают руководство для регулирования деятельности провайдеров услуг внутри страны.

Пятая рекомендация касается анонимных счетов, которые представляют основной риск отмывания денег и финансирования терроризма, определенный для новых методов платежей, анализируемых в данном отчете. В Пятой рекомендации сказано, что «финансовым организациям<sup>35</sup> не следует вести анонимных счетов или счетов, открываемых на явно вымышленные имена».

Восьмая рекомендация специально касается рисков отмывания денег и финансирования терроризма, которые могут быть связаны с новыми методами платежей: «Финансовые организации должны обращать особое внимание на любые угрозы отмывания денег, которые могут появиться в результате развивающихся технологий, которые могут содействовать анонимности, и принимать меры, в случае необходимости, для противодействия их использованию в схемах отмывания денег».

Рекомендация 23 подчеркивает необходимость для всех провайдеров финансовых услуг принимать адекватные меры правового регулирования и контроля. В отношении широкой категории услуг по переводу денег и ценностей в рекомендации 23 сказано: «Как минимум, финансовые организации, предоставляющие услуги по переводу денег или ценностей или обмену валюты, должны лицензироваться и регистрироваться и подлежать эффективным системам мониторинга, а также обеспечивать соблюдение национальных требований по борьбе с отмыванием денег и финансированием терроризма».

Специальная рекомендация VI дополняет Рекомендацию 23, утверждая, в частности: «Каждая страна должна принять меры для обеспечения того, чтобы физические и юридические лица, включая агентов, которые оказывают услуги по переводу денег или ценностей, а также осуществляют транзакции через неофициальные системы или сети денежных переводов или ценностей, должны иметь лицензию, быть зарегистрированными и соблюдать все Рекомендации ФАТФ, применяемые для банков и небанковских финансовых организаций».

Специальная Рекомендация VII устанавливает объем информации, обязательной для предоставления при осуществлении национальных и международных электронных переводов, но предоставляет достаточно широкую свободу действий в отношении того, как финансовые организации и юрисдикции могут понимать и реагировать на полноту полученной информации по электронным переводам.

Рекомендация 21 указывает потенциальную необходимость прекращения «деловых отношений и операций с лицами, включая компании и финансовые организации, из стран, которые не применяют или применяют в недостаточной мере Рекомендации ФАТФ».

Глоссарий ФАТФ описывает виды деятельности, которые осуществляются финансовыми организациями, как вид деятельности в пользу или от имени клиента, «выпускающих и управляющих способами платежей (то есть кредитными и дебетовыми картами, чеками, туристическими чеками, платежными поручениями и банковским траттами, электронным деньгами)».

### **Нормативные подходы**

Определение размеров и типов транзакций, которые используют новые методы платежей, описанные в данном отчете, является трудной задачей, так как лишь немногие страны показывают свою информированность в данных методах платежей и ведут мониторинг их использования. Банк по международным расчетам сообщает: «С технологией, упрощающей разделение традиционных банковских услуг на многочисленные компоненты, и дополнением аналитических способов и других возможностей к традиционным банковским услугам, вероятно, большое число нелицензированных небанковских организаций предоставляют услуги, подобные банковским, через Интернет, включая также и предоставление услуг на международном уровне».

---

34. Нормативные подходы, упомянутые в данном разделе, были проверены участвующими юрисдикциями. Некоторые меры специально не были приняты в целях противодействия отмыванию денег, но только органами финансового контроля и денежно-кредитного регулирования для защиты других финансовых интересов.

35. Термин «финансовые учреждения» относится к провайдерам услуг, которые осуществляют перевод денег и ценностей как в официальном, так и в неофициальном секторе.



Разница в определениях того, что является «банком» в различных юрисдикциях, по-видимому, будет увеличиваться и все в большей степени влиять на то, как руководители надзорных банковских инстанций будут поступать с финансовыми организациями, не имеющими внутреннего надзора<sup>36</sup>. Банк по международным расчетам отмечает, что «с течением времени некоторые технологические компании, предлагающие услуги, подобные электронным банковским операциям, могут переместиться в юрисдикции, где их особый набор продуктов и услуг не будет требовать получения банковской лицензии, подобно тому, как раньше развивались оффшорные центры<sup>37</sup>».

«Тенденция относительно большого диапазона провайдеров услуг и увеличения сетей на рынках конечного пользования вызвала несколько вопросов в отношении нормативно-правовой базы. Нормативные подходы, принятые разными странами с общей эффективностью, проблемы определения рисков и клиентов, связанных с новыми методами платежей, провайдеров и устройств рынков в некоторой степени отличались. В некоторых европейских странах ответом на проблему было введение ограничений финансовым учреждениям на предоставление некоторых услуг по платежам. В других странах предоставление платежных инструментов и услуг не было ограничено<sup>38</sup>».

### **Регулятивные нормы Германии в отношении prepaid карт**

В схеме использования prepaid карты немецкие финансовые надзорные органы сосредотачивают внимание на эмитенте карты (в основном, банках) и брокере карты (провайдер услуг, являющийся посредником между банком и владельцем карты). Действуя как агент для налаживания клиентских отношений между эмитентом карты и клиентом/владельцем карты, брокер карты считается получателем депозитного брокерского вознаграждения. Это связано с тем, что в Германии принятие денежных средств для выпуска prepaid карты считается равноценным открытию вклада. Как следствие, для выпуска prepaid карт требуется генеральная лицензия на ведение банковской деятельности. Эмитент карты считается кредитным учреждением, и, таким образом, должен полностью выполнять программу противодействия отмыванию денег, включая установление личности клиента.

Относительно данных схем prepaid карт, где эмитент карты находится за границей, эмитент карты может опираться на провайдера услуг, являющегося посредником (так называемого «брокера карт») для продвижения карты на ключевом рынке. Действуя как агент для налаживания клиентских отношений между эмитентом карты и клиентом/владельцем карты, брокер карты считается получателем депозитного брокерского вознаграждения. Данный тип деятельности брокерского депозита не требует лицензии, если депозитарий (в данном случае эмитент карты) находится на территории Европейской экономической зоны.

Однако, если брокер карты действует как агент эмитента карты, находящегося за пределами Европейской экономической зоны, брокер карты считается финансовой организацией и подлежит лицензированию. Как организация по финансовым услугам, брокер карт должен полностью выполнять программу противодействия отмыванию денег, включая установление личности клиента.

### **Режим ЕС по электронным деньгам**

В Европейском Союзе есть два законодательных акта, которые регулируют системы электронных денег: Директива 2000/46/ЕС<sup>39</sup> (Директива об организациях, использующих электронные деньги) и Директива 2005/60/ЕС (третья Директива об отмывании денег); последняя должна быть внесена государствами-членами в их государственное законодательство к декабрю 2007 года.

Пока еще широко принято, что определение электронных денег включает prepaid карты, электронные кошельки и системы оплаты через Интернет, такие, как PayPal, есть некоторое противоречие в отношении того, входят ли в это понятие мобильные платежи. Во всем ЕС есть только шесть «чистокровных» эмитентов электронных денег, так как большинство организаций-эмитентов электронных денег являются банками, ведущими также иную банковскую деятельность.

---

36. Управление и надзор над международными электронными банковскими операциями, Банк международных расчетов, июль 2003г. Доступно на сайте: <http://www.bis.org/publ/bcbs99.pdf>

37. Там же.

38. CPSS #33

39. Официальный бюллетень L275, 27.10.2000

40. Официальный бюллетень L309, 26.10.2005

Вследствие гибкости, обеспеченной Директивой по учреждениям электронных денег в отношении применения мер противодействия отмыванию денег и финансированию терроризма, государства-члены ЕС в настоящее время применяют различные режимы для электронных денег: большинство государств-членов применяет те же положения о противодействии отмыванию денег и финансированию терроризма, что и установлены для банков, некоторые применяют менее строгий режим, но ожидается изменение ситуации после того, как третья Директива об отмывании денег будет внесена в государственное законодательство.

В частности, третья Директива об отмывании денег дает возможность государствам-членам ЕС разрешать эмитентам электронных денег не применять меры по надлежащей проверке клиентов в отношении электронных денег в случае, если механизм не может быть повторно использован, максимальная сумма, хранимая в системе, не превышает 150 евро, или если в случае возможности повторного использования инструмента, ограничение в 2500 евро введено для общей суммы транзакций в течение календарного года, за исключением случая, когда сумма в 1000 евро или более выплачивается держателем в этом же календарном году.

Упрощенные меры по надлежащей проверке клиентов применяются для других продуктов или транзакций, имеющих низкий риск отмывания денег и финансирования терроризма, в соответствии с техническим критерием, установленным для того, чтобы помочь оценить, когда ситуации представляют низкий, а когда высокий риск отмывания денег и финансирования терроризма.

Несмотря на установленные технические критерии, упрощенные меры по надлежащей проверке клиентов не применяются в случае, когда имеется доступная информация, которая подсказывает, что продукт представляет собой высокий риск ненадлежащего применения в целях отмывания денег и финансирования терроризма.

### **Правовое регулирование платежей через Интернет и других новых систем платежей в Соединенных Штатах**

Всеобъемлющий режим противодействия отмыванию денег и финансированию терроризма в Соединенных Штатах требует от «финансовых организаций» (как определено в Законе о банковской тайне и исполнительных распоряжениях), помимо прочего, установить и выполнять программы противодействия отмыванию денег, регистрировать транзакции с наличными деньгами, вести отчеты по подозрительной деятельности и другие документы, соблюдать меры по надлежащей проверке клиентов и применять и сохранять записи, касающиеся установления и проверки личности клиентов. В рамках этой программы недепозитарные финансовые организации, которые предоставляют услуги по платежам, имеют тенденцию принадлежать к определенной категории «предприятий по оказанию денежных услуг». Предприятия по оказанию денежных услуг определяются как включающие пять четких типов провайдеров финансовых услуг: валютные дилеры или специалисты по обмену валюты, инкассаторы чеков, эмитенты дорожных чеков, платежных поручений или предоплаченных карт, продавцы или плательщики дорожных чеков, платежных поручений или предоплаченных карт, и отправители денег. Пять типов финансовых услуг являются взаимосвязанными и часто предлагаются совместно в одном месте. Предприятия по оказанию денежных услуг сейчас предлагают ряд финансовых продуктов, которые традиционно исполняли банки.

Как отмечено выше, отправители денег и эмитенты, продавцы или плательщики продуктов с «предоплаченной стоимостью» являются предприятиями по оказанию финансовых услуг, подлежащими выполнению режима противодействия отмыванию денег и финансированию терроризма в Соединенных Штатах, который требует от некоторых предприятий по оказанию финансовых услуг зарегистрироваться в Сети по расследованию финансовых преступлений (Управлении финансовой разведки), а также установить программы противодействия отмыванию денег и соблюдать требования по предоставлению различных отчетов и ведению записей. Многим типам предприятий по оказанию услуг также необходимо иметь лицензию государственного уровня. Соответствие определению о предприятии по оказанию финансовых услуг отдельной сетевой платежной системы, провайдера услуг предоплаченных обезличенных драгоценных металлов, другого провайдера предоплаченных продуктов, платежных систем или обезличенной валюты, согласно нормативным положениям, определяется в каждом конкретном случае. Это определение зависит от таких факторов, как структура, месторасположения, оказываемые операции и услуги данного вида деятельности. Если выявлено, что услуга или деятельность является предприятием по оказанию финансовых услуг согласно данным нормативным положениям, он подлежит выполнению всех требований по выполнению программы, предоставлению отчетов и ведению записей, описанных здесь. Многие платежные системы, в особенности провайдеры платежных систем онлайн, находятся за пределами Соединенных Штатов и не принадлежат к юрисдикции США. Американские федеральные банковские организации, Сеть по расследованию финансовых преступлений и другие организации регулярно предоставляют инструкции для депозитных учреждений, касающиеся потенциальных рисков, связанных с провайдерами небанковских платежных услуг и доступные методы уменьшения данных рисков<sup>41</sup>.

41. Например, статьи Федерального совета по надзору за финансовыми учреждениями Справочное руководство Закона о банковской тайне/противодействия отмыванию денег, касающееся электронных наличных денег, предоплаченных продуктов и сторонних платежных устройств были обновлены в июле 2006 года для выделения факторов риска данных продуктов и рекомендации действий, которые депозитные учреждения должны предпринять для уменьшения данных рисков.

### **Использование «специальных мер» в Соединенных Штатах**

Соединенные Штаты могут возбудить судебное дело против новых методов платежей, расположенных за пределами страны, которые представляют угрозу отмывания денег в Соединенных Штатах<sup>42</sup>. Министр финансов США уполномочен – проконсультировавшись с Министерством юстиции, Министерством иностранных дел и соответствующими федеральными финансовыми инспекциями – определить иностранную юрисдикцию, учреждение, класс транзакции или тип счета, представляющих особо значительный риск отмывания денег.

Есть целый ряд доступных способов для эффективного определения особого риска отмывания денег. Через установление различных «специальных мер», министр финансов может получить подробную информацию о юрисдикциях, учреждениях, транзакциях и счетах, которые являются подозрительными, и предпринять соответствующее действия для обеспечения безопасности финансовых организаций США.

Специальные меры, доступные министру финансов, включают требование от финансовых организаций США: (1) вести записи и предоставлять отчеты о некоторых финансовых транзакциях; (2) собирать информацию о доверительном управлении; (3) собирать информацию о некоторых транзитных счетах; (4) собирать информацию о некоторых корреспондентских счетах; и (5) запрещать или устанавливать условия на открытие и обслуживание корреспондентских и транзитных счетов.

### **Индия запрещает использование обезличенных драгоценных металлов**

В октябре 2002 года индийский Центробанк, Резервный банк Индии, запретил использование системы “e-gold”, как нарушающей национальные правила, требующие использования в транзакциях внутри страны только государственных валют. Центральный банк постановил в пресс-релизе: «Кажется, у некоторого числа лиц населения и агентств создалось впечатление, что транзакции с использованием системы “e-gold”, подразумевающей электронную валюту, свободно разрешены в Индии и что e-gold имеет статус иностранной валюты... Резервный банк прояснил общественности ситуацию о том, что e-gold не является валютой ни одного суверенного государства<sup>43</sup>».

### **Австралия: нелицензированные сайты по обезличенным драгоценным металлам**

В 2004 году Австралийская комиссия по ценным бумагам и инвестициям выявила несколько онлайн дилеров обезличенных драгоценных металлов, некоторые из которых находились за пределами страны, ведущих свою деятельность без соответствующей лицензии: «проводя исследование web-сайтов, торгующих электронной валютой, Австралийская комиссия по ценным бумагам и инвестициям заинтересовалась тремя компаниями, расположенными в Австралии, которые работали на данных сайтах как агенты иностранных предприятий с подобным видом деятельности. Эти предприятия обменивали общепринятую валюту на электронные деньги и наоборот, а за свои услуги взымали комиссию. Австралийская комиссия по ценным бумагам и инвестициям считает, что данные продукты могут быть определены как безналичные платежные системы, и лица, ведущие данную деятельность с клиентами из Австралии, должны иметь австралийскую лицензию на оказание финансовых услуг». Установленные предприятия «закрыли все сайты и добровольно прекратили свою деятельность<sup>44</sup>».

## **6. Результаты ответов на вопросы анкеты о новых методах платежей и их анализ**

### **Цели и методика**

Данный раздел дает обзор ответов на анкету, созданную исполнительной группой, и на которую ответило 37 стран. Большинство респондентов определили новые методы платежей в своих юрисдикциях. В некоторых странах респонденты еще не определили новых методов платежей (например, в Аргентине, Камбодже и Словении) или только предоставили информацию о традиционных способах платежей (например, Катар, Латвия, Макао и Словакия), или даже традиционных способах платежей,

---

42. Некоторые онлайн платежные системы могут быть лицензированы в одной стране и проводить операции (включая набор персонала, компьютерных систем и привлечение клиентов) во многих других странах без физического присутствия в них торговой организации.

43. [http://www.rbi.org.in/scripts/BS\\_PressReleaseDisplay.aspx](http://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx)

44. [http://www.asic.gov.au/asic/asic\\_pub.nsf/byheadline/04-366+ASIC+acts+to+shut+down+electronic+currency+trading+websites?openDocument](http://www.asic.gov.au/asic/asic_pub.nsf/byheadline/04-366+ASIC+acts+to+shut+down+electronic+currency+trading+websites?openDocument)

которые могут быть оценены новыми способами, как банковские операции через Интернет (например, Азербайджан). Некоторые респонденты конфиденциально сообщили исполнительной группе, что есть нерешенные случаи и расследования, проходящие в настоящее время, касающиеся новых методов платежей, но эти случаи не могут быть разглашены.

Итоговые результаты по каждому методу платежей из анкеты представлены ниже, более подробная информация дана в Приложении Б о следующих позициях: категория нового метода платежей, размер рынка, нормы доступа к деятельности, положения противодействия отмыванию денег и финансирования терроризма и случаи противодействия отмыванию денег и финансирования терроризма, а также наличие нелегальных операторов. Выводы также представлены в конце данного раздела по каждой категории новых методов платежей.

#### **Предоплаченные карты**

Четырнадцать стран, приблизительно одна треть респондентов, сообщили о наличии предоплаченных карт как с открытой, так и с закрытой системой. В отношении карт с открытой системой, часто есть доступность банкоматов, иногда они предоставляют возможность переводить деньги по всему миру.

Немного информации было сообщено в отношении размеров рынка, но в случае, когда эта информация была представлена, сообщалось о небольшом или развивающемся рынке.

Большинство из сообщаемых типов предоплаченных карт выполняют как требования регистрации, так и лицензирования, или же находятся под контролем (исключениями являются Палау и Новая Зеландия). В отношении положений противодействия отмыванию денег и финансированию терроризма ситуация разнородна, так как менее чем в половине<sup>45</sup> стран положения противодействия отмыванию денег и финансирования терроризма не применяются (исключая США и Чехию). Интересно заметить, что все методы платежей, которые не подлежат правовому регулированию противодействия отмыванию денег и финансированию терроризма, имеют ограничение суммы перевода.

За исключением США и Новой Зеландии, не было сообщено о случаях отмывания денег и финансирования терроризма. Не было также выявлено и нелегальных операторов, без исключений.

#### **Платежи, выполняемые с помощью мобильного телефона (и связанного с банковским счетом)**

Четыре страны сообщили об использовании мобильных телефонов для доступа к банковскому счету (Корея, Финляндия, Новая Зеландия и Китай). Если платежный метод основан на банковском счете, применяется регистрация/лицензия, а также осуществляется надзор и выполняются положения противодействия отмыванию денег и финансированию терроризма.

Не сообщалось о случаях отмывания денег и финансирования терроризма или о наличии нелегальных операторов.

#### **Электронный кошелек**

Четыре страны (Бельгия, Швейцария, Германия и Нидерланды) сообщили о наличии электронных кошельков в своих юрисдикциях. Во всех случаях от эмитентов электронных кошельков требуется наличие регистрации и лицензии, применение надзора и выполнение положений противодействия отмыванию денег и финансированию терроризма. Во всех случаях установлены лимиты на суммы переводов. Ни в одной из этих стран не было выявлено случаев отмывания денег или правоприменительных действий.

#### **Платежи через Интернет**

Это самая большая группа новых методов платежей, так как о ней сообщило 15 из 37 стран (40%). Системы различаются в разных странах; некоторые из них (например, PayPal, Neteller) работают в нескольких юрисдикциях.

Большинство стран применяют требования о регистрации/лицензировании и надзоре, или же работают над применением этих нормативных положений. Большинство стран также применяют положения о противодействии отмыванию денег и финансированию терроризма (иногда даже если не применяются требования регистрации/лицензирования/надзора).

Среди стран, где положения о противодействии отмыванию денег и финансированию терроризма не применяются (Нидерланды, Испания, Китай), только Китай нашел основания для применения положений от отмывания денег и финансировании терроризма. Примеры правоприменительных действий были в США, Эфиопии и Канаде.

---

45. Слово «половина» правильно только в том случае, если принять в расчет, что Палау и Новая Зеландия указали, что даже если они применяют положения о противодействии отмыванию денег и финансировании терроризма, у них нет требования о регистрации или лицензировании, а также о надзоре.

Одной из проблем, сообщенной в отношении новых методов платежей, является возможность провайдеров платежных услуг предлагать свои услуги оффшорно, и, таким образом, обходить правила регистрации/лицензирование в стране назначения, а также требования о надзоре и выполнении положений о противодействии отмыванию денег и финансированию терроризма.

#### **Мобильные платежи**

Только пять стран (примерно 10% от числа стран, участвующих в опросе) сообщили о наличии этого нового метода платежей. В этих странах данный новый метод платежей, скорее всего, используется для микроплатежей. Картина разнородна в отношении регулирующей системы и применения требований положений о противодействии отмыванию денег и финансированию терроризма.

Ни в одной из этих стран не было выявлено случаев отмывания денег и финансирования терроризма или правоприменительных действий.

#### **Обезличенные драгоценные металлы**

Данный новый метод платежей не является широко распространенным, так как только 2 страны (Эстония и США) сообщили и его наличии в своих юрисдикциях. Эстония больше не сообщила никакой информации. В США работает значительное количество операторов, но они не обязательно находятся на территории США, и открыто большое количество счетов. Применяемая правовая система и положения о противодействии отмыванию денег и финансированию терроризма зависят от штата, в котором функционирует метод платежа. Однако большинство услуг по обезличенным драгоценным металлам находятся за пределами США и не подчиняются законам США, хотя они и могут быть использованы американскими гражданами. Было сообщено о случаях правоприменительных действий.

## **7. Выводы и задачи для дальнейшего изучения**

Ответы, данные странами в анкете, отправленной в начале данного исследования, отражают обоснованный спрос рынка, на который отвечает каждый из анализируемых методов платежей, хотя существуют некоторые реальные и потенциальные угрозы отмывания денег и финансирования терроризма. Рекомендации ФАТФ 40+9, вероятно, позволяют внедрение инноваций платежных систем и положений о противодействии отмыванию денег и финансированию терроризма, так как они обеспечивают необходимый уровень гибкости в применении стандартов о противодействии отмыванию денег и финансированию терроризма для новых методов платежей, развивающихся на основе технологий.

Среди основных определенных факторов риска данное исследование подчеркивает, что провайдеры новых методов платежей, которые расположены за пределами юрисдикции данной страны, могут создавать дополнительные риски по сравнению с провайдерами, расположенными на территории страны, особенно когда: (i) используемым каналом связи является Интернет; (ii) нет прямого контакта с клиентом; и (iii) новый метод платежей работает через открытую сеть, доступ в которую возможен в большом числе юрисдикций.

Случаи, когда новые методы платежей, определенные в данном исследовании, могут использоваться в незаконных целях, в настоящее время трудно определить. Ответы на вопросы анкеты, изданной нашей исполнительной группой, предоставляют только ограниченное число типологий и показывают, что уровень развития и/или информированность о новых методах платежей неодинаковы по всему миру. В этом отношении необходимо заметить, что новые методы платежей быстро и значительно развиваются; следовательно, случаи правоприменительных действий могут также участиться в ближайшем будущем.

Как отмечено ранее, считается, что Сорок рекомендаций и Девять специальных рекомендаций ФАТФ создают подходящую программу для предотвращения угроз, которые представляют новые методы платежей, определенные исполнительной группой. Однако, отмечая различные характеристики и разное развитие новых платежных систем в каждой юрисдикции, в исследовании подчеркивается возможность для дальнейшего исследования специальных мер, которые могут быть приняты странами для ограничения определенных рисков. В случае новых методов платежей технология играет двойную роль: с одной стороны, она может увеличить типичные риски отмывания денег и финансирования терроризма (то есть анонимность, всемирное использование, скорость переводов, правомерный арбитраж, оффшорное оказание услуг), а с другой стороны, поможет предотвратить или ограничить данные риски (например, введение лимитов на использование, электронная запись транзакций и т.д.). Эти дополнительные меры могут быть приняты в дополнение или вместо традиционных положений о противодействии отмыванию денег (например, меры по надлежащей проверке клиентов могут быть заменены на установление лимитов на переводы и снятие сумм по платежному инструменту, которые будут иметь пороговые значения, или установление границ использования – таких, как невозможность пополнения счета или географические ограничения использования платежного инструмента).

С учетом результатов данного проекта, рекомендуется, чтобы рабочая группа рассмотрела следующие возможные будущие действия по данной теме:

- А) обеспечение руководства юрисдикциям в отношении того, какие превентивные меры могут быть приняты для ограничения риска новых методов платежей, используемых для отмывания денег и/или финансирования терроризма (это может происходить по Рекомендации 8 ФАТФ);
- Б) обновление данного исследования вследствие развития новых методов платежей, а также связанных с ними типологий и анализов рисков по истечении двухлетнего периода;
- В) предложение о включении новых методов платежей в специальную задачу для мониторинга – в течение двухлетнего периода, упомянутого выше под буквой Б) - в рамках проекта по тенденциям и показателям отмывания денег и финансирования терроризма.

## **Приложение А. Описание традиционных сетей кредитных и дебетовых карт**

### **Описание сети**

Существует, по меньшей мере, шесть всемирных сетей кредитных карт: Visa (лидер данного рынка), MasterCard, American Express, Diners Club, JCB и Discover. Также существуют собственные сети кредитных карт, которые могут работать по всему миру для ограниченных целей совершения покупок в торговых сетях. В дополнение к этому есть разнообразные сети, которые поддерживают дебетовые карты и транзакции через банкоматы: Plus (Visa), Cirrus (MasterCard), Electron (Visa) и Maestro (MasterCard) работают во всем мире; Interact (Канада), STAR (США) и другие сети работают в одной или нескольких странах или регионально внутри одной страны. Исторически карта и услуги сети EFT (эффективных финансовых транзакций) и POS (терминалов оплаты) немного различались, не только в определении разницы кредита и дебета для продуктов, но и в способах авторизации подхода к этим продуктам. Кредитные карты появились от точек продаж, моделей расходной карты, и первоначально использовались «оффлайн» или на основе авторизации подписи. Сети EFT (эффективных финансовых транзакций) и POS (терминалов оплаты) появились на основе карт «онлайн» или карт с индивидуальным личным номером (PIN) и определенной модели банкоматов. Позднее, особенно в Европе и других регионах за пределами США, использование инфраструктуры карт с Pin-кодом и чип-карт стало широко распространенным как для кредитных, так и для дебетовых карт.

### **Материально-техническая база**

Поддерживающая материально-техническая база большинства сетей кредитных карт и EFT (эффективных финансовых транзакций) и POS (терминалов оплаты) перешла от использования собственных сетей и платформ к открытым системам. Так как через данные сети ежегодно проводится более миллиарда транзакций электронных платежей, стандарты и правила безопасности, принятые данными организациями, оказывают влияние на будущую технологию, доступную для индустрии платежей. Традиционное электронное соединение продавца и ассоциации, и соединение между банками в ассоциации для сети карт похоже на соединение с использованием собственной системы.

Ассоциации и компании по выпуску карт имеют собственные централизованные базовые платежные сети, которые связывают организации розничной торговли и ассоциации, а также банки внутри ассоциации, использующей специальное программное и аппаратное обеспечение. Региональные или национальные сети EFT/POS обеспечивают подобный доступ к другим финансовым организациям и возможность выполнения транзакций через банкоматы и терминалы оплаты. Эти сети могут предложить финансовым учреждениям целый ряд услуг по коммутации (маршрутизации), авторизации, клирингу и расчету, включая соответствующие операции операционного отдела банка. Другие только осуществляют коммутацию на основе сторонних процессоров для обработки большинства данных, связанных с этими услугами. Финансовые учреждения, присоединившиеся к данным сетям, могут выбирать список задач, предлагаемые данными сетями.

### **Клиринг и расчет**

У транзакции по кредитной карте есть три этапа: авторизация основного платежа и требования на покупку, клиринг бухгалтерских проводок между сторонами и расчет между сторонами в действительных денежных средствах, включающий оплату различных межбанковских и иных комиссий, связанных с проведением транзакции<sup>46</sup>. Авторизация и клиринг дебетовых транзакций, основанных на предоставлении кредита и подписи, проходят через процесс «двойного сообщения», который состоит из двух отдельных электронных передач данных; дебетовые транзакции на основе PIN, напротив, имеют процессы «одного сообщения», в которых авторизация и клиринг происходят в течение одной передачи данных. Кредитные и дебетовые транзакции, включающие материально-техническую базу карт на основе PIN и чип-карт, соответствуют одному из этих способов авторизации и клиринга.

### **Кредитные карты**

Первая передача данных по кредитной карте или дебетовой транзакции с подписью является оперативным запросом на авторизацию во время покупки. Платежная информация от карты и продавца отправляется с терминала продавца в обслуживающий банк и подключается к сети, работающей с кредитной картой, которая передает ее банку-эмитенту. Банк-эмитент отвечает «ОК», указывая, что счет кредитной карты клиента функционирует и что клиент не превысил установленный кредитный лимит. Затем банк-эмитент уменьшает «расходную» сумму кредитного лимита владельца карты на сумму покупки. Дублирующий процессор может также провести авторизацию в качестве альтернативы для банка-эмитента. Некоторые кредитные карты на основе PIN и чипа могут работать аналогичным образом.

---

46. Точные процессы, включенные во все три этапа, могут значительно варьироваться в зависимости от индивидуального оговоренных условий между банками-членами и сетями карт, или особых характеристик транзакции и участвующих сторон. Остальная часть данного исследования предназначена только для общего ознакомления с данными процессами.

В этот же день (хотя это также может различаться), в предварительно определенные часы или один раз в конце дня, торговая организация отправляет в свой обслуживающий банк второй командный файл клирингового сообщения с данными всех транзакций, проведенных с момента последней подобной передачи данных. Обслуживающий банк сверяет данные с информацией по авторизации. После проверки обслуживающий банк отправляет кредит на счет продавца на сумму транзакций за вычетом платы продавца за обслуживание транзакций. Банк пересылает отдельный файл с данными о всех транзакциях продавца в ассоциацию кредитных карт. Конечный расчет обычно начинается с ассоциации кредитных карт, использующей объединенную информацию о транзакциях банков-членов для составления чистой расчетной позиции каждого члена. Ассоциация кредитных карт предоставляет данную информацию членам через собственное расчетное программное обеспечение или «разъяснительное» сообщение, которое составляет журнал аудита и преобразует данные в формат, интерпретируемый банком. Для расчета этих чистых позиций каждый банк-эмитент в чистой дебетовой позиции (или его банк-корреспондент) делает кредитный перевод в расчетный банк ассоциации кредитных карт и его специальный расчетный счет. Кредитная ассоциация удерживает часть средств платежа для покрытия межбанковской комиссии, комиссии за обмен валют и другие виды комиссий. Затем расчетный банк делает кредитный перевод с расчетного счета на счет приобретателя с оставшейся суммой, за вычетом комиссии ассоциации. Банки члены должны иметь обеспечение в расчетных банках ассоциации кредитных карт в случае невыполнения обязательств. Банки также могут рассчитываться по транзакциям по кредитным и дебетовым картам напрямую друг с другом, через региональный расчетный банк, или другими чистыми механизмами расчета. В процессах расчетов могут быть значительные различия, которые зависят от участвующих членов.

#### Дебетование по подписи

Дебетовая транзакция на основании подписи авторизуется наподобие транзакции по кредитной карте, за исключением того, что банк-эмитент подтверждает по запросу держателя карты депозитный счет или дублирующую систему авторизации, управляемую карточной сетью. Процесс клиринга такой же, как и у транзакции по кредитной карте. Кредитные и дебетовые переводы на основе подписи могут быть отправлены отдельно. Расчет часто происходит по той же схеме, что и транзакция по кредитной карте. Некоторые сети EFT/POS также проводят дебетовые транзакции на основе подписи с конечным расчетом, включающим или кредитные переводы, или прямые дебеты. В основном сети карт рассматривают дебетовые транзакции на основе подписи и транзакции по кредитной карте как почти идентичные для обработки, клиринга и расчета. Некоторые кредитные карты с PIN-кодом и чипом могут работать аналогичным образом.

### Авторизация кредитных и дебетовых карт с подписью



Рисунок 7



## Клиринг кредитных и дебетовых карт с подписью



**Рисунок 8**

### Дебет на основе PIN-кода

В США сети карт рассматривают дебет на основе PIN-кода как существенно отличающимся и отдельным от дебета на основании подписи и транзакций по кредитным картам методом. Этот случай не похож на другие страны, где карты на основе PIN-кода и чипа одинаковы. Для дебета на основе PIN-кода авторизация и клиринг транзакции происходят через одну передачу данных. Она может быть проведена как через региональную сеть EFT/POS, такую как STAR, или национальную или международную сеть дебета на основе PIN-кода, такую как Interact (терминал оплаты или банкомат) или Maestro или Interlink, если это транзакция через терминал оплаты, или Cirrus и Plus, если это транзакция через банкомат<sup>47</sup>. Также может быть использован дублирующий процессор. Процесс авторизации в банке-эмитенте такой же, как и для авторизации дебета на основе подписи, за исключением того, что клиент должен ввести PIN-код на терминале продавца или банкомате. Банк-эмитент обычно дебетует счет владельца карты немедленно, так как конечная сумма транзакции подтверждается во время покупки. Банк-эквайер или его процессор также осуществляет полную запись транзакции в результате передачи данных, проводящей клиринг транзакции между банками. Банк-эквайер обычно кредитует продавца на сумму транзакции в то же время.

Окончательный расчет между членами EFT/POS может происходить большим количеством разных способов, так же, как он может осуществляться в сетях карт. Один из способов включает бездокументарный чистый расчет в расчетном банке, выбранном сетью EFT/POS. Каждый банковский член открывает расчетный счет в расчетном банке сети EFT/POS. Сеть EFT/POS и ее расчетный банк дебетует и кредитует счета эмитентов и эквайеров для завершения перевода денежных средств. Это включает как реальную сумму транзакции, так и различные комиссии, установленные сетью. Второй способ подходит членам, имеющим собственного операционного агента, открывающего расчетный счет в другом расчетном банке, чем у сети EFT/POS, или для членов, имеющих собственный счет. В этом случае сеть EFT/POS выплачивает прямой дебет на расчетный счет члена-эмитента (авторизация на это дается как часть требований сетевого партнерства) для кредитования счета члена-эквайера (или расчетного счета в расчетном банке сети EFT/POS в случае сетевых комиссий).

47. Когда транзакция может проходить как по региональным, так и по национальным или международным EFT/POS сетям, региональная сеть обычно имеет преимущественное право согласно региональным правилам маршрутизации. Однако продавец и Банк-эквайер могут определить собственные приоритеты для прохождения маршрутизация другим способом.

В зависимости от сети EFT/POS, процесс ежедневного расчета может включать только суммы индивидуальных транзакций или же могут быть отдельные расчеты по транзакциям, проведенным за день, и связанные с ними сетевые комиссии. Некоторые сети EFT/POS могут предоставлять отсрочку по выплате сетевых комиссий до конца месяца.

Напротив, если транзакция проходит через карточную сеть, клиринг между банками и национальной сетью происходит позже аналогично процессу чистого расчета, который обычно используется для транзакций дебета на основе подписи и транзакций по кредитным картам. Расчет может использовать традиционные национальные системы по переводу прямого дебета или кредита. Расчет основывается на положительном ответе банка-эмитента на запрос на авторизацию. Эмитент, а также эквайер платят банковскую сетевую комиссию за проведение транзакций на основе PIN через банкомат.

### Авторизация и клиринг дебетовых карт на основе PIN



Рисунок 9

## **Приложение Б. Дополнительные результаты ответов на анкету о новых методах платежей и их анализ**

Таблица А. Краткое описание новых методов платежей

Таблица Б. Двумя основными индикаторами размера рынка являются оцененное количество провайдеров услуг внутри страны и оцененное количество открытых счетов или выпущенных карт

Таблица В. Информация о регулятивных нормах. Указано различие между регистрацией (Р) и лицензированием (Л). Основное различие между этими двумя категориями заключается в том, что лицензирование предполагает в качестве предварительного условия выдачи разрешения для осуществления платежных услуг (на таких условиях, как экономические нормативы и т.д.), тогда как регистрация проводится без условий. В отношении надзора возможны различные подходы, во всех случаях, когда дается подробная информация, она записывается в отчете как «дополнительна информация».

Таблица Г. Положения о противодействии отмыванию денег и финансированию терроризма могут возникать из рабочих инструкций или из практики деловых отношений (обычным примером практики деловых отношений является установление лимитов на суммы переводов).

Таблица Д. Отчеты о случаях противодействия отмыванию денег и финансирования терроризма или о наличии нелегальных операторов (нелегальными операторами считаются незарегистрированные или не имеющие лицензии операторы).

### **Предоплаченные карты и предоплаченные платежные карты**

#### **А. Описание нового метода платежей**

<b>Страны</b>	<b>Краткое описание нового метода платежей</b>
Ирландия (IE)	«Виртуальные карты VISA» (“Virtual Visa Voucher”) – предлагаемые постоянным банком TSB совместно с VISA и службами обработки транзакций 3V, доступны с декабря 2005 года, регистрация клиентов проходит онлайн, карта печатается по запросу у участвующего распространителя, выпускается «одноразовая» предоплаченная карта; эта карта может быть использована для покупок в Интернете или при заказах по почте/телефону.
Турция (TR)	Упомянуты «предоплаченные дебетовые карты», но не предоставлено никакой дополнительной информации.
Ливан (LB)	Упомянуты предоплаченные карты, но предоставлена недостаточная информация (например, в отношении фирменных сетей Visa и MasterCard). - («Liters Plus» - это предоплаченная карта с ограниченными целями использования).
Палау (PA)	Упомянуты предоплаченные дебетовые карты, которые могут быть использованы в сетях банкоматов, но не предоставлено никакой дополнительной информации.
Литва (LT)	Упомянуты предоплаченные дебетовые карты, выпускаемые банками или магазинами, но не предоставлено никакой подробной информации
Новая Зеландия (NZ)	Карта “Visa Cash Passport” (предназначенная для покупок на территории Новой Зеландии и для снятия наличных в банкоматах Новой Зеландии и за границей); другие карты с оплаченной стоимостью используются в Новой Зеландии для покупок в закрытых системах (транспортные компании, образовательные учреждения и т.д.).
Кипр (CY)	Предоплаченные карты, выпускаемые банками; они могут использоваться в местах, где принимаются карты Visa electron и для совершения Интернет платежей; информация ограничена.
Чешская Республика (CZ)	Электронные билеты на оплату общественного транспорта; эта услуга не является международной

Италия (IT)	Пополняемые предоплаченные карты требуют полного выполнения мер по надлежащей проверке клиентов и положений о противодействии отмыванию денег и финансированию терроризма. Предоплаченные карты, которые не могут пополняться, не могут превышать сумму в 500 евро и не требуют применения мер по надлежащей проверке клиентов, таким образом, они могут быть анонимными. Данные карты выпускаются финансовыми учреждениями (например, банками и организациями работы с электронными деньгами). В некоторых случаях клиент первоначально открывает кредит в телефонной компании (карта на этой стадии является телефонной картой), а затем преобразует данный кредит в кредит в финансовом учреждении, которое является законным эмитентом предоплаченных карт (на этом этапе карта является платежным инструментом).
Австрия (AT)	Предоплаченные дебетовые карты (2 системы), которые не требуют открытия банковского счета и которые могут быть использованы для снятия наличных в банкомате и оплаты за покупки в торговых точках; методы внесения средств включают в себя наличные и кредитные переводы. Нет информации о размере рынка.
США	Указаны различные типы предоплаченных карт, включающие различные методы использования и разные технологии, работающие как по открытой, так и по закрытой системам.
Испания (ES)	Карта Hal-Cash; основана на предоплаченном счете, который обеспечивает доступ к снятию наличных с банкоматов по всему миру; мобильный телефон используется как средство доступа и передачи сообщений; это продукт в основном предлагается иммигрантам, не имеющим возможности открыть счет в банке.
Швейцария (CH)	Предоплаченная дебетовая карта многоцелевого использования. Микроплатежи могут осуществляться через Интернет и/или мобильный телефон онлайн продавцами. Пользователи счищают защитный слой карты для получения доступа к коду, который соответствует их предоплаченной кредитной сумме. Осуществляя платеж за товары или услуги, заказанные по Интернету или с помощью мобильного телефона, пользователи должны указать код карты, который дает доступ к предоплаченному счету, открытому на сервере пользователя. Затем сумма вычитается из реального баланса карты.

## Б. Размер рынка

Примерное число провайдеров услуг в стране		Примерное количество счетов, открытых эмитентами карт	
≤ 3	> 3	≤ 1000	> 1000
IT, IE, PA, NZ, CH	CZ, USA, ES	NZ (за год)	CZ, IT, USA

## В. Доступ к деятельности

Регистрация/лицензирование		Надзор		Дополнительная информация
Да	Нет	Да	Нет	
AT, CZ, IT, IE (Л), LB (Л), CH	PA, NZ, HK, ES (?), USA	IE, LB, AT, CZ, IT, CH	PA, NZ, HK, ES (?)	IE, LB: провайдерами являются банки

### Г. Положения о противодействии отмыванию денег и финансированию терроризма

Меры по надлежащей проверке клиента		Ведение бухгалтерских записей		Сообщений о подозрительных операциях		Другие правила и методики противодействия отмыванию денег		Лимит переводимой суммы, если есть	
Да	Нет	Да	Нет	Да	Нет	Да	Нет	≤ 500	> 500
AT, IT, IE, LB, PA, NZ, CH	DE, IT, USA, HK, ES	IE, LB, PA, NZ, IT, AT, USA, CH	IT, HK, ES	IE, LB, PA, NZ, AT, IT, CH	USA, HK, ES	IE, LB, PA, AT, IT, USA, CH	NZ, HK, ES	AT, CZ, IT, IE (350), NZ (25 000 NZ\$), NZ да, но зависит от сети банкоматов	USA, ES PA – не ограничено

### Д. Случаи противодействия отмыванию денег и финансированию терроризма – выявление нелегальных операторов

Сведения об отмывании денег		Примеры правоохранительных действий		Нелегальные операторы	
Да	Нет	Да	Нет	Да	Нет
NZ	AT, CZ, IT, USA, IE, LB, ES, CH	USA, NZ	AT, CZ, IT, IE, LB, ES, CH		AT, CZ, IT, USA, IE, LB, NZ, ES, CH

### Платежи, выполняемые с помощью мобильных телефонов (и связанные с банковским счетом)

#### А. Описание нового метода платежей

Страны	Краткое описание нового метода платежей
Финляндия (FI)	Система "Mobiiliraha" - связанная с банковским счетом; не предоставлено подробной информации
Новая Зеландия (NZ)	Система «Mobile phone banking» – означающая доступ к банковскому счету с помощью мобильного телефона
Китай (CN)	Система «Mobile phone banking» – означающая доступ к банковскому счету с помощью мобильного телефона
Корея (KO)	Использование мобильных телефонов или коммуникаторов для международных платежей с банковского счета на (иностраный) банковский счет

**Б. Размер рынка**

Примерное число провайдеров услуг в стране		Примерное количество счетов, открытых эмитентами карт	
< 3	> 3	< 1000	> 1000
	KO, FR		KO

**В. Доступ к деятельности**

Регистрация/лицензирование		Надзор		Дополнительная информация
Да	Нет	Да	Нет	
KO, FL, NZ, CN, FR		KO, FL, NZ, CN, FR		

**Г. Положения о противодействии отмыванию денег и финансированию терроризма**

Меры по надлежащей проверке клиента		Ведение бухгалтерских записей		Сообщение о подозрительных операциях		Другие правила и методики противодействия отмыванию денег		Лимит переводимой суммы, если есть	
Да	Нет	Да	Нет	Да	Нет	Да	Нет	<= 500	> 500
KO, FL, NZ, CN		KO, FL, NZ, CN		KO, FL, NZ, CN		KO, FL, NZ, CN			KO

**Д. Случаи противодействия отмыванию денег и финансированию терроризма – выявление нелегальных операторов**

Сведения об отмывании денег		Примеры правоохранительных действий		Нелегальные операторы	
Да	Нет	Да	Нет	Да	Нет
	KO, FL, FR		KO, FL, FR		KO, FL, FR

**Электронный кошелек****А. Описание нового метода платежей**

<b>Страны</b>	<b>Краткое описание нового метода платежей</b>
Германия (DE)	GeldKarte: Денежные средства карты находятся на самой карте; в основном, денежные средства приходят с банковского счета, для выполнения платежа не требуется подключения онлайн или идентификации личности владельца карты; данная карта фактически не работает международно. GeldKarte является в настоящее время общим технологическим стандартом для чип-карт; многие банки выпускают собственные карты GeldKarte. Однако, так как все данные карты работают полностью внутри страны, в целях данного отчета GeldKarte считается отдельным платежным инструментом.

Нидерланды (NL)	Chipknip: Деньги поступают с банковского счета и могут быть использованы как независимый электронный кошелек
Швейцария (CH)	Cash system: Деньги поступают с банковского счета и могут быть использованы как независимый электронный кошелек

### Б. Размер рынка

Примерное число провайдеров услуг в стране		Примерное количество счетов, открытых эмитентами карт	
≤ 3	> 3	≤ 1000	> 1000
DE, NL	CH		DE, NL, CH

### В. Доступ к деятельности

Регистрация/лицензирование		Надзор		Дополнительная информация
Да	Нет	Да	Нет	
DE, NL, CH		DE, NL, CH		

### Г. Положения о противодействии отмыванию денег и финансированию терроризма

Меры по надлежащей проверке клиента		Ведение бухгалтерских записей		Сообщение о подозрительных операциях		Другие правила и методики противодействия отмыванию денег		Лимит переводимой суммы, если есть	
Да	Нет	Да	Нет	Да	Нет	Да	Нет	≤ 500	> 500
CH, NL	DE <sup>48</sup>	CH, DE, NL		CH, DE, NL		CH, DE, NL		DE, NL, CH	

### Д. Случаи противодействия отмыванию денег и финансированию терроризма – выявление нелегальных операторов

Сведения об отмывании денег		Примеры правоохранительных действий		Нелегальные операторы	
Да	Нет	Да	Нет	Да	Нет
	DE, NL, CH		DE, NL, CH		DE, NL, CH

48. В Германии электронные кошельки могут быть законно выпущены только кредитными учреждениями, которые подлежат полному выполнению правил и методик противодействия отмыванию денег, с только одним исключением: из-за низкого лимита пополнения средств установление личности клиента/меры по надлежащей проверке клиента не являются необходимыми.

## Платежи через Интернет

### А. Описание нового метода платежей

Страны	Краткое описание нового метода платежей
Канада (CA)	Множество провайдеров, включая оффшорные
Бельгия (BE)	PayPal (который поднадзорен управлению по финансовым услугам Великобритании и предлагает услуги в Бельгии по лицензии для учреждений по работе с электронными деньгами, предоставленной Управлением по финансовым услугам Великобритании, которая дает возможность ведения деятельности на всей территории ЕС). Таким образом, он находится под надзором не Бельгии, а Великобритании.
Финляндия (FI)	“Digiraha”, описанная как «цифровой кошелек для платежей через Интернет». Нет подробной информации
Эстония (ET)	Fogott, PayPal, Netteller – нет подробной информации.
Новая Зеландия (NZ)	PayPal
Австрия (AT)	Развивающаяся серверная система для покупок в Интернете
Китай (CN)	Различные новые предприятия, работающие электронно, и сторонние посредники ведут собственную деятельность и оказывают посреднические услуги онлайн платежей.
Чешская Республика (CZ)	Internet shopping: пользователь имеет виртуальный счет на сайте и провайдер дебетует этот счет в момент покупки; предоставлена ограниченная информация
Франция (FR)	Neosurf: клиент обменивает денежные средства на скретч-карту (различные суммы), которая предоставляет код для оплаты в Интернете. Данная система работает во Франции, Бельгии и Швейцарии.
Германия (DE)	PayPal (который поднадзорен управлению по финансовым услугам Великобритании и предлагает услуги в Германии по лицензии для учреждений по работе с электронными деньгами, предоставленной Управлением по финансовым услугам Великобритании, которая дает возможность ведения деятельности на всей территории ЕС). Таким образом, он находится под надзором не Германии, а Великобритании.
Индонезия (ID)	Онлайн платеж для онлайн продавцов и денежных переводов от одного лица другому; данные услуги могут быть использованы для платежей по стране и международных переводов; эти методы платежей находятся только в разработке и пока не действуют.
Италия (IT)	1) Moneta On Line: Это скретч-карта, выпущенная банком для совершения покупок с низкой стоимостью через Интернет у продавцов, имеющих доступ к сети Visa circuit; личность пользователей не проверяется 2) BankPass Web: Это электронный кошелек для оплаты через Интернет
Нидерланды (NL)	Несколько провайдеров, включая PayPal
Испания (ES)	1) PayPal: в Испании, по видимому, введены более строгие положения о противодействии отмыванию денег и финансированию терроризма, чем в Германии и Нидерландах 2) Click & Buy: это расчетный механизм через Интернет для предприятий; он может быть использован для совершения покупок у продавцов в различных странах мира
Швейцария (CH)	Микроплатежи Click & Buy через Интернет у онлайн продавцов, за исключением эмитента карты
США (USA)	Есть несколько услуг онлайн платежей внутри страны, включая PayPal, и другие оффшорные провайдеры, которые имеют доступ на американский рынок



## Б. Размер рынка

Примерное число провайдеров услуг в стране		Примерное количество счетов, открытых эмитентами карт	
< 3	> 3	< 1000	> 1000
CZ, FR, DE, ID, ES (1), ES (2), CH, BE	NL, IT, USA, CA	CZ, ES (1)	NL, FR, DE, USA

## В. Доступ к деятельности

Регистрация/лицензирование		Надзор		Дополнительная информация
Да	Нет	Да	Нет	
AT, GE, ID, IT, NL, ES (1), CH, USA, BE	CN, ES (2), NZ, CA, ET	AT, DE, IT, ID, NL, ES (1), CH, CA (для банкоматов), USA, BE	CN, ES (2), NZ, ET	CN работает над регулированием; ET скоро будет применять Директиву ЕС об электронных деньгах

## Г. Положения о противодействии отмыванию денег и финансированию терроризма

Меры по надлежащей проверке клиента		Ведение бухгалтерских записей		Сообщение о подозрительных операциях		Другие правила и методики противодействия отмыванию денег		Лимит переводимой суммы, если есть	
Да	Нет	Да	Нет	Да	Нет	Да	Нет	≤ 500	> 500
AT, ID, IT, ES (1), CH, USA, NZ, CA, ET, DE, BE	CN, NL, ES (2)	AT, ID, USA, IT, ES (1), CH, USA, NZ, CA, ET, DE, BE, NL	CN, ES (2)	AT, ID, IT, ES (1), CH, USA, NZ, CA, ET, DE, BE, NL	CN, ES (2)	AT, ID, IT, ES (1), CH, USA, CA, DE, BE	CN, NL, ES (2), NZ, ET	AT, FR, CH, CA (имеет лимит, но сумма зависит от вида деятельности)	DE, IT, NL, ES (1), ES (2), CN

**Д. Случаи противодействия отмыванию денег и финансированию терроризма – выявление нелегальных операторов**

Сведения об отмывании денег		Примеры правоохранительных действий		Нелегальные операторы	
Да	Нет	Да	Нет	Да	Нет
CN, ET, CA, USA	AT, FR, DE, ID, IT, NL, ES (1), ES (2), CH, NZ, BE	USA, ET, CA	AT, CN, FR, DE, ID, IT, NL, ES (1), ES (2), CH, NZ, BE	CN, ID, USA	AT, FR, DE, IT, NL, ES (1), ES (2), CH, BE

**Мобильные платежи**

**А. Описание нового метода платежей**

Страны	Краткое описание нового метода платежей
Франция (FR)	Телефонными компаниями предлагаются услуги с предварительной оплатой и оплатой по факту
Бельгия (BE)	Мобильные платежи (только через перезагрузку SIM-карты) используются в Бельгии в уменьшенном масштабе, по меньшей мере, уже 2 года
Литва (LT)	Предлагается использовать мобильный телефон для оплаты в ограниченных целях (парковка, билеты на концерты и другие мероприятия) с предоплаченного счета или счета мобильного телефона; не предоставлено подробной информации
Германия (DE)	<ol style="list-style-type: none"> <li>1) Standy является системой предоплаченных мобильных платежей, которая позволяет делать переводы от одного лица к другому и платить в терминалах оплаты, средства переводятся с банковского счета</li> <li>2) Предоплаченные скретч-карты для оплаты с мобильного телефона</li> </ol>
Нидерланды (NL)	Услуги платежей телефонной компании для платежей, использующих мобильный телефон (например, для покупки ринг-тонов)

**Б. Размер рынка**

Примерное число провайдеров услуг в стране		Примерное количество счетов, открытых эмитентами карт	
≤ 3	> 3	≤ 1000	> 1000
	FR, DE, NL		FR, DE, NL

**В. Доступ к деятельности**

Регистрация/лицензирование		Надзор		Дополнительная информация
Да	Нет	Да	Нет	
DE (Л)	NL	DE	NL	

**Г. Положения о противодействии отмыванию денег и финансированию терроризма**

Меры по надлежащей проверке клиента		Ведение бухгалтерских записей		Сообщение о подозрительных операциях		Другие правила и методики противодействия отмыванию денег		Лимит переводимой суммы, если есть	
Да	Нет	Да	Нет	Да	Нет	Да	Нет	≤ 500	> 500
	NL, DE, BE	DE, BE (но это не требуется законом)	NL	DE	NL, BE	DE	NL, BE	DE, NL, BE (зафиксировано телефонным оператором)	

**Д. Случаи противодействия отмыванию денег и финансированию терроризма – выявление нелегальных операторов**

Сведения об отмывании денег		Примеры правоохранных действий		Нелегальные операторы	
Да	Нет	Да	Нет	Да	Нет
	FR, DE, BE		FR, DE		FR, DE

**Обезличенные драгоценные металлы****А. Описание нового метода платежей**

Страны	Краткое описание нового метода платежей
Эстония (ET)	“Icegold”. Не предоставлено подробной информации
США (USA)	Много дилеров обезличенных драгоценных металлов доступно онлайн. Пополнение счетов и снятие наличных средств осуществляется через «службу обмена». Каждая служба обмена устанавливает собственные правила того, как она будет получать и выдавать денежные средства. Одни могут принимать только переводы от банков и со счетов кредитной карты, тогда как другие принимают наличные деньги и платежные поручения.

## Б. Размер рынка

Примерное число провайдеров услуг в стране		Примерное количество счетов, открытых эмитентами карт	
< 3	> 3	< 1000	> 1000
ЕТ	USA		USA

## В. Доступ к деятельности

Регистрация/лицензирование		Надзор		Дополнительная информация
Да	Нет	Да	Нет	
USA		USA		В Соединенных Штатах организации, выполняющие перевод денег, являются учреждениями банковских услуг, которые необходимо регистрировать в Управлении финансовой разведки (Сети по расследованию финансовых преступлений). Они обязаны предоставлять отчет о противодействии отмыванию денег и выполнять требования ведения бухгалтерских записей, также часто требуется наличие лицензии государственного уровня. Факт соответствия системы онлайн платежей или дилера обезличенных драгоценных металлов «учреждению банковских услуг» определяется, согласно соответствующим нормативно-правовым актам, его местоположением и методами, которые он использует для участия в транзакциях или их проведении. Многие системы онлайн платежей расположены за пределами США и не подлежат законам юрисдикции США

## Г. Положения о противодействии отмыванию денег и финансированию терроризма

Меры по надлежащей проверке клиента		Ведение бухгалтерских записей		Сообщение о подозрительных операциях		Другие правила и методики противодействия отмыванию денег		Лимит переводимой суммы, если есть	
Да	Нет	Да	Нет	Да	Нет	Да	Нет	≤ 500	> 500
	USA	USA			USA		USA	USA: установлено каждым эмитентом	USA: установлено каждым эмитентом

## Д. Случаи противодействия отмыванию денег и финансированию терроризма – выявление нелегальных операторов

Сведения об отмывании денег		Примеры правоохранительных действий		Нелегальные операторы	
Да	Нет	Да	Нет	Да	Нет
USA		USA		USA: оффшорные	