ФАТФ

Международная группа разработки финансовых мер борьбы с отмыванием денег

УЯЗВИМЫЕ МЕСТА КОММЕРЧЕСКИХ ИНТЕРНЕТ-САЙТОВ И СИСТЕМ ИНТЕРНЕТ-ПЛАТЕЖЕЙ, ПОЗВОЛЯЮЩИЕ ИСПОЛЬЗОВАТЬ ИХ ДЛЯ ОТМЫВАНИЯ ДЕНЕГ И ФИНАНСИРОВАНИЯ ТЕРРОРИЗМА

Неофициальный перевод

18 июня 2008 года

ОГЛАВЛЕНИЕ

ОСНОВНЫЕ ПОЛОЖЕНИЯ

1. Преступные элементы успешно находят новые каналы для финансирования терроризма и отмывания денежных средств, получаемых ими в результате незаконной деятельности. По мере распространения Интернета, выясняется, что коммерческим Интернет-сайтам и системам Интернет-платежей присущи многие риски и что они имеют множество уязвимых мест, позволяющих преступным организациям и террористическим группировкам использовать их в своих целях.

2. В настоящем исследовании представлен анализ рисков, связанных с отмыванием денег и финансированием терроризма (ОД/ФТ) с помощью коммерческих Интернет-сайтов и систем Интернет-платежей, при этом основное внимание уделено сайтам-посредникам в продажах от потребителя к потребителю, являющимся наиболее уязвимыми в плане таких злоупотреблений благодаря своей популярности, доступности (для широкой публики) и большого объема трансграничных торговых сделок. Кроме того, в рамках такого анализа на конкретных примерах описываются способы использования сайтов-посредников в продажах от потребителя к потребителю для ОД/ФТ.

3. В исследовании выделены следующие уязвимые места коммерческих Интернет-сайтов и систем Интернет-платежей: заочная регистрация, возможная анонимность пользователей, скорость совершения сделок, меньший объем участия человека, отсутствие государственных границ, ограниченная подсудность, сложность мониторинга и обнаружения подозрительных операций традиционными финансовыми учреждениями, которые могут оказаться не столь эффективными в тех случаях, когда сделка осуществляется с участием поставщика услуг Интернет-платежей.

4. В исследовании говорится о том, что некоторые риски ОД/ФТ, связанные с отмыванием денег с помощью торговых операций[1] и заочными коммерческими и финансовыми сделками, также присущи коммерческим Интернет-сайтам и системам Интернет-платежей. Финансовые операции, осуществляемые через банковский счет или кредитную карту (два наиболее распространенные метода Интернет-платежей) предусматривают удостоверение личности клиента, сохранение информации об операциях и предоставление отчетности. Риск, связанный с операциями на небольшие суммы, далеко не всегда бывает небольшим, поэтому для снижения риска к таким операциям должны применяться регулятивные меры, которые используются в финансовом секторе. В той части исследования, которая относится к рискам, связанным с заочной регистрацией и анонимностью пользователей, говорится о необходимости поиска решений, обеспечивающих удостоверение личности в режиме онлайн (например, с помощью электронных карт-удостоверений личности, использующихся в некоторых странах), позволяющих снизить риски преступной деятельности, которым подвержены поставщики услуг Интернет-сайтов и поставщики услуг Интернет-платежей. В исследовании также говорится о том, что если поставщики услуг Интернет-платежей обеспечат надлежащий мониторинг финансовых операций своих клиентов, следя за отклонениями от сложившейся модели поведения клиента и адекватно на них реагируя, то недостаток личного контакта, имеющийся в начале взаимоотношений с поставщиком услуг коммерческого Интернет-сайта и поставщиком услуг Интернет-платежей, может перестать быть проблемой. Лица, осуществляющие торговые операции через

[1] ФАТФ (2006b)

Интернет, и лица, осуществляющие такие торговые операции традиционными методами, должны иметь сСПОставимые объемы обязательств по ПОД/ФТ (борьба с отмыванием денег/борьба с финансированием терроризма).

5. Также важно добиться того, чтобы у поставщиков услуг коммерческих Интернет-сайтов и у поставщиков услуг Интернет-платежей из разных стран, противодействующих ОД/ФТ, не возникало сложностей из-за несогласованности законов о защите частной жизни, ограничивающих объемы информации о клиентах, которой могут обмениваться поставщики услуг по операциям, могущим быть связанными с ОД/ФТ.

6. Требования по выявлению операций, связанных с финансированием терроризма (в основном, с помощью сопоставления имен клиентов с именами, предоставленными компетентными органами), предъявляются ко всем системам Интернет-платежей в равной мере, при этом поставщики услуг Интернет-платежей, в своих сообщениях о подозрительных операциях (СПО), предоставляемых в рамках содействия борьбе с финансированием терроризма, не всегда обязаны указывать, что та или иная деятельность, по их мнению, связана с финансированием терроризма. Важно сообщать о любой подозрительной деятельности независимо от ее типа. Некоторые поставщики услуг Интернет-платежей начали внедрять и использовать системы обнаружения, мониторинга и анализа подозрительных операций, в том числе операций с небольшими суммами денег.

7. Говоря о подходе к борьбе с ОД/ФТ, основанном на оценке рисков, следует упомянуть Рекомендации ФАТФ (июнь 2007 года), в которых сказано следующее: «При использовании подхода на основе оценки рисков компетентные органы и финансовые учреждения смогут обеспечить соразмерность мер, предпринимаемых для профилактики или снижения объемов отмывания денег и финансирования терроризма, тем рискам, которые были определены. Это позволит распределять имеющиеся ресурсы наиболее эффективным способом. Принцип наиболее эффективного распределения ресурсов предполагает распределение на основе приоритетности – наибольшее внимание должно уделяться наибольшим рискам». Применяя данный принцип к операциям, осуществляемым через Интернет, представители частного сектора будут рассматривать мелкие платежи, совершаемые через финансовые учреждения или счета кредитных карт (что предполагает идентификацию и проверку личности клиента, а также учет и отчетность) в качестве операций, риск по которым будет меньше, чем по операциям, осуществляемым с помощью поставщиков услуг, не имеющих обязательств по борьбе с отмыванием денег и с финансированием терроризма (ПОД/ФТ).

8. Риск мошенничества и продаж незаконных товаров являются для поставщиков услуг коммерческих Интернет-сайтов и поставщиков услуг Интернет-платежей еще одним поводом для беспокойства, заставляющим их принимать меры для защиты передаваемой ими информации, имеющихся у них Интернет-сайтов и систем Интернет-платежей. В некоторых странах никаких официальных требований, связанных с обнаружением и борьбой с ОД/ФТ, поставщикам услуг коммерческих Интернет-сайтов не предъявляется – для этого используются рыночные стимулы.

9. Некоторые поставщики услуг коммерческих Интернет-сайтов и поставщики услуг Интернет-платежей, знающие о рисках, связанных с возможностью использования имеющихся у них ресурсов для незаконной деятельности, открыли специальные подразделения, занимающиеся мониторингом и анализом операций своих клиентов на основе подхода, предполагающего оценку рисков. Некоторые поставщики услуг Интернет-платежей, в дополнение к использующимся ими средствам мониторинга случаев мошенничества, также внедрили механизмы ПОД/ФТ. Использование

передовых методов работы (таких как, например, методы надлежащей проверки клиентов, мониторинг операций, отказ от анонимных платежей (например, платежей наличными), введение ограничений на размер операций, ведение учетной документации по осуществляемым операциям, уведомление компетентных органов о крупных или подозрительных операциях) также может оказаться эффективным средством противодействия ОД/ФТ.

10. Сотрудничество между поставщиками услуг коммерческих Интернет-сайтов и поставщиками услуг Интернет-платежей с целью обмена информацией о коммерческих операциях, являющихся причиной финансовых сделок, позволяет снизить риски ОД/ФТ и мошенничества. Правовое стимулирование обмена такой информацией может оказаться весьма полезным.

11. В настоящем отчете сделан следующий вывод: до тех пор, пока представители данного сектора и соответствующие компетентные органы знают и понимают, какие составляющие коммерческих Интернет-сайтов и систем Интернет-платежей являются потенциально уязвимыми, и какие меры (с учетом возможных рисков) необходимо принять для обеспечения идентификации клиента, ведения учетной документации и предоставления необходимой отчетности, риски, связанные с операциям через Интернет, не обязательно будут превышать риски, связанные с традиционными (несетевыми) финансовыми операциями.

12. Составители отчета полагают, что, несмотря на то, что благодаря усилиям регулятивных органов и профессиональных объединений уровень осведомленности об ОД/ФТ среди ключевых игроков в сфере Интернет-бизнеса постоянно повышается, необходимо принимать дальнейшие меры по повышению уровня осведомленности, особенно в отношении того, что касается механизмов борьбы с ОД/ФТ.

13. В настоящем исследовании определены области деятельности, которые в дальнейшем могут стать ключевыми для усовершенствования механизмов снижения соответствующих рисков ОД/ФТ, а именно: *i)* улучшение взаимопонимания между государственными органами и представителями частного сектора в части снижения рисков отмывания денег/финансирования терроризма через Интернет и разработка рекомендаций по внедрению механизмов обнаружения подозрительных операций; *ii)* принятие мер к тому, чтобы обычные финансовые учреждения осознали, что они играют важнейшую роль в обнаружении и мониторинге подозрительных финансовых операций, даже если платежи совершаются через поставщика услуг Интернет-платежей; *iii)* учитывая глобальный характер коммерческих Интернет-сайтов и систем Интернет-платежей, международное сотрудничество является залогом успешной борьбы с ОД и ФТ; *iv)* определение иных, новых способов, с помощью которых подразделения финансовой разведки (ПФР) смогут увеличить объемы обмена информацией и данными об использовании коммерческих Интернет-сайтов и систем Интернет-платежей в преступных целях. И наконец, учитывая глобальный характер сети Интернет, сложно определить, в каком месте или стране находится регулятивный орган, имеющий право регламентировать деятельность поставщиков услуг Интернет-платежей, и каким образом осуществлять принудительное обеспечение правопорядка в случае возможных нарушений. Поставщики услуг Интернет-платежей, осуществляющие свою деятельность в глобальном масштабе, расположены и имеют лицензии, выданные в разных странах и регионах. Поэтому важно, чтобы во всех странах принимались схожие законы, предусматривающие обязательную идентификацию клиента, надлежащую проверку клиента, ведение учетной документации и предоставление отчетности – в противном случае некоторые поставщики услуг Интернет-платежей могут выбрать страну с самым

несовершенным законодательством или страну, в которой такая деятельность вообще не регламентируется.

ВВЕДЕНИЕ

14. В арсенале преступных элементов имеется большое количество средств, используемых ими для финансирования терроризма и отмывания доходов, получаемых в результате незаконной деятельности; среди них – использование традиционной финансовой системы, перевозка наличных курьерами и перевод средств в безналичном виде (перевод стоимости активов) с помощью торговых операций.

15. В течение многих лет Целевая группа по финансовым мероприятиям в области отмывания денег (ФАТФ) тщательно изучала такие механизмы и их разновидности. Следует надеяться, что накопленные знания позволяют как частному, так и государственному сектору повысить свою бдительность и наработать необходимый опыт, затрудняющий финансирование терроризма и отмывание доходов, получаемых преступниками в результате незаконной деятельности.

16. Несмотря на вышесказанное, преступные элементы успешно находят новые каналы для финансирования терроризма и отмывания денежных средств, получаемых ими в результате незаконной деятельности. А коммерческие Интернет-сайты и системы Интернет-платежей имеют множество уязвимых мест, которыми преступные организации и финансисты террористов могут воспользоваться для достижения своих целей.

17. Учитывая то, что торговля через Интернет может использоваться для отмывания денежных средств и финансирования терроризма, все чаще стали раздаваться заявления о необходимости регулирования государством электронных методов торговли, в частности, работы систем Интернет-платежей.

18. Областью настоящего исследования являются коммерческие Интернет-сайты и системы Интернет-платежей, при этом основное внимание уделено коммерческим сайтам-посредникам в продажах от потребителя к потребителю. Главная задача настоящего исследования – сделать так, чтобы представители частного и государственного сектора стали лучше понимать риски ОД/ФТ, связанные с использованием коммерческих Интернет-сайтов и систем Интернет-платежей, и повысить, в глобальном масштабе, уровень осведомленности о методах, использующихся для отмывания незаконных доходов и финансирования терроризма. Значительная часть данной работы основывается на результатах специальных целевых исследований и анализа рисков ОД/ФТ, связанных с использованием коммерческих Интернет-сайтов и систем Интернет-платежей.

19. Авторы настоящего исследования не ставили себе целью заменить или продублировать отчет ФАТФ «Новые способы платежей», однако его можно использовать в качестве дополнения к указанному отчету.

20. В написании настоящего исследования приняли участие представители десяти стран: Австралии, Бельгии (руководители коллектива авторов), Китая, Гонконга, Финляндии, Франции, Люксембурга, Нидерландов, США и Великобритании. Представители нескольких стран сделали презентации во время семинара, проведенного в Бангкоке (Таиланд) 28-30 ноября 2007 года и посвященного исследованию типологий ФАТФ. Авторы отчета ответили на вопросы предложенной им анкеты. В работе семинара также приняли участие некоторые другие страны, которые также внесли свою лепту в данное исследование: Бангладеш, Тайбэй (Китай), Фиджи, Германия, Индия, Япония, Новая Зеландия, Филиппины, ЮАР, Россия, Испания, Швеция, Швейцария и Таиланд.

21. При написании настоящего исследования его авторы также использовали на опыт и сведения, предоставленные представителями частного сектора. Сотрудники компаний eBay и PayPal посетили семинар и приняли участие в исследовании. Британская компания PrePay Technologies и европейская торговая ассоциация Electronic Money Association (EMA) со штаб-квартирой в Лондоне, представляющая группу из 33 эмитентов электронных денег и поставщиков услуг Интернет-платежей, также приняли участие в данном проекте и внесли свой вклад в исследование.

22. Представители частного сектора также высказали свое мнение по вопросам, связанным с настоящим отчетом, и выводами, сделанными в рамках проведенного исследования. Руководители коллектива авторов организовали встречу вышеупомянутых представителей частного сектора с некоторыми авторами данного исследования, проведенную 4 апреля 2008 года в Брюсселе. Представители частного сектора, принявшие участие в исследовании, получили по экземпляру отчета и возможность высказать свои замечания. Авторы учли замечания, которые, по мнению авторов, оказались полезными.

23. И наконец, риски и уязвимые места, указанные в настоящем исследовании, послужат полезным дополнением к работе ФАТФ «Стратегии анализа опасности отмывания денег».

ХАРАКТЕРИСТИКИ КОММЕРЧЕСКИХ ИНТЕРНЕТ-САЙТОВ И СИСТЕМ ИНТЕРНЕТ-ПЛАТЕЖЕЙ

Определения

24. В настоящем разделе дано функциональное определение коммерческих Интернет-сайтов различных классов/типов. Такие коммерческие Интернет-сайты можно разделить на пять категорий:[2]

- Сайты-посредники в продажах от потребителя к потребителю, т.е. сайты, при посредничестве которых одни частные лица совершают продажи другим частным лицам;
- Сайты-посредники в продажах от компании к потребителю, т.е. сайты, при посредничестве которых многие предприятия продают свои продукты потребителям на виртуальном рынке;
- Сайты, работающие по системе «потребитель для потребителя», но не являющиеся посредниками в продажах (электронные доски объявлений, сайты тематических объявлений), т.е. сайты, с помощью которых клиенты могут рекламировать, но не продавать свои товары;
- Сайты прямых продаж от компании к потребителю, собственные сайты предприятий, позволяющие им продавать свои продукты потребителям напрямую, без посредничества;
- Сайты прямых продаж от компании к компании, собственные сайты предприятий, позволяющие им продавать свои продукты другим предприятиям напрямую, без посредничества.

25. В настоящем исследовании основное внимание уделено коммерческие сайтам, относящимся к первой категории. Сайты-посредники в продажах от потребителя к потребителю весьма популярны, открыты для всех и облегчают осуществление трансграничных торговых операций. Именно поэтому они и становятся легкой мишенью преступных элементов. Коммерческие сайты такого типа позволяют осуществить с их помощью операции между частными лицами, в отличие от сайтов для простого обмена контактной информацией с последующим совершением сделок вне сети.

26. Интернет-сайты тематических объявлений, электронные доски объявлений и сайты социальных сетей часто позволяют продавцам предлагать с их помощью имеющиеся продукты на продажу, с последующим совершением сделок вне сети. Хотя такие сайты и облегчают встречу продавца с покупателем и общение между ними, какой-либо значительной роли в конечной продаже или окончательном расчете они не играют. Соответственно, такие сайты, работающие по системе «потребитель для потребителя», но не являющиеся посредниками при продажах, в большинстве случаев не позволяют отслеживать какие-либо аспекты сделок после встречи покупателя с продавцом.

27. Сайты-посредники, напротив, играют активную роль в заключении основных сделок: с их помощью определяется цена продажи на Интернет-аукционе, осуществляется идентификация (в той или иной форме) продавца и покупателя (в том числе и с помощью отзывов других клиентов), облегчается расчет за сделку (например, за счет предоставления услуг эскроу или аналогичных посреднических услуг). Несмотря на то, что сайты, не являющиеся посредниками в совершении

[2] Стоит заметить, что некоторые коммерческие Интернет-сайты относятся к нескольким категориям.

продаж, также могут использоваться в преступных целях (например, в мошеннических целях), авторы настоящего исследования сосредоточили свое внимание на сайтах-посредниках, играющих активную роль в осуществлении операций, которые могут использоваться для ОД/ФТ.

28. Сайты-посредники в продажах от компании к потребителю также подвержены рискам ОД/ФТ. В течение дня сайт может использоваться, например, для продажи одежды и казаться поставщику услуг Интернет-платежей вполне законным, однако ночью, в течение нескольких часов, адрес сайта (URL) может использоваться для продажи детской порнографии. В некоторых случаях компании могут разрешать продавцам-третьим сторонам продавать свои товары и услуги через собственные онлайн-порталы, имеющиеся у таких компаний.

29. Коммерческие Интернет-сайты и системы Интернет-платежей могут использоваться для совершения незаконных операций, включая продажу запрещенных наркотических средств, оружия, огнестрельного оружия, контрафактных товаров и детской порнографии, а также для мошенничества. Кроме того, Интернет-платежи могут использоваться для отмывания прибылей, полученных в результате такой преступной деятельности.

30. В настоящем отчете термин «система Интернет-платежей» используется для общего обозначения Интернет-компаний, предоставляющей клиентам услуги по осуществлению финансовых операций. В большинстве случаев оказание таких услуг через систему Интернет-платежей осуществляется через небанковские финансовые учреждения, которые в некоторых случаях могут контролироваться регулятивными органами, а в некоторых случаях могут работать вне их контроля – это зависит от места оказания таких услуг клиентам и принятых там законов. Системы Интернет-платежей привлекают клиентов своим удобством и тем, что они представляют собой альтернативу платежам через банковский счет или кредитную карту, которые могут быть не у всех.

31. Учитывая риски, которым подвергаются поставщики услуг коммерческих Интернет-сайтов и поставщики услуг Интернет-платежей, авторы настоящего отчета считают необходимым четко разграничить деловые операции, осуществляемые с помощью коммерческих Интернет-сайтов, и платежи, связанные с такими деловыми операциями (услуги Интернет-платежей) – даже в тех случаях, когда сайты предлагают как услуги по осуществлению коммерческих операций, так услуги по оплате таких операций.

Основные характеристики

32. В настоящем разделе изложены основные характеристики изученных коммерческих Интернет-сайтов, а также основные характеристики систем Интернет-платежей, связанных с такими сайтами.

Коммерческие Интернет-сайты

33. Как правило, коммерческие Интернет-сайты имеют все или несколько из перечисленных ниже характеристик:[3]

[3] Некоторые из этих характеристик также являются характеристиками сети Интернет и поставщиков услуг Интернет-платежей.

- Наличие обычного подключения к Интернету достаточно для создания на коммерческом сайте учетной записи пользователя и покупки/продажи товаров;
- Теоретически на сайт можно зайти в любой точке земного шара;
- Клиент может зайти на сайт с помощью собственного подключения к Интернету, с помощью подключения к Интернету третьей стороны (например, в Интернет-кафе, в телефонных переговорных пунктах с доступом к Интернет), или через точку доступа, которая на клиента не зарегистрирована;
- Клиент может зарегистрироваться в одной стране, а выходить в Интернет – в другой;
- Регистрация происходит очень просто и очень быстро (в течение нескольких минут);
- Регистрация делается заочно;
- Количество информации, которую необходимо указать для регистрации, невелико;
- В некоторых случаях идентификация клиента вообще не требуется;
- В качестве контактных данных клиент может использовать анонимные адреса электронной почты;
- Торговые операции осуществляются очень быстро. Продавец уведомляется о продаже выставленного им товара с помощью сообщения на электронную почту;
- Клиенты имеют доступ к большому количеству разнообразных товаров (от самых дешевых до очень дорогих), выставленных на продажу на множестве коммерческих Интернет-сайтов, зарегистрированных в разных странах мира;
- Товары продаются как по фиксированным, так и по изменяющимся ценам. Например, на онлайновых аукционах цена может устанавливаться как самим продавцом, так и покупателями, в результате чего определить действительную рыночную стоимость продаваемого товара бывает достаточно сложно;
- С помощью коммерческих Интернет-сайтов можно совершать продажи и расчеты, однако доставкой товара занимаются сами покупатели продавцы. Зачастую единственным свидетельством непоставки товара является жалоба покупателя.

34. Некоторые поставщики услуг Интернет-сайтов и поставщики услуг Интернет-платежей при идентификации клиентов используют подход, основанный на оценке рисков. Если риски, связанные с клиентом и сделкой, высоки, используются дополнительные методы проверки (упрощенный порядок надлежащей проверки клиентов заменяется на расширенный). Механизмы проверки можно адаптировать к использованию в стране регистрации и изменять с учетом преступных схем, использующихся для того, чтобы обойти процедуру идентификации и проверки. Представители частного сектора, принявшие участие в исследовании, указали, что преступники действительно пытаются обойти указанные процедуры, и хотя ни один из использующихся методов сам по себе не является стопроцентно безотказным, в совокупности такие методы позволяют эффективно снижать существующие риски.

Системы Интернет-платежей

35. Точно так же, как и в любых других видах онлайнового бизнеса, структура и принципы работы различных систем Интернет-платежей могут очень сильно отличаться. Тем не менее, большинство таких систем объединяет то, что для осуществления сделки клиенты (или пользователи) должны в них зарегистрироваться. Регистрация в большинстве случаев предполагает сбор и проверку идентифицирующей информации и/или его контактной информации.

Например, для регистрации в системе Интернет-платежей пользователь должен указать адрес своей электронной почты, номер телефона, фактический адрес проживания, а также информацию, необходимую для создания пароля и идентификатора пользователя для последующей регистрации в системе Интернет-платежей.[4] В зависимости от методов работы, принятых в той или иной системе Интернет-платежей, типа оказываемых услуг и систем управления рисками, использования которых требуют компетентные органы, под юрисдикцию которых попадает система, от пользователя может потребоваться предоставление иной информации. Собранная информация затем проверяется различными способами – начиная с проверки предоставленных бумажных копий удостоверений личности и заканчивая использованием средств, предоставленных третьими сторонами, позволяющих проверить личность пользователя в режиме онлайн.

36. До того, как пользователь той или иной системы Интернет-платежей сможет перечислить с ее помощью необходимые средства, он, как правило, должен сначала их внести. Внесение денежных средств для последующего перевода через систему Интернет-платежей может осуществляться с помощью перечисления таких средств на «счет», с которого они будут в дальнейшем списаны для совершения необходимых операций или переводов, или внесения таких средств в систему Интернет-платежей в размере, равном сумме перечисления. Пользователь может внести необходимую сумму несколькими способами (количество которых зависит от количества операций, предусмотренных той или иной системой Интернет-платежей), не ограничивающихся использованием кредитной карты или личного банковского счета. Для недопущения мошенничества или злоупотребления системой в преступных целях поставщик услуг Интернет-платежей может проверить, имеет ли пользователь право на использование некоторых способов внесения средств – например, с помощью кредитной карты или банковского счета. После проверки пользователь получает возможность выполнить необходимые операции в системе Интернет-платежей.

37. Необходимо отметить, что во многих случаях без взаимодействия систем Интернет-платежей с традиционными банковскими и финансовыми системами перевод денежных средств невозможен. Например, системы Интернет-платежей, средства в которые можно вносить с помощью кредитных карт крупнейших эмитентов, для принятия платежей по таким кредитным картам должны иметь транзитный счет в банке. Средства пользователей, поступающие в систему Интернет-платежей через такой транзитный счет, проходят по финансовым каналам эмитентов таких кредитных карт. И только после этот средства перечисляются в соответствии с указаниями пользователя системы Интернет-платежей. По такому же принципу работают и системы Интернет-платежей, принимающие средства пользователей через их личные банковские счета. Следует еще раз обратить внимание на то, что в большинстве случаев системы Интернет-платежей должны иметь текущий счет в банке, на который могут быть переведены средства с личного банковского счета пользователя. Такие переводы осуществляются, как правило, через системы клиринговых расчетов.

38. Системы Интернет-платежей могут предусматривать различные способы приема платежей от пользователей, покупающих товары и/или услуги через коммерческие

---

[4] Обратите внимание, что в момент регистрации в той или иной системе Интернет-платежей требования об указании индивидуального идентификационного номера (например, номера социального страхования, номера паспорта и т.д.) или даты рождения к пользователю могут и не предъявляться. В некоторых системах Интернет-платежей получение от пользователя такой информации вообще не предусмотрено.

Интернет-сайты (такие сделки принято называть сделками C2B («покупка потребителя у компании»)), и от предприятий, приобретающих товары и/или услуги через коммерческие Интернет-сайты у других предприятий (сделка B2B («покупка компании у компании»)).[5] Однако опасения (из-за наличия уязвимых мест, позволяющих заниматься ОД и ФТ, взывают сделки P2P («покупка частного лица у частного лица»), т.е. сделки между двумя лицами, одно из которых что-либо покупает у другого через коммерческий сайт-посредник.

39. Другие способы внесения средств, которые могут предлагаться пользователю некоторыми коммерческими Интернет-сайтами напрямую, без участия поставщика услуг Интернет-платежей, или запрашиваться потребителями, продающими свои товары на коммерческих P2P Интернет-сайтах, перечислены ниже:

- Кредитные карты;
- Карты с заранее внесенной на них суммой денег (которые в некоторых странах выдаются на условиях анонимности, без указания имени владельца)[6];
- Банковский перевод (на банковский счет коммерческого Интернет-сайта для дальнейшего перевода продавцу);
- Банковский перевод на банковский счет продавца (с сообщением о том, что данный перевод делается для оплаты покупки по Интернету);
- Подарочные кредитные карты или подарочные чеки (без указания имени и с правом передачи);
- Чеки (которые в некоторых странах отправляются на адрес коммерческого Интернет-сайта, а в некоторых – клиентам);
- Банковские чеки;
- Почтовые/денежные переводы на имя продавца[7];
- Перевод денежных средств на имя продавца;
- На некоторых коммерческих Интернет-сайтах принимаются наличные.

Оплата наличными возможна непосредственно между покупателем и продавцом, однако считается, что этот способ оплаты распространен не очень широко.

40. В системе Интернет-платежей сделки совершаются очень быстро и в электронном виде.

41. Политика, методы работы и способы платежа, предлагаемые транснациональными игроками (коммерческие Интернет-сайты и системы Интернет-платежей, работающие сразу в нескольких странах) своим клиентам, могут различаться в зависимости от местонахождения компании-учредителя, местного отделения или Интернет-сайта.

---

[5] Некоторые поставщики услуг Интернет-сайтов и поставщики услуг Интернет-платежей предлагают своим клиентам более безопасный способ платежа, совершаемый с помощью доверенного лица-третьей стороны. Используя такое доверенное лицо (за вознаграждение в виде комиссионных), покупатель знает, что средства за покупку, сделанную по Интернету, будут переданы в распоряжение продавца только после того, как купленный товар будет доставлен покупателю, и он удостоверится в том, что товар соответствует своему описанию на коммерческом Интернет-сайте.

[6] В некоторых странах банки (в тех случаях, когда они не хотят предоставлять свои клиентам возможность использования кредита, например, безработным и лицам без постоянного дохода) предлагают банковские карты с заранее внесенной на них сумой денег (предоплаченные карты).

[7] Некоторые коммерческие Интернет-сайты рекомендуют своим пользователям проявлять осторожность в тех случаях, когда при покупке товара через Интернет для его оплаты они должны сделать почтовый перевод – как показывает опыт, почтовый перевод как средство оплаты часто используется в мошеннических целях (например, при продаже товаров, которые не будут поставлены).

ПРИМЕРЫ ОТМЫВАНИЯ ДЕНЕГ И ФИНАНСИРОВАНИЯ ТЕРРОРИЗМА

42. В этом разделе сделан обзор примеров отмывания денег и финансирования терроризма с использованием коммерческих Интернет-сайтов и систем Интернет-платежей. Раздел состоит из двух частей: *i)* изучение случаев, имевших место в реальной жизни; *ii)* потенциально уязвимые места. Потенциально уязвимые места рассмотрены для того, чтобы дать правоохранительным органам, управлениям финансовой разведки и представителям частного сектора представление о тех мерах, которые должны быть приняты с их стороны.

Случаи, имевшие место в реальной жизни

43. В этой части настоящего раздела описаны различные способы использования коммерческих Интернет-сайтов и систем Интернет-платежей для ОД/ФТ на примере случаев, имевших место в реальной жизни.

44. Для продажи/покупки незаконных продуктов – таких как наркотики или контрафактные товары – могут использоваться коммерческие Интернет-сайты и системы Интернет-платежей. Иногда проданные/купленные товары, являющиеся товарами двойного назначения или составными частями других товаров, сами по себе незаконными не являются, однако относятся к категории товаров, на основе которых изготовляются взрывчатые вещества, оружие и иная продукция, контролируемая государством. Такие товары часто отправляются по почте и через службы экспресс-доставки.

45. Коммерческие Интернет-сайты и системы Интернет-платежей могут использоваться для совершения незаконных сделок, мошеннических сделок, для осуществления незаконной деятельности, деятельности за пределами компетенции ФАТФ. Тем не менее, проведенные целевые исследования свидетельствуют о том, что коммерческие Интернет-сайты и системы Интернет-платежей используются, среди прочего, для сбора доходов, полученных в результате такой незаконной деятельности, а также для ОД и ФТ (за счет сокрытия полученных средств: деньги переводятся на счет в банке, находящемся в стране пребывания преступников (или заграницей), используются для других покупок через коммерческие Интернет-сайты и т.д.).

Пример использования коммерческих Интернет-сайтов и систем Интернет-платежей для продажи наркотиков

Поставщик услуг Интернет-платежей сделал несколько небольших денежных переводов (всего на 4700 евро) на счет физического лица в бельгийском банке. Данное лицо находилось под следствием в другой европейской стране по делу о продаже легких наркотиков. Правоохранительные органы подтвердили, что данное лицо занималось продажей легких наркотиков через коммерческий Интернет-сайт.

Источник: Бельгия

46. В рассмотренном случае поставщик услуг Интернет-платежей использовался для получения преступником доходов от незаконной деятельности; В дальнейшем преступником мог бы использовать его для совершения преступных действий и сделок. Преступник мог использовать доходы от незаконной деятельности на покупку новых наркотиков и продолжать заниматься незаконной деятельностью через коммерческий Интернет-сайт.

Пример использования коммерческих Интернет-сайтов и систем Интернет-платежей для продажи контрафактных товаров

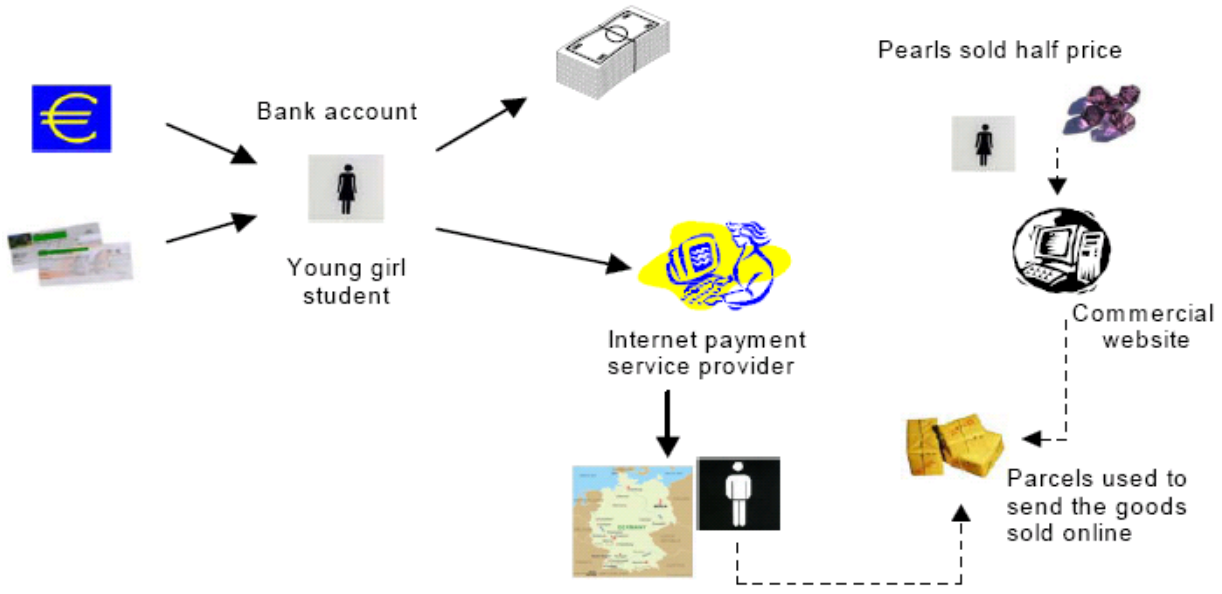
Банк сообщил о подозрительных операциях, осуществляемых молодой девушкой. С января по август 2005 года (в течение восьми месяцев) на банковский счет этой девушки, студентки, поступали денежные переводы и чеки от физических лиц со всех уголков Франции. Чеки выписывались на небольшие суммы (от 20 до 40 евро). Расходные операции, совершаемые этой девушкой, включали в себя снятие наличных денег со счета и их перевод с пометкой «оплата счетов поставщика услуг Интернет-платежей». Общая сумма покупок составила 6340 евро, а количество платежных операций – 43.

В сентябре 2005 год она начала пользоваться кредитной картой, и банку стало сложнее понимать характер осуществляемых ею операций. Теперь банку была известна только ежемесячно регистрируемая общая сумма платежей, поступающих на ее банковский счет.

В результате проведенного расследования выяснилось, что с сентября 2005 по март 2006 года (в течение восьми месяцев) она сделала 63 покупки онлайн на сумму 39282,24 евро.

Молодая особа продавала поддельные изделия из жемчуга известного производителя за полцены. Посылки, в которых она отправляла товар, проданный через сайт, покупались ею у поставщика из другой страны.

За 16 месяцев она заработала более 43000 (около 2800 евро в месяц).



Источник: Франция

Bank account	Банковский чет
Young girl student	Молодая девушка, студентка
Internet payment service provider	Поставщик услуг Интернет-платежей
Pearls sold half price	Изделия из жемчуга, продаваемые за полцены

Commercial website	Коммерческий Интернет-сайт
Parcels used to send the goods sold online	Посылки для отправки товара, проданного через сайт

Пример использования коммерческих Интернет-сайтов и систем Интернет-платежей для продажи компонентов взрывчатых веществ

Управление финансовой разведки Бельгии получило информацию из управления финансовой разведки другого государства о том, что от одного из поставщиков услуг Интернет-платежей поступил отчет о подозрительных операциях, совершаемых гражданином европейской страны. Данный гражданин продавал через коммерческий Интернет-сайт следующие вещества: калий, хлорат, нитрат бария, нитрат стронция и нитрат аммония. Данные товары считаются товарами двойного назначения, так как могут использоваться для создания взрывчатки. Указанные вещества продавались клиентам из Восточной Европе.

Преступники планировали собирать деньги, полученные в результате своих незаконных продаж в Интернете, через поставщика услуг Интернет-платежей, одновременно отмывая их – также через этого поставщика.

Источник: Бельгия

Пример использования коммерческих Интернет-сайтов и систем Интернет-платежей, связанного с контрабандой оружия

Банк сообщил, что некий юрист, используя три личных банковских счетов, получал и отправлял большое количество Интернет-платежей, делал банковские переводы физическим лицам, живущим в других странах, получал чеки и вносил наличные деньги на счета без каких-либо видимых экономических оснований.

Анализ сообщений, сопровождавших финансовые операции с поставщиком услуг Интернет-платежей («платеж за пистолет X», «платеж за пистолет Y»), и банковских переводов позволил определить, что деятельность юриста в Интернете была связана с операциями по продаже оружия и запчастей к нему.

Дальнейшее расследование ПФР показало, что:

– в течение 4 лет этот человек сделал более 1600 операций, связанных с продажами. Такая активность в Интернете могла свидетельствовать о незаконной деятельности, связанной с использованием коммерческих Интернет-сайтов, торгующих оружием;

– он регулярно ездил в страны Центральной и Восточной Европы, не имеющих надежных заслонов от контрабанды оружия, и часто оставался в этих странах на неделю и более, что свидетельствовало о том, что он мог заниматься контрабандой оружия в эти страны.

Дело было передано в компетентные органы, занимающиеся контрабандой оружия.

Источник: Франция

E-shopping and weapons trafficking	Электронные покупки и контрабанда оружия
Internet payment service provider	Поставщик услуг Интернет-платежей
Transfers	Переводы
Int'l wire transfers to individuals	Международные банковские переводы физическим лицам
3 personal bank accounts	3 личных банковских счета
Spends money on weapons shopping websites	Тратит деньги на сайтах, торгующих оружием
The number of transactions (nearly one a day) makes his online activity suspicious, going beyond the simple hobby, and seems to be a real business	Количество сделок через Интернет (почти по одной сделке в день) вызывает подозрение: скорее всего, это не обычное хобби, а бизнес

47. Коммерческие Интернет-сайты и системы Интернет-платежей также могут использоваться для осуществления коммерческих операций без регистрации в качестве плательщика НДС и уплаты налогов.

Пример использования коммерческих Интернет-сайтов и систем Интернет-платежей для нелегальной продажи товаров (с уклонением от уплаты налогов)

Лица, в отношении которых было начато расследование, являлись директорами компании, закупавшей большое количество не облагаемых пошлиной сигарет и алкоголя для последующей продажи на отечественном рынке, и, таким образом, уклонявшейся от уплаты налогов. Неуплата налогов на указанные товары позволила компании значительно увеличить доходы от их реализации. Компания также занималась подделкой платежных квитанций, якобы полученных от экспортной компании, экспортирующей эти сигареты. Расследование показало, что никакие сигареты эта компания никогда не экспортировала. Расчет за сигареты производился наличными с доставившим их водителем по факту доставки.

Большую часть товара компания продавала через Интернет – клиентам, платившим кредитными картами. Большинство таких продаж через Интернет являлись незаконными и совершались с использованием трех разных адресов электронной почты. Платежи по заказам делались с одной или двух кредитных карт с банковскими счетами в Белизе. Одна из этих карт была выдана на имя компании. Деньги на

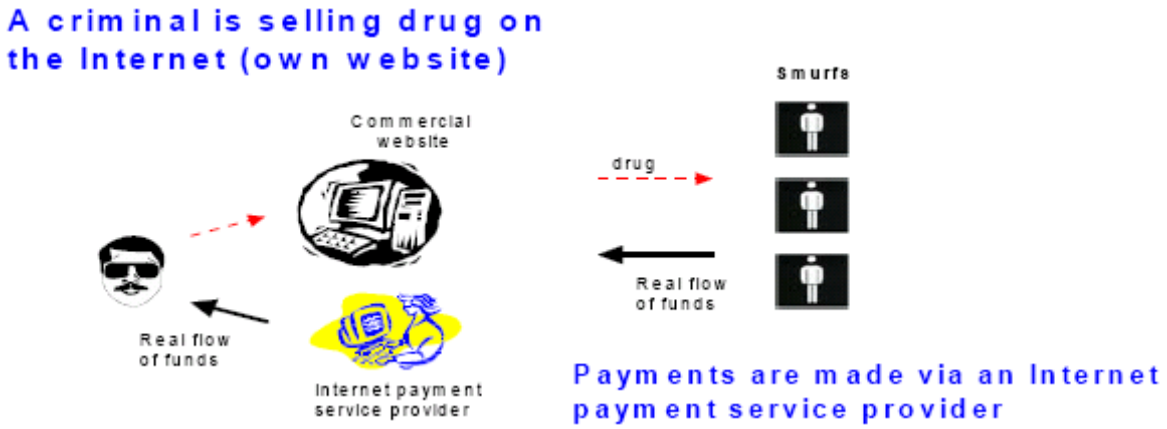
банковский счет в Белизе отправлял один из директоров (используя для этого несколько вымышленных имен), причем не только из Австралии, но и из Белиза, Гонконга и Вьетнама. Банковские переводы этот директор делал со счетов подставных компаний, под вымышленными именами и по методу «структуринга» (дробления платежей): деньги приобретались у хорошо известных банков – в один и тот же день совершалось множество покупок в разных отделениях банка, а сумма каждого денежного перевода была немного меньше 10000 австралийских долларов (для того, чтобы не превысить предел, после которого банковские сотрудники должны сообщать о таких переводах в соответствующие органы).

Источник: Австралия

48. Преступники могут разрабатывать свои собственные коммерческие Интернет-сайты для того, чтобы продавать незаконные продукты или заниматься незаконной деятельностью и использовать поставщиков услуг Интернет-платежей для сбора выручки от незаконной деятельности.

Пример использования коммерческих Интернет-сайтов и систем Интернет-платежей для сбора выручки от незаконной деятельности

Пользователь системы Интернет-платежей владеет коммерческим Интернет-сайтом, на котором он продает коноплю, семена конопли и принадлежности для приема наркотиков. Так как он хочет, чтобы ему платили через систему Интернет-платежей, покупатели используют систему Интернет-платежей, пользователем которой он является.



Источник: Люксембург

A criminal is selling drug on the Internet (own website)	Преступник продает наркотики через Интернет (через собственный сайт)
Commercial website	Коммерческий Интернет-сайт
Real flow of funds	Реальный получатель денег
Internet payment service provider	Поставщик услуг Интернет-платежей
Drug	Наркотик
Smurfs	Покупатели-сообщники
Payments are made via an Internet payment service provider	Платежи совершаются через поставщика услуг Интернет-платежей

Пример использования счета поставщика услуг Интернет-платежей для сбора

выручки от преступной деятельности

Лицо, использующееся услугами поставщика услуг Интернет-платежей, получает платежи с сайта, предлагающего услуги сопровождения или интимные услуги. Пользователь зарегистрирован на сайте и получает деньги от покупателей на счет. На сайте указана система Интернет-платежей. Сайт содержит откровенные материалы, клиенту предлагается несколько проституток на выбор, сайт профессионально сделан. Поставщик услуг Интернет-платежей обнаруживает этот сайт, определяет его IP-адрес и отправляет соответствующую информацию в ПФР.

Источник: Люксембург

49. Как уже говорилось в отчете ФАТФ «Новые способы платежей», виртуальные драгоценные металлы являются основой новой системы Интернет-платежей, заключающейся в обмене опционами (или правами) на покупку определенного количества виртуальных драгоценных металлов по определенной цене. Держатели счета в системе драгоценных металлов могут своПОДно обмениваться такими деривативами (так же, как и традиционными товарными или фондовыми деривативами). Покупатели приобретают определенное количество долей в виртуальных драгоценных металлах, цена на которые рассчитывается по ценам на металл на мировых товарных биржах. После приобретения покупателем доли в виртуальном драгоценном металле, эта доля или ее часть может передаваться либо другому лицу, либо торговцу в обмен на товары или услуги – также по Интернету. В результате обмен виртуальными драгоценными металлами позволяет несвязанным между собой третьим сторонам обмениваться фиксированной стоимостью активов, являясь средством перевода денежных средств и стоимости.

Пример использования платежного средства e-gold в качестве способа оплаты

27 апреля 2007 года в Вашингтоне, округ Колумбия, большое федеральное жюри предъявило обвинение двум компаниям, предоставлявших услуги, связанные с использованием электронных валют, а также их владельцам. Против компании E-Gold Ltd и компании Gold and Silver Reserve, Inc. и их владельцев было выдвинуто несколько обвинений на основании федерального законодательства: обвинение в сговоре с целью отмывания кредитно-денежных документов, обвинение в сговоре с целью управления нелицензированным предприятием по переводу денежных средств, обвинение в управлении нелицензированным предприятием по переводу денежных средств, и одно обвинение на основании законодательства округа Колумбия – обвинение в переводе денежных средств без лицензии. В обвинении сказано, что лицам, желавшим воспользоваться альтернативной платежной системой E-Gold, для открытия счета в системе E-Gold нужно было всего лишь сообщить действительный адрес электронной почты – никакая другая контактная информация не проверялась. Обвинительное заключение явилось результатом следствия, которое в течение двух с половиной лет велось секретной службой министерства финансов США, которое также обращалось за помощью к другим органам, включая налоговое управление США (НУ), Федеральное бюро расследований (ФБР) и другие государственные и местные органы правСПОрядка. Атторней округа Колумбия Джеффри Эй Тэйлор заявил: «Подсудимые руководили изощренным и масштабным предприятием по переводу денежных средств,

деятельность которого не контролировалась и не регламентировалась ни в одной стране мира, позволявшим анонимно совершать международные денежные переводы с помощью нескольких щелчков компьютерной мыши». Неудивительно, что преступники всех мастей потянулись к системе E-Gold для того, чтобы иметь возможность безнаказанно переводить свои деньги».

Источник: Министерство юстиции США

50. Во время семинара его участники также приводили примеры того, как коммерческие Интернет-сайты и системы Интернет-платежей используются не для отмывания денег, но для совершения преступлений (в большинстве случаев – мошенничества), являющихся причиной последующего отмывания денег. Такие примеры, даже если они напрямую и не относятся к теме настоящего исследования, будут, тем не менее, рассмотрены в нем, так как соответствующая информация может пригодиться традиционным финансовым учреждениям для борьбы с отмыванием денег.

51. Коммерческие Интернет-сайты и системы Интернет-платежей могут использоваться преступными элементами в мошеннических целях. Один из использующихся видов мошенничества заключается в продаже фиктивных товаров, которые продавец не станет поставлять покупателю после получения платежа. И если для привлечения покупателей (в этом случае – жертв мошеннических действий) используются коммерческие Интернет-сайты, то для получения денег (выручки от мошеннических действий) системы Интернет-платежей используются далеко не всегда. Часто для оплаты товаров, которые не будут поставлены, преступники используют банковские счета в традиционных финансовых учреждениях, денежные переводы, почтовые переводы. Эти же каналы используются впоследствии и для отмывания средств, полученных преступным путем (а именно, для сокрытия таких средств).

Примеры переводов денежных средств, связанных с мошенническими продажами на коммерческих Интернет-сайтах (оплаченный товар не поставляется)

Бельгийское ПФР получило из нескольких бельгийских банков несколько отчетов о подозрительных операциях. В них сообщалось, что на некоторые банковские счета поступали денежные переводы, которые могли быть связаны с (происхождение которых можно было объяснить) продажами на коммерческих сайтах. После поступления денежного перевода на счет все переведенные деньги с такого счета снимались.

Большая часть денежных переводов была на небольшие суммы (не более 800 евро), отправителями переводов были различные лица, и, судя по сообщению в графе «цель платежа», такие переводы были связаны с продажами на коммерческих Интернет-сайтах, иногда – с продажами предметов роскоши. Платежи делались не через поставщиков услуг Интернет-платежей, а перечислялись с банковского счета покупателя на банковский счет продавца. После поступления на счет деньги немедленно снимались.

Товары в таких случаях покупателю (жертве мошенничества, заключающегося в

непоставке товара) не поставляются.

В некоторых отчетах говориться о том, что поступившие на счет деньги не снимаются, а перечисляются в какую-либо страну, о которой известно, что в ней производят контрафактные товары (в случаях, имеющих отношение к продажам контрафактных товаров).

Банковский счет, использующийся для мошеннических операций, используется в течение ограниченного времени (из-за жалоб покупателей долгое время его использовать нельзя).

Расследование показало, что на коммерческих Интернет-сайтах используются вымышленные имена (имя, использующееся продавцом на коммерческом Интернет-сайте (во всех случаях вымышленное имя) и имя владельца банковского счета, на который переводятся деньги, являются разными). В одном случае, в соответствии с информацией, предоставленной правоохранительными органами, преступник использовал на коммерческом сайте разные имена. В другом случае преступник использовал два разных паспорта и разные имена.

Источник: Бельгия

Примеры продаж через коммерческие Интернет-сайты несуществующих товаров и использования платежной системы Western Union для сбора выручки от таких фиктивных продаж

Центр анализа информации об отмывании денег Национального бюро расследований в настоящий момент расследует дело крупномасштабном мошенничестве и отмывании денег. Два главных подозреваемых, находящиеся в Финляндии, действовали в этой стране качестве агентов Western Union. Офисы этих агентов были закрыты 27 марта 2007 года, а подозреваемые – взяты под стражу.

Некоторые лица, проживающие за пределами Финляндии, доверившись мошеннической информации, оплатили покупку несуществующих товаров (в данном случае автомобилей и иных транспортных средств) через коммерческие Интернет-сайты[8], перечислив деньги за них через Western Union на имена вымышленных лиц в Финляндии.

Два агента Western Union, выдавая себя за других, вымышленных лиц, получили эти деньги в Финляндии. После чего указанные агенты, снова выдавая себя за других лиц, направили полученные деньги через Western Union за пределы страны.

Двое подозреваемых в Финляндии получили от двух человек (организаторов аферы)

[8] Стоит заметить, что на некоторых коммерческих Интернет-сайтах продавец не имеет возможности требовать у потенциальных покупателей оплаты покупки почтовым переводом. Для противодействия мошенничеству владельцы таких коммерческих Интернет-сайтов не позволяют своим пользователям предлагать почтовые переводы в качестве способа оплаты (такой возможности на сайте просто не предусмотрено, и продавец, при обмене сообщениями через систему обмена сообщениями коммерческого сайта, не может просить у потенциальных покупателей оплатить покупку почтовым переводом).

на свои мобильные телефоны СМС с:

– информацией о жертвах из-за границы (имена, получатель денег, отправленная сумма и контрольный номер денежного перевода);

– инструкциями по отправке денег заграницу (имя получателя, сумма перевода и страна, в которую должны быть отправлены деньги).

Организаторы аферы проживают где-то в Европе.

Общее количество пострадавших превысило 300 человек, а сумма понесенных ими убытков составляет около 1,07 млн. евро. Большая часть из них проживает в США и Великобритании, а общее количество стран, граждане которых пострадали в результате описанных действий, составляет около двадцати пяти.

Два агента Western Union в Финляндии рассказали, что на их долю приходилось 10% денежных средств, которые они получали. Они также заявили, что оба организатора данной аферы приезжали в Финляндию во время ее активной фазы и забрали с собой крупную сумму наличных.

В ходе проведенного расследования было выяснено, что по крайней мере один из двух организаторов данной аферы имел аналогичные договоренности с агентами Western Union из нескольких других европейских стран.

27 марта 2007 года в офисах компании Western Union и в домах агентов были проведены обыски и сделаны аресты.

Проверка телефонов, SIM–карт и персональных компьютеров позволила получить большое количество улик. Были обнаружены сотни СМС и несколько сообщений электронной почты с инструкциями агентам Western Union, связанными с мошенническими действиями и денежными операциями.

Для дальнейшего расследования и успешного представления дела в суде нужна информация о как можно большем количестве предикатных (основных) преступлений, совершенных в других странах. Поэтому в 24 страны были направлены соответствующие запросы (Управлением финансовой разведки, Интерполом или Агентством по борьбе с отмыванием денег). На данный момент получена информация о 181 случае мошенничества из 19 стран.

Источник: Финляндия

52. Стоит упомянуть, что некоторые коммерческие Интернет-сайты используют клиентам механизмы, препятствующие осуществлению таких мошеннических действий через сайт, среди которых использование рейтингов для оценки надежности пользователей (покупателей и продавцов) на основе операций, сделанных ими на сайте ранее, уведомление клиентов о нежелательности оплаты заказов почтовыми переводами, рекомендации использовать поставщика услуг Интернет-платежей, сотрудничающего с данным сайтом (для снижения рисков), отслеживание и недопущение к сайту мошенников.

Потенциально уязвимые места

53. Потенциально уязвимые места, рассмотренные в этом разделе, могут помочь представителям частного сектора, которые пока не знают о механизмах ОД и ФТ, научиться определять подозрительные операции. Ниже сделан анализ нескольких потенциально возможных проблем, имеющих сходство с реальными проблемами, изученными управлениями финансовой разведки и рассмотренными в предшествующей части настоящего раздела.

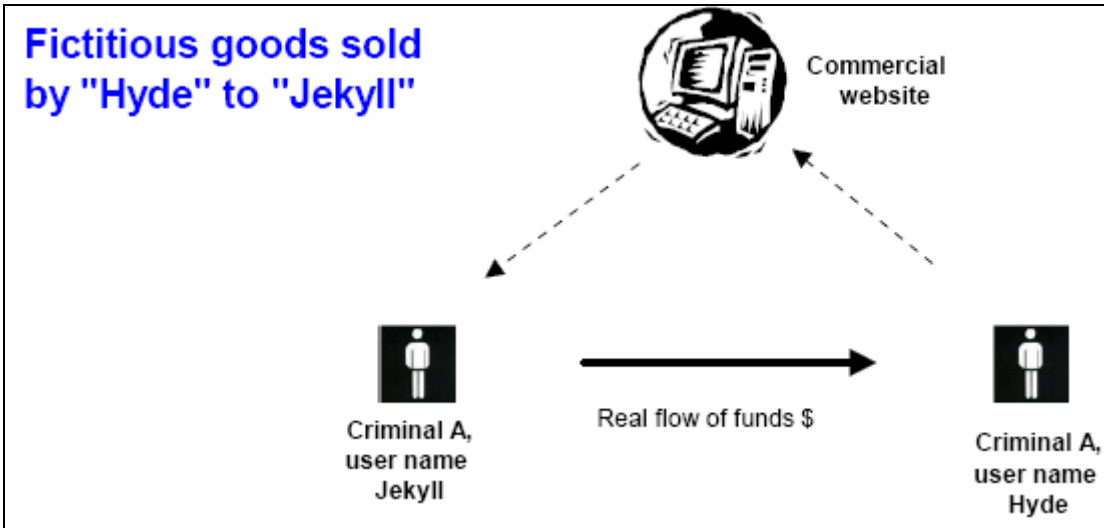
54. Представители частного сектора, принявшие участие в исследовании, считают, что такие потенциально уязвимые места могут представлять реальную опасность. При этом некоторые поставщики услуг Интернет-сайтов и поставщики услуг Интернет-платежей разработали системы и механизмы мониторинга и обнаружения (см. также раздел «Меры по снижению риска, предпринимаемые представителями отрасли»), позволяющие более эффективно выявлять мошеннические операции и ставить барьеры на пути преступных элементов, пытающихся использовать такие сайты и системы.

55. Преступники, для того, чтобы объяснить происхождение получаемых ими средств, могут осуществлять фиктивные операции через коммерческие Интернет-сайты с использованием традиционных финансовых учреждений или систем Интернет-платежей. Такая разновидность мошенничества имеет много общего с отмыванием денег с помощью продаж, при которых сумма перечисляемых денег несоразмерна стоимости поставляемых товаров.

Анализ потенциально возможной проблемы: фиктивные продажи на коммерческих Интернет-сайтах с последующей реальной оплатой

Покупатель и продавец знают друг друга и могут проживать в разных странах или на разных континентах. Поставки товара при совершении сделок такого типа не происходит. Некоторые коммерческие Интернет-сайты являются всего лишь связующим звеном между покупателями и продавцами, являющимися частными лицами. Они не несут ответственности за доставку товара, проверку качества и/или наличия/существования товара, предложенного на продажу. Покупатель не станет жаловаться на непоставку товара, так как продавец и покупатель состоят друг с другом в сговоре. Покупатель оплачивает продавцу стоимость покупки на банковский счет продавца заграницей. Получатель платежа без труда сумеет объяснить происхождение полученных средств, так как имеются все свидетельства того, что они были получены в результате продаж по Интернету.[9] Покупатель также легко сможет объяснить движение средств по счету своей кредитной карты, заявив, что он использует ее для оплаты покупок по Интернету. Коммерческие Интернет-сайты для частных лиц дают возможность покупать и продавать относительно дорогие товары, позволяя преступным элементам отмывать значительные суммы денег.

[9] Выписка или распечатка с экрана монитора с изображением коммерческого Интернет-сайта, на котором, например, изображен выставленный на продажу товар, не должна немедленно и безоговорочно рассматриваться как счет-фактура или документ, объясняющий происхождение средств, перечисленных на банковский счет клиента. И наоборот – если для того, чтобы объяснить происхождение средств, представлен такой документ, то финансовое учреждение может рассматривать его в качестве сигнала (признака) опасности. Об этом также говорится в разделе «Некоторые замечания о средствах контроля второго и третьего уровня».

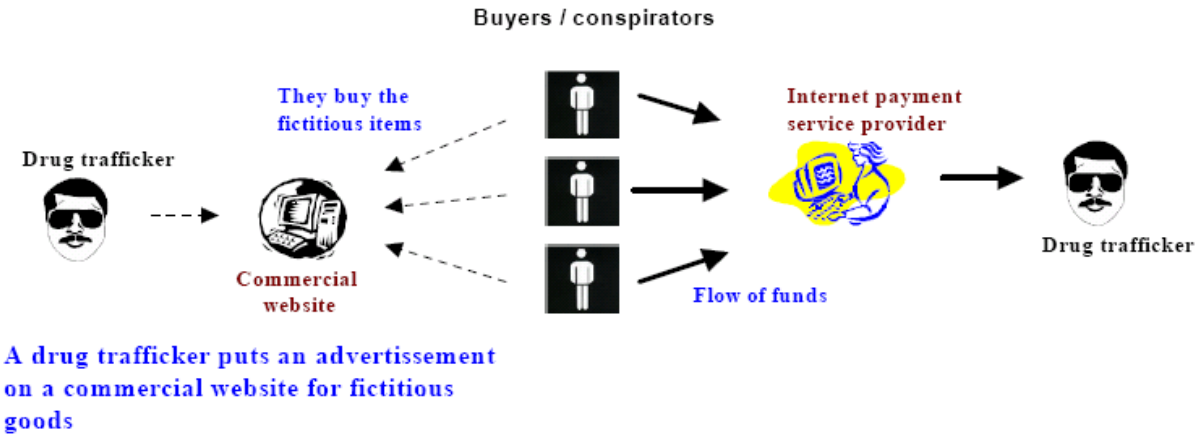


Источник: Бельгия

Fictitious goods sold by "Hyde" to “Jekyll”	Несуществующие товары, проданные «мистером Хайдом» «доктору Джекилу»
Commercial website	Коммерческий Интернет-сайт
Criminal A, user name Jekyll	Преступник А, имя пользователя «доктор Джекил»
Criminal A, user name Hyde	Преступник А, имя пользователя «мистер Хайд»
Real flow of funds	Движение средств

Анализ потенциально возможной проблемы: использование коммерческого Интернет-сайта для отмывания выручки от незаконного оборота наркотиков

Торговец наркотиками может использовать коммерческие Интернет-сайты для получения средств, вырученных от незаконной продажи наркотиков. Вместо того чтобы получать деньги на свой банковский счет напрямую, вызывая подозрения у банка, торговец наркотиками дает объявление о продаже каких-либо несуществующих товаров. Лица, приобретающие у него наркотики, начинают делать «покупки» на сайте. После получения платежа торговец наркотиками поставляет им наркотики. При этом он всегда может объяснить, что деньги, зачисленные на его счет, были получены «в результате продаж через Интернет». Для отмывания денег указанным способом «продавцу» и «покупателю» необходимо согласовывать свои действия.



Источник: Франция

Buyers/conspirators	Покупатели/участники преступного сговора
Drug trafficker	Торговец наркотиками
Commercial website	Коммерческий Интернет-сайт
They buy the fictitious items	Покупатели вымышленных товаров
Internet payment service provider	Поставщик услуг Интернет-платежей
Flow of funds	Движение средств
A drug trafficker puts an advertisement on a commercial website for fictitious goods	Торговец наркотиками размещает на коммерческом Интернет-сайте объявление о продаже вымышленных товаров

56. Если же товар, который продают преступники, существует на самом деле, продавцы и покупатели, которые знают друг друга, могут сильно завысить его цену, получая таким образом возможность объяснить движение относительно крупных сумм. Данный способ отмывания доходов является разновидностью отмывания денег с помощью торговых операций.

Анализ потенциально возможной проблемы: продажа товаров по завышенной цене

Механизм такой же, как и в вышеописанном примере, за исключением того, что продаваемые товары действительно существуют, но продаются по завышенной цене через нескольких подставных покупателей. Чистая разница между номинальной ценой продажи и фактической стоимостью поставленных товаров составляет сумму отмытых денежных средств. Сделки такого типа являются более безопасными для лиц, отмывающих деньги, так как в этом случае остаются официальные записи, документы, регистрационные данные о фактически поставленных товарах, а правоохранительным органам нужно доказать, что стоимость продажи сильно завышена по сравнению с реальной стоимостью товара на рынке.

Как вариант, отмывание денег может осуществляться прямо противСПОложным способом: покупатель приобретает товар по цене, которая значительно ниже его рыночной стоимости, а затем выгодно перепродает его. Впоследствии покупатель сможет заявить, что низкая стоимость товара, обеспечившая прибыль, была обусловлена разницей цен на него на разных рынках, а продавец спишет такую разницу на коммерческий убыток.

На многих Интернет-сайтах, особенно на сайтах, продающих товар на онлайновых аукционах, продаются товары, рыночная цена которых точно неизвестна, или которая с трудом поддается определению. Кроме того, аукционеры достаточно часто завышают цену даже при совершении законных сделок. И наконец, так как выставленный на продажу товар во время проведения аукциона остается у продавца, компания, занимающаяся организацией онлайновых аукционов, практически не имеет возможности установить действительную рыночную стоимость товара.

Источник: Бельгия

57. На коммерческих Интернет-сайтах могут продаваться уже упоминавшиеся выше контрафактные товары, а также похищенные товары (такие сайты также называют «виртуальной «малиной»). Системы Интернет-платежей могут использоваться для перевода или отмывания денежных средств, полученных в результате таких продаж.

Анализ потенциально возможной проблемы: продажа контрафактных или

похищенных товаров с использованием нескольких личных имен и имен пользователя

Преступник продает украденные и контрафактные товары через сайте-посреднике в продажах от потребителя к потребителю. Используя несколько личных имен и имен пользователя, преступник снижает риск быть обнаруженным мониторинговым отделом Интернет-сайта. Выручку, полученную от незаконных продаж, он может использовать либо для покупки других товаров или услуг онлайн, либо перевести ее на свой личный банковский счет. В этом случае происхождение средств, поступающих на счет, можно будет объяснить как выручку от «продаж по Интернету».

Источник: Франция

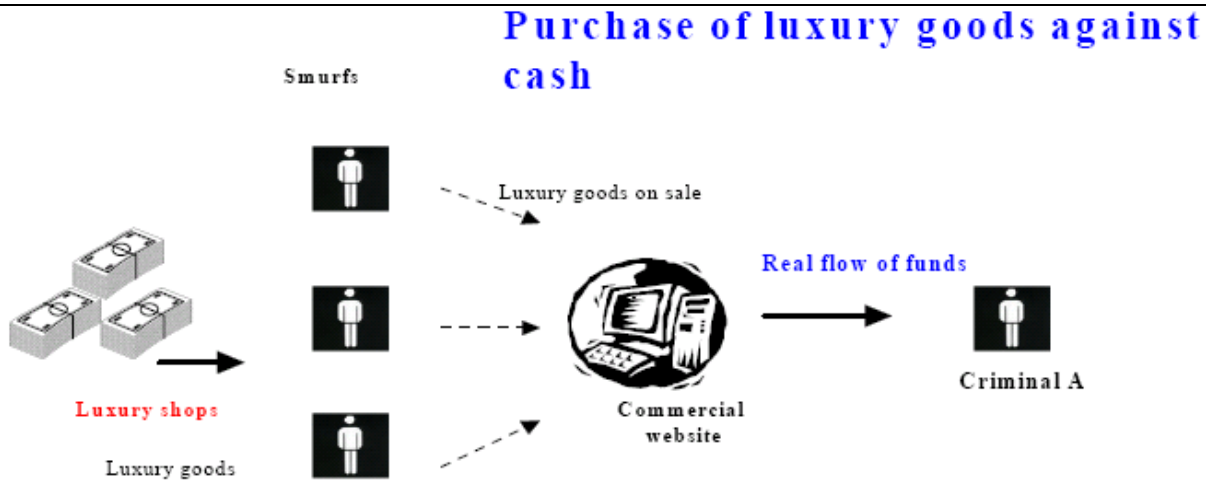
58. На коммерческих Интернет-сайтах могут продаваться не только поддельные, но и настоящие предметы роскоши, покупаемые за наличные лицами, нанятыми преступниками для отмывания доходов от незаконной деятельности.

Анализ потенциально возможной проблемы: использование коммерческих Интернет-сайтов для продаж (по заниженным ценам) настоящих предметов роскоши, приобретенных специально нанятыми людьми в дорогих магазинах

Преступники посылают своих сообщников в магазины, торгующие предметами роскоши, для покупки относительно дорогих товаров (например, дамских сумочек и тому подобных товаров) за наличные. Первый этап отмывания денег заключается в том, чтобы избавиться от имеющихся наличных, потратив их на товар (желательно мелкими купюрами). Для этой цели используются магазины, торгующие предметами роскоши, владельцы которых имеют слабое представление о способах отмывания денег.[10]

Впоследствии приобретенные предметами роскоши продаются на коммерческих Интернет-сайтах по более низкой цене. Для отмывания выручки, полученной в результате незаконной деятельности, преступники согласны потерять достаточно большую сумму денег. Выручка от продаж поступает на заграничный банковский счет продавца.

[10] Третья директива ЕС по ПОД/ФТ применяется к физическим или юридическим лицам, занимающимся торговлей товарами, в тех случаях, когда платеж наличными равен или превышает 15000 евро (независимо от того, выплачивается ли такая сумма за одну или за несколько покупок (если такие покупки предположительно могут быть связаны между собой)). Продавцы дорогостоящих товаров, принимающие платеж наличными, превышающий 15000 евро, обязаны выполнять требования по ПОД/ФТ (правила «знай своего клиента», ведение учета, сотрудничество с ПФР, надлежащая организация работы). В некоторых странах продавцы дорогостоящих товаров не имеют права принимать платеж наличными, если стоимость приобретенных товаров превышает определенный лимит (в Бельгии – 15000 евро).



Источник: Бельгия

Purchase of luxury goods against cash	Покупка предметов роскоши за наличные
Smurfs	Покупатели-сообщники
Luxury shops	Магазины, торгующие предметами роскоши
Luxury goods	Предметы роскоши
Luxury goods on sale	Предметы роскоши, идущие на продажу
Commercial website	Коммерческий Интернет-сайт
Real flow of funds	Получатель денег
Criminal A	Преступник А
Surfs of criminal A buy luxury goods in cash using money of criminal A and sell them on a commercial website	Покупатели-сообщники преступника А покупают предметы роскоши за наличные преступника А и продают их на коммерческом Интернет-сайте

59. Операции по отмыванию денег осуществляются не только на первом этапе отмывания денег (этап «размещения»), но и на двух других этапах (на этапах «расслоения» и «интеграции»). Обычно преступники стараются запутать свои финансовые операции, сделать их непонятными для правоохранительных органов и следователей, разбивая процесс отмывания денег на несколько этапов. Интернет-сайты и системы Интернет-платежей могут использоваться на разных этапах процесса отмывания денег. Традиционные финансовые учреждения могут использоваться на этапе размещения, а поставщики услуг Интернет-сайтов и поставщики услуг Интернет-платежей – на последующих стадиях, например, на стадии «расслоения» (как в вышеприведенном примере) и «интеграции» (покупка товаров за незаконные средства, введенные в финансовые системы ранее). Два примера, рассмотренных ниже, позволяют лучше понять этап «интеграции».

Анализ потенциально возможной проблемы: использование электронного кошелька в сочетании с другими методами ОД

– Человек, проживающий рядом с границей, регулярно импортирует из соседней страны табачную и алкогольную продукцию в количествах, превышающих объемы, не облагающиеся таможенной пошлиной;

– Указанная продукция продается частным лицам. Полученные наличные кладутся на сберегательный счет, открытый на имя одного из несовершеннолетних детей этого человека. Происхождение этих денег он может объяснить как денежные подарки ребенку от родственников;

– Средства, поступающие на сберегательный счет ребенка, регулярно перечисляются на банковский счет этого человека, имеющийся у него в другом банке. Кажется, что эти деньги имеют законное происхождение – они поступают со сберегательного счета одного из его детей. Перевод этих денег можно объяснить временными финансовыми трудностями, расходами на ребенка (например, на покупку мопеда, оплату уроков вождения и т.д.);

– Деньги, переведенные на банковский счет указанного лица, могут в дальнейшем использоваться для пСПОлнения электронного кошелька для покупки товаров и услуг через Интернет.

Источник: Франция

60. Принимая во внимание, что для финансирования терроризма могут использоваться небольшие суммы денег, существует потенциальная опасность использования коммерческих Интернет-сайтов и систем Интернет-платежей для финансирования терроризма.

61. Как уже упоминалось, поставщики услуг Интернет-сайтов и поставщики услуг Интернет-платежей зависят от информации, которую правоохранительные и иные органы передают им для того, чтобы они могли обнаруживать подозрительные операции, связанные с финансированием терроризма, при этом поставщики услуг Интернет-платежей, в своих отчетах о подозрительных операциях, предоставляемых в рамках содействия борьбе с финансированием терроризма, не всегда обязаны указывать, что та или иная деятельность, по их мнению, связана с финансированием терроризма.

Анализ потенциально возможной проблемы: использование коммерческого Интернет-сайта и поставщика услуг Интернет-платежей для финансирования террористической деятельности (также в сочетании с другими методами ОД)

– Известный террорист Y, проживающий в Германии и находящийся под плотным контролем спецслужб, желает перевести деньги террористу Z, проживающему во Франции для того, чтобы террорист Z мог купить мобильные телефоны или другие компоненты, необходимые для изготовления взрывных устройств;

– Опасаясь, что его могут обнаружить, если он воспользуется системой денежных переводов наподобие Western Union или MoneyGram, террорист Y решает использовать нестандартный способ перевода денег;

– Он просит студента зарегистрироваться на сайте-посреднике в продажах от потребителя к потребителю и открыть счет у поставщика услуг Интернет-платежей. Террорист Y дает студенту предоплаченную банковскую карту, на которой лежит 799 евро, для внесения этих денег на счет студента в Интернете;

– После этого студент переводит деньги со свого счета в Интернете на Интернет-счет другого студента, находящегося во Франции;

– Деньги, перечисленные на Интернет-счет студента из Франции, студент из Франции переводит на свой банковский счет и покупает предоплаченную банковскую карту,

которую передает террористу Z;

– Террорист Z может использовать предоплаченные банковские карты либо для расчетов за покупки, либо для пСПОлнения своего банковского счета.

Источник: Франция

62. Подставных лиц или посредников (таких как студенты в вышеприведенном примере) вербуют даже в Интернете, соблазняя комиссионными от 5% до 10% от переводимой суммы. Рассылается большое количество спама с предложением стать партнером «финансовой компании», получая и переводя денежные средства. Такие подставные лица используются для ОД/ФТ.

63. Другие возможные способы отмывания денег:

Другие возможные способы отмывания денег

– Преступник или третья сторона, используемая таким преступником, покупает товары через Интернет с помощью предоплаченных банковских карт (анонимно);

– Покупка предоплаченных банковских карт за наличные (в местах их продажи или с помощью третьих сторон);

– Покупка у третьей стороны (за наличные) активов/средств, имеющихся у этой стороны на счету в Интернете (с помощью поставщика услуг Интернет-платежей);

– Лицо, занимающееся отмыванием денег, объясняет, что движение средств связано с торговлей по Интернету (фиктивной);

– Преступник или лицо, занимающееся отмыванием денег, держит деньги на счетах, открытых в Интернете (используя для этой цели поставщика услуг Интернет-платежей).

Источник: Нидерланды

64. Если потенциально возможные способы отмывания денег и финансирования терроризма, описанные выше, окажутся осуществимыми, подозрительные операции можно будет обнаружить за счет надлежащей проверки клиентов и использования соответствующего программного обеспечения – ведь для того, чтобы сделать их экономически оправданными, их нужно совершать многократно[11]. Поставщики услуг Интернет-сайтов и поставщики услуг Интернет-платежей, применяющие подобные методы надлежащей проверки, проверяют клиентов, совершающих множество одинаковых операций, с использованием специальных процедур, позволяющих им получить больше информации о продавце (учредительный договор, идентификационный номер НДС и т.д.). Для обнаружения лиц, занимающихся торговлей поддельными товарами, коммерческие Интернет-сайты также сотрудничают с компаниями, продающими дорогие товары.

[11] Поставщики услуг Интернет-сайтов и поставщики услуг Интернет-платежей, опрошенные в рамках исследования, используют методы надлежащей проверки клиентов и мониторинговое программное обеспечение.

Сигналы (признаки) опасности

65. В этом разделе, являющимся результатом типологического анализа, сделан обзор потенциальных признаков ОД/ФТ. На такие сигналы (признаки) опасности должны обращать внимание поставщики услуг Интернет-платежей при анализе подозрительных операций. Сам по себе сигнал (признак) опасности не является основанием для того, чтобы считать ту или иную операцию подозрительной и сообщать о ней в ПФР. Для анализа подозрительных операций поставщик услуг Интернет-платежей должен собрать дополнительную информацию.

66. Некоторые поставщики услуг Интернет-платежей уже пользуются такими сигналами (признаками) опасности для определения подозрительных операции/подозрительной деятельности, используя для этого модели риска и программное обеспечение (см. также раздел «Меры по снижению риска, предпринимаемые представителями отрасли»). Однако такие сигналы (признаки) опасности рассчитаны на поставщиков услуг Интернет-платежей, которые еще на знакомы ни с рисками ОД/ФТ, ни с самими такими признаками опасности.

67. Данный раздел был также написан для того, чтобы представители частного сектора смогли использовать рассмотренные в нем сигналы (признаки) опасности наряду с сигналами (признаками) опасности, разработанными ими самими.

68. Для анализа подозрительных финансовых сделок у поставщиков услуг Интернет-платежей имеются возможность доступа к большому количеству информации, в том числе к информации о коммерческих операциях, лежащих в основе таких финансовых сделок (об этом говорится далее в разделе «Механизмы, использующиеся для снижения рисков ОД/ФТ»).

69. Были выделены следующие сигналы (признаки) опасности:

- Клиент открывает личный счет в системе Интернет-платежей в одной стране, после чего регулярно заходит в систему в другой стране или странах);
- На открытый клиентом счет приходит большое количество денежных переводов из другой страны, что может свидетельствовать о том, что клиент проживает не в стране, в которой он зарегистрировался, а в стране, в которой он зарегистрироваться не может (так как ее граждане по соображениям безопасности к регистрации на сайте не допускаются), или что он зарегистрировался в одной стране, а занимается незаконной деятельностью в другой, или что он скрыл результаты своей незаконной деятельности в другой стране;
- Клиент начинает делать покупки в Интернете на суммы, не соответствующие суммам его покупок в прошлом;
- Клиент пополняет свой счет в системе Интернет-платежей наличными[12] (если это предусмотрено поставщиком услуг Интернет-платежей[13]);

[12] Стоит заметить, что само по себе пополнение счета или карты наличными не является достаточным основанием для того, чтобы подозревать клиента в ОД/ФТ. Источник происхождения наличных может быть законным. При использовании клиентом наличных поставщик услуг Интернет-платежей должен использовать методы контроля или надлежащей проверки клиентов более высокого уровня (мониторинг операций, лимиты, ограничения и т.д.).

[13] Следует упомянуть, что системы, не принимающие оплату наличными, могут быть более надежными.

- Какая-либо третья сторона, не имеющая с клиентом никакой видимой связи, перечисляет средства на счет клиента в системе Интернет-платежей;
- Клиент регулярно покупает очень дорогие[14]/достаточно дорогие предметы с помощью предоплаченной дебетовой карты[15] или подарочной карты, происхождение средств на которых отследить гораздо сложнее[16];
- Клиент перепродает товары, которые скорее всего были куплены им ранее, безо всяких видимых причин, со значительной скидкой, или с существенной надбавкой к цене (в том случае мониторинг осуществим только если поставщик услуг Интернет-платежей, анализирующий подозрительные операции, сотрудничает с соответствующим коммерческим Интернет-сайтом);
- Покупатель требует, чтобы товары были отправлены либо на абонентский ящик, либо по адресу, отличающемуся от адреса, указанного при регистрации счета (зависит от способа получения товара, доступного в стране назначения);
- Клиент использует счет, открытый у поставщика услуг Интернет-платежей, не для покупки товаров через Интернет, а для сокрытия незаконно полученных денежных средств; Клиент открывает у поставщика услуг Интернет-платежей счет, кладет на него необходимую сумму денег, оставляет эти деньги на счету на нужный ему период времени, после чего забирает их[17];
- Клиент требует, чтобы деньги с его счета в Интернете были перечислены третьей стороне, не имеющей к нему никакого видимого отношения;
- Клиент использует кредитные карты (особенно предоплаченные), выпущенные в другой стране;
- Клиент занимается продажами незаконных товаров или изделий, находящихся в списке запрещенных товаров;
- Неадекватность цены, предлагаемой на аукционе в Интернете или во время аукционной продажи, которая может свидетельствовать о сговоре между покупателем и продавцом (клиент предлагает купить товар по цене, существенно выше запрашиваемой). Дополнительными признаками опасности могут являться неоднократные продажи товара одним и тем же покупателем одному и тому же продавцу;
- Купленные товары регулярно отправляются в другую страну;

---

[14] В соответствии с информацией, полученной от представителей частного сектора, участвовавших в исследовании, посвященном коммерческим Интернет-сайтам и поставщикам услуг Интернет-платежей, средняя стоимость коммерческой операции и сумма последующего платежа весьма мала. Поэтому лица, занимающиеся отмыванием денег и желающие использовать коммерческие Интернет-сайты и системы Интернет-платежей в своей преступной деятельности и для отмывания денег, для того, чтобы не быть обнаруженными, должны сделать несколько небольших операций подряд. Если они заплатят крупную сумму сразу, их обнаружат поставщики услуг Интернет-сайтов и поставщики услуг Интернет-платежей, использующие соответствующее программное обеспечение.

[15] Поставщикам услуг Интернет-платежей иногда бывает сложно отличить кредитную карту от предоплаченной, так как эмитенты кредитных и предоплаченных карт используют похожие номера для карт обоих типов.

[16] Следует упомянуть, что в большинстве случаев эмитенты подарочных картах кладут на них небольшие суммы. Поэтому для обеспечения рентабельности операций по отмыванию денег преступники должны использовать несколько подарочных карт. Эмитенты подарочных карт также используют механизмы внутреннего контроля, отслеживая их выпуск в местных магазинах и супермаркетах. Это снижает степень анонимности, но не устраняет ее полностью.

[17] Некоторые онлайновые электронные кошельки предусматривают временные ограничения на хранение денег.

- Клиент использует кредитную карту, выпущенную банком в какой-либо в оффшорной стране или в стране, не желающей сотрудничать с ФАТФ[18];
- Деньги происходят из страны, не желающей сотрудничать с ФАТФ;
- По информации ФАТФ, страна происхождения клиента не желает сотрудничать в области противодействия отмыванию денег и финансированию терроризма;
- Неожиданно большой оборот денежных средств на недавно открытом коммерческом Интернет-сайте или неожиданное увеличение стоимости коммерческого Интернет-сайта после нескольких продаж.

Поведение клиента или осуществленные им операции могут рассматриваться как подозрительные при наличии одного или нескольких признаков опасности.

70. Представители частного сектора, принявшие участие в исследовании, заявили, что считают (на основании имеющегося у них опыта) данный список сигналов (признаков) опасности точным и релевантным.

[18] Все страны, отказывающейся сотрудничать с ФАТФ, были исключены. Некоторые страны по-прежнему находятся под наблюдением.

РИСКИ ОТМЫВАНИЯ ДЕНЕГ И ФИНАНСИРОВАНИЯ ТЕРРОРИЗМА

71. Риски ПОД/ФТ, возникающие в связи с отмыванием денег с помощью торговых операций и заочными сделками, также присущи коммерческим Интернет-сайтам и системам Интернет-платежей. Требования ПОД/ФТ для коммерческих Интернет-сайтов сравнимы с требованиями ПОД/ФТ для традиционных торговых предприятий (которые применяются только к предприятиям, принимающим наличные в суммах, превышающих установленный порог), а требования ПОД/ФТ для систем Интернет-платежей сравнимы с требованиями для обычных платежных систем (несмотря на заочный характер отношений в системах Интернет-платежей, так как для снижения рисков ОД/ФТ применяются меры по надлежащей проверке клиентов и мониторингу, основанные на оценке возможных рисков).

72. Эти риски можно классифицировать в соответствии с этапами отмывания денег:

Этап «размещения»:

- **Анонимность[19] клиентов на некоторых коммерческих Интернет-сайтах и в системах Интернет-платежей.** В некоторых случаях как регистрация, так и операции могут осуществляться анонимно (для регистрации на некоторых сайтах достаточно указать анонимный адрес электронной почты);
- **Отношения с клиентами являются заочными.** Поставщики услуг Интернет-сайтов и поставщики услуг Интернет-платежей работают вне личного контакта с клиентами, поэтому им сложно быть уверенными в том, что они общаются именно с тем человеком, который были идентифицирован при регистрации;
- **Возможность многократной регистрации**. Многократная (анонимная) регистрация пользователем для покупки и продажи товаров может стать причиной возникновения сложностей при обнаружении, мониторинге и обратном отслеживании операций и денежных потоков;
- **Удаленный доступ к коммерческим Интернет-сайтам и системам Интернет-платежей**. Зайти на коммерческий Интернет-сайт и воспользоваться системой Интернет-платежей можно в любой точке мира. Преступник может выйти в Интернет с любого терминала, не зарегистрированного на его имя или никак не связанного с ним, что усложняет работу правоохранительных органов по отслеживанию и поимке преступников и лиц, занимающихся отмыванием денег;
- **Относительная «анонимность» некоторых способов платежей.** При оплате с помощью предоплаченных кредитных карт, подарочных карт/подарочных чеков[20], происхождение средств отследить либо невозможно, либо очень трудно[21].

---

[19] Надлежащая идентификация клиента является необходимым условием не только для обнаружения подозрительных действий, осуществляемых физическим лицом/компанией, но и для эффективного расследования подозрительной операции.

[20] Даже учитывая тот факт, что в большинстве случаев эмитенты анонимных подарочных карт кладут на них небольшие суммы.

[21] Даже при использовании механизмов внутреннего контроля для мониторинга и надзора за выпуском подарочных карт в местных магазинах или супермаркетах, недопущения или контроля внезапного увеличения количества эмитированных подарочных карт и положенных на них сумм (анализ информации о покупках, структура покупок и места расхода денег, IP-адреса, физический мониторинг территории), степень анонимности можно снизить, однако полностью ее устранить нельзя.

Этап «расслоения»:

- **Быстрота перевода денежных средств.** Операции, выполняемые продавцами и покупателями через коммерческие Интернет-сайты и системы Интернет-платежей, проходят очень быстро, так как делаются в электронном виде;
- **Глобальный характер операций и проблема подсудности**. Операции через коммерческие Интернет-сайты и системы Интернет-платежей могут совершаться глобально, вне границ какого-то одного государства, поэтому компетентные органы страны, в которой находится поставщик услуг Интернет-платежей не всегда имеют право на расследование случаев ОД или ФТ и на преследование в судебном порядке. Точно так же не существует какого-либо единого органа, выполняющего регулирующие и контролирующие функции.

Быстрота перевода денежных средств, глобальный характер операций и проблема подсудности, связанные с использованием коммерческих Интернет-сайтов и систем Интернет-платежей, затрудняют деятельность ПФР и правоохранительных органов, расследующих случаи отмывания денег или финансирования терроризма.

- **Объем – большое количество операций и сумм[22].** Поставщикам услуг Интернет-платежей сложно определить критерии мониторинга и обнаружения подозрительных операций из-за большого количества таких операций и, соответственно, сумм по таким операциям (операции какого типа стоит считать подозрительными?)[23];
- **Ограниченное участие человека**. Так как операции, совершаемых через коммерческие Интернет-сайты и системы Интернет-платежей, характеризуются меньшими объемами участия человека, традиционные механизмы обнаружения первого уровня, почти полностью построенные на личном общении с клиентом, в данном случае отсутствуют – их роль должны выполнять тщательно продуманные механизмы обнаружения второго уровня[24];
- **Отсутствие или несоответствие необходимым требованиям журналов контроля, учетной документации или отчетов о подозрительных операциях со стороны некоторых поставщиков услуг Интернет-платежей.**

Этап «интеграции»:

- **Возможность приобретения дорогостоящих товаров.** Приобретение (дорогостоящих) товаров, драгоценных металлов, недвижимости или ценных бумаг через коммерческие Интернет-сайты с помощью систем Интернет-платежей;

---

[22] Поставщик услуг Интернет-платежей должен уметь снижать потенциальный риск за счет введения необходимых ограничений на использование счета.

[23] Следует заметить, что традиционным финансовым учреждениям также трудно определить критерии мониторинга операций тех клиентов, которые осуществляют их с помощью программного обеспечения.

[24] Если поставщики услуг Интернет-платежей обеспечат надлежащий мониторинг финансовых операций своих клиентов, реагируя на отклонения от сложившейся модели поведения клиента, то недостаток личного контакта, имеющийся в начале взаимоотношений с поставщиком услуг коммерческого Интернет-сайта и поставщиком услуг Интернет-платежей, может перестать быть проблемой.

НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОТНОШЕНИЙ В ДАННОЙ ОТРАСЛИ

73. По причинам, которые были рассмотрены выше, а также из-за опасений того, что преступники и террористы смогут использовать коммерческие Интернет-сайты и системы Интернет-платежей для отмывания денег и финансирования терроризма, заявления о необходимости регулирования их работы государством стали раздаваться все чаще.

Общие сведения

74. Как правило, работа коммерческих Интернет-сайтов регламентируется в основном в части защиты клиента (обеспечение надлежащей информированности пользователей об имеющихся у них правах и обязанностях, общие условия использования, использование электронных договоров, определение коммерческого Интернет-сайта, реклама и т.д.), запрета на продажу определенных товаров и возможности отмены онлайновой покупки.

75. Например, электронная торговля регулируется несколькими директивами ЕС. Целью такого регулирования в основном является обеспечение ее прозрачности для потребителей и, как следствие, обеспечение их защиты. Основные правила и требования содержатся в Директиве об электронной торговле (2000/31/EC) и в Директиве о дистанционной торговле (1997/7/EC). В первой директиве содержится несколько требований к обеспечению прозрачности деятельности электронно-коммерческих компаний, а именно, к обеспечению прозрачности информации о типе компании, общей информации о компании, а также информации о процессе покупки продукта. Во второй директиве изложены правила об аннулировании покупок (в течение определенного времени). И наконец, в Директиве ЕС (2006/2004/EC) о гармонизации трансграничных операций оговаривается порядок сотрудничества между различными государствами в части защиты прав потребителя.

76. В США защитой потребителей от недобросовестных, вводящих в заблуждение, мошеннических методов торговли занимается Бюро защиты потребителей при Федеральной торговой комиссии США (ФТК). Бюро занимается расследованиями, преследует компании и лиц, нарушающих закон, в судебном порядке, разрабатывает нормы и правила защиты клиентов, информирует потребителей и компании об имеющихся у них правах и обязанностях. Бюро также занимается сбором информации об обмане потребителей и хищениях персональных данных (так называемые «кражи личности») и передает ее в правоохранительные органы страны.[25] Правоприменяющая служба ФТК возбуждает дела, связанные с неисполнением судебных решений и с применением гражданско-правовых санкций для приведения в исполнение судебных запретов и административных приказов федеральных судов по делам ФТК о защите прав потребителя; согласовывает (через Отдел по связям) действия ФТК с органами исполнения судебных решений по криминальным делам: разрабатывает, анализирует и обеспечивает исполнение постановлений о защите прав потребителей, координирует многосторонние инициативы по решению текущих вопросов защиты прав потребителей, обеспечивает исполнение программы банкротства Бюро защиты потребителей.[26]

---

[25] Федеральная торговая комиссия США (2007a).

[26] Федеральная торговая комиссия США (2007b).

77. В большинстве случаев каких-либо обязательств по идентификации или по предоставлению СПО в отношении коммерческих Интернет-сайтов не выдвигается. В Нидерландах такие обязательства применяются к таким коммерческим Интернет-сайтам, которые в дополнение к стандартным услугам также оказывают и услуги Интернет-платежей.

78. Точно так же, в соответствии с международными стандартами ПОД/ФТ, применяющимися к традиционным торговым предприятиям, если получаемая ими сумма наличных не превышает установленного порога, применения мер ПОД/ФТ (меры по надлежащей проверке клиентов, сотрудничество с ПФР, надлежащий внутренний контроль) от торговых предприятий не требуется.

79. Обязательства ПОД/ФТ (включающие в себя, среди прочего, обязательства по мониторингу и обнаружению подозрительных операций) являются обязательствами, налагаемым на финансовые учреждения и поставщиков услуг, связанных с электронными деньгами.

80. В Европейском Союзе эмитенты электронных денег подлежат лицензированию, а их деятельность регулируется органами той страны, в которой выпускаются электронные деньги. Европейский паспорт позволяет любому эмитенту электронных денег, получившему лицензию в одной стране ЕС, работать на всей территории ЕС. Электронные деньги, выпущенные в одной стране ЕС, могут быть потрачены на коммерческом Интернет-сайте в другой стране ЕС. Большинство эмитентов электронных денег находятся в Великобритании, Люксембурге и ФРГ. В США лицензированные поставщики услуг Интернет-платежей называются «компаниями по оказанию денежных услуг» (КДУ). Лицензии предоставляются поставщикам услуг Интернет-платежей и в других странах, например, в Австралии. В Китае, по-видимому, к поставщикам услуг Интернет-платежей никаких требований не предъявляется. При этом эмитент вправе выпускать электронные деньги только для клиентов из той страны, в которой они были выпущены (страна, в которой ему была выдана лицензия).

81. В Европейском Союзе пруденциальный контроль за эмитентами электронных денег осуществляется в соответствии с Директивой ЕС 2000/46/ЕС (Директива ЕС по электронным деньгам). Директива содержит нормативные положения, на основе которой осуществляется пруденциальный контроль за эмитентами электронных денег для обеспечения рациональной, разумной работы и финансовой устойчивости таких эмитентов. Нормативные положения предусматривают, среди прочего, обязательства по наличию начального капитала, требования о наличии денежных средств, достаточных для исполнения всех финансовых обязательств по выпущенным и неоплаченным электронным деньгам, ограничения на инвестирование, обязательства по обеспечению рационального и разумного управления, надлежащего порядка управления делами, учетной политики и механизмов внутреннего контроля.

82. Европейские директивы ПОД/ФТ распространяются и на эмитентов электронных денег. Директива 2005/60/ЕС предусматривает упрощенный порядок надлежащей проверки клиентов, оговаривающий, что если устройство не может быть пополнено, максимальная сумма хранения не должна превышать 150 евро, а если устройство может быть пополнено, то общая сумма операций за календарный год не может превышать 2500 евро, за исключением случаев снятия владельцем наличных владельцем такого устройства на сумму 1000 евро или более в том же календарном году (Статья 3 Директивы 2000/46/ЕС).

83. Для тех предприятий, деятельность которых регламентируется, например, для поставщиков услуг Интернет-платежей, регулятивные органы и профессиональные

объединения стараются разработать рекомендации по обеспечению соответствия требованиям ПОД/ФТ и умению различать различные виды мошенничества и способы ОД/ФТ.

Обзор по странам

Великобритания

84. Специальной нормативной базы, регламентирующей электронную торговлю, в Великобритании нет. При этом в этой стране существует орган – Служба финансового надзора – регулирующий деятельность, связанную с выпуском электронных денег и продажей компаниями в Великобритании финансовых услуг с помощью электронных средств.

85. По законодательству Великобритании, электронные деньги представляют собой денежную стоимость, представленную обязательствами эмитента, которая хранится в электронной форме и принимается при платежах третьими лицами. Электронные деньги считаются электронным эквивалентом монет и банкнот, предназначенным для осуществления платежей на небольшие суммы.

86. Служба финансового надзора регулирует использование электронных денег в соответствии с Директивой ЕС по электронным деньгам. Эмитенты электронных денег также имеют обязательства в соответствии с Положениями об отмывании денег 2007, например, обязательства по надлежащей проверке клиентов и обеспечению постоянного мониторинга своих отношений с деловыми партнерами. При обнаружении подозрительных действий компания юридически обязана сообщить об этом властям. Служба финансового надзора требует от эмитентов электронных денег доказательств того, что они в состоянии надлежащим образом контролировать риски, с которыми они сталкиваются в своей работе. Меры, которые могут быть приняты эмитентами электронных денег для исполнения своих юридических обязательств, обсуждаются в Руководстве Совместной руководящей группы по контролю за отмыванием денег.

Люксембург

87. В Люксембурге законодательство страны имеет преимущественную силу по отношению к Директиве ЕС по электронным деньгам и к Директивам ПОД/ФТ. В июле 2007 года первый поставщик услуг Интернет-платежей открыл свою штаб-квартиру в Люксембурге. В лицензии, выданной Комиссией по надзору за финансовым сектором (Commission de Surveillance du Secteur Financier) (далее – «КНФС») данное предприятие было признано банком. Таким образом, деятельность этого поставщика услуг Интернет-платежей регламентируется теми же законами и положениями ПОД/ФТ КНФС, что и деятельность любого банка в Люксембурге. Данный поставщик услуг Интернет-платежей имеет, в частности, такие обязательства: идентификация клиента (надлежащая проверка клиентов (по упрощенной/расширенной процедуре) с использованием подхода на основе оценки рисков), учет, надлежащие внутренние процедуры ПОД/ФТ, сотрудничество с властями Люксембурга (в частности, с ПФР). При непреднамеренном нарушении вышеперечисленных обязательств ПОД/ФТ применяются меры административного наказания, при намеренном – меры уголовного наказания.

Нидерланды

88. В Нидерландах применяется Директива ЕС по электронным деньгам (2000/46/EC) и Третья директива по противодействию отмыванию денег (2005/60/EC). Для предоставления услуг Интернет-платежей нужна лицензия на использование электронных денег, после получения которой в отношении поставщика таких услуг действуют специальные юридические нормы. Обязанности включают в себя регистрацию/лицензирование, (пруденциальный) контроль, ведение учетной документации, уведомление о подозрительных операциях, иные специальные стратегии и процедуры ПОД (меры по надлежащей проверке клиентов). Юридические нормы, действующие в отношении поставщиков услуг, которым был предоставлено разрешение на отступление от требований, менее обременительны. Обязанности включают в себя: ведение учетной документации, уведомление об отсутствии подозрительных операций. Какие-либо иные стратегии и процедуры ПОД не применяются. Официальные разрешения на отступление от требований для целей пруденциального контроля были предоставлены пяти эмитентам электронных денег. Кроме того, некоторые поставщики услуг Интернет-платежей разработали механизмы саморегулирования деятельности своих компаний. Главной целью создания таких механизмов является защита доброго имени компании, решение вопросов, связанных с юридической ответственностью и кредитными рисками.

США

89. Деятельность банковских организаций, предлагающих своим клиентам методы платежей, использующиеся в электронной торговле в США, регламентируется целым комплексом требований ПОД/ФТ, включая, среди прочего, требования об обнаружении и уведомлении о подозрительных операциях, ведении учета переводимых средств и выполнении программ соответствия требованиям ПОД и идентификации клиента. Целью программы соответствия требованиям ПОД является принятие и выполнение всеобъемлющих стратегий, процедур и методов надлежащей проверки всех без исключения клиентов, которые помогут банковским организациям США определять потенциально опасные операции.

90. Если какая-либо банковская организация, работающая в США, посчитает, что та или иная операция является подозрительной, она обязана представить в управление финансовой разведки США – Службу по борьбе с финансовыми преступлениями (СБФП) – отчет о подозрительной деятельности (ОПД). Банковские организации, работающие в США, обязаны сообщать об операции или нескольких операциях, на (общую) сумму равную или превышающую 5000 долл. США, которые были осуществлены (в отношении которых была сделана попытка осуществления) учреждением, в учреждении или через учреждение, о котором банковской организации «известно, которое оно подозревает или имеет причины подозревать» в совершении такой операции, которая *i)* включает в себя средства, полученные в результате незаконной деятельности, или осуществляется для утаивания средств, полученных в результате незаконной деятельности; *ii)* предназначена для уклонения от соблюдения требований Закона о банковской тайне (ЗБТ) к отчетности или учету (напр., разделение платежей на небольшие суммы (структуринг) для уклонения от отражения валютной операции в отчетности); *iii)* «не имеет деловой или иной очевидной законной цели или не относится к типу операций, осуществления которых можно было бы ожидать от данного клиента, и цель которой банковская организация, после изучения имеющихся фактов (включая предпосылки и возможные причины), понять не может».

91. Федеральные банковские агентства и Служба по борьбе с финансовыми преступлениями (СБФП) Министерства Финансов США являются основными органами

власти, ответственными за обеспечение исполнения соответствующих требований ПОД/ФТ.

92. Федеральным банковским агентствам США было поручено (в соответствии с федеральными банковскими законами 12 USC 1818(s) и 12 USC 1786(q) для банков и сберегательных банков) обеспечить выполнение банковскими организациями (в соответствии с их юрисдикцией) программ соответствия требованиям Закона о банковской тайне/ПОД.

93. Деятельность, связанная с электронными переводами платежей, регулируется и некоторыми другими нормативными актами. Они относятся к правам, ответственности и обязанностям сторон по электронным переводам платежей (ЭПП), и к защите потребителей, пользующихся системами ЭПП (такими как банкоматы и дебетовые карточки).

Сингапур

94. В Сингапуре электронные деньги часто называют «средством хранения денежной стоимости» (СХДС). По законодательству Сингапура, СХДС являются разновидностью предоплаченного электронного кошелька или карты, которые могут использоваться в системе эмитента СХДС. Эмитентов СХДС также называют «держателями СХДС».

95. Эмиссия и использование СХДС регулируется Законом о платежных системах (надзор) 2006 года (PS(O)A) и соответствующими подзаконными актами.[27] Любая организация вправе выпустить СХДС для хранения денежной стоимости. Однако выпуск СХДС, общая денежная стоимость которых превышает 30 млн. сингапурских долларов, должен быть утвержден Валютным управлением Сингапура (ВУС), а банк, получивший лицензию ВУС, несет всю полноту ответственности за хранимую стоимость. Эмитентам СХДС с общей хранимой стоимостью ниже установленного лимита в 30 млн. сингапурских долларов, разрешение ВУС на осуществление своей деятельности получать не нужно, однако они должны уведомлять своих потенциальных клиентов о том, что их СХДС не подлежат утверждению ВУС.

96. Помимо нормативных требований (PS(O)A), любой держатель СХДС, выпускающий СХДС с лимитом, превышающим 1000 сингапурских долларов, обязан соблюдать и применять положения Уведомления ВУС для держателей СХДС о требованиях по борьбе с отмыванием денег/финансированием терроризма.[28]

97. Уведомление обязывает держателей принимать превентивные меры, нацеленные на снижение риска использования СХДС в незаконных целях. В Уведомлении изложены обязательства держателей СХДС, в соответствии с которыми они должны принять меры к снижению рисков отмывания денег и финансирования терроризма, включая такие меры как: надлежащая проверка клиентов (по упрощенной/расширенной процедуре), идентификация пользователей (клиентов), проверка идентификации пользователей, идентификация и проверка личности бенефициарных владельцев, заочная проверка, анализ соответствующих операций, ведение учетной документации, уведомление о подозрительных операциях, внутренний контроль, проверки и обучение.

---

[27] *Закон о системах платежей (надзор) 2006 года (PS(O)A).*

[28] Валютное управление Сингапура (2007).

98. Любой держатель СХДС, не могущий или не желающий выполнять требования Уведомления, после признания его виновным в их невыполнении, облагается штрафом, размер которого не может превышать 1000000 сингапурских долларов, а при повторном нарушении указанных требований облагается штрафом в размере 100000 сингапурских долларов за каждый день такого нарушения после признания его виновным (в соответствии с разделом 27B закона ВУС[29]).

99. ВУС также выпустило Рекомендации по СХДС[30], в которых изложены принципы рациональной работы и методы снижения рисков для всех держателей СХДС. Эти рекомендации, разработанные на основе указанных принципов, затрагивают такие вопросы, открытость и прозрачность, общественное доверие, защита хранимой стоимости, профилактика отмывания денег и борьба с финансированием терроризма.

Китай

100. Нормативной базы, регламентирующей электронную торговлю или использование систем Интернет-платежей, в Китае нет. Тем не менее, 13 декабря 2007года китайское Министерство торговли издало рекомендательный документ под названием «О содействии регулируемому развитию электронной торговли». В документе поставщикам услуг Интернет-платежей предложены рекомендации по улучшению репутации предприятий отрасли, обеспечению их стабильной и разумной работы, недопущению неоправданного расширения предприятий и беспорядочной конкуренции между ними, обеспечению безопасности средств пользователей. В документе рекомендуется обеспечить принятие таких мер, как стандартизация управления, надзор за работой предприятия, обеспечение безопасности электронных платежей, сохранение данных об операциях, профилактика незаконных финансовых операций и т.д.

Гонконг, Китай

101. в Гонконге (Китай), работа эмитентов электронных денег и поставщиков услуг Интернет-платежей, не лицензируется. В этой стране электронные деньги в основном представлены многофункциональными картами с хранимой стоимостью. В соответствии с главой 155 (ВО) Банковских правил[31], учреждения в Гонконге, выпускающие или содействующие выпуску многофункциональных карт с хранимой стоимостью, должны иметь соответствующее разрешение Валютного управления Гонконга (ВУГ). Такие предприятия называются уполномоченными предприятиями (УП) и контролируются ВУГ.

---

[29] *Валютное управление Сингапура (Глава 186).*

[30] Валютное управление Сингапура (2006).

[31] В соответствии с определением, данным в Банковских правилах, многофункциональная карта с хранимой стоимостью представляет собой карту, позволяющую хранить данные в электронной, магнитной или оптической форме, по которым или в связи с которыми владелец карты (прямо или косвенно) уплачивает ее эмитенту определенную сумму денег за: *i)* хранение стоимости (всех или части) этих денег на карте; и за *ii)* обязательство эмитента (явно выраженного или подразумеваемого), заключающееся в том, что по предъявлению карты эмитент или какая-либо третья сторона предоставят товары или услуги (которые могут включать в себя предоставление денежных средств). В настоящий момент выпуском многофункциональных карт с хранимой стоимостью в Гонконге занимается всего одна компания (Octopus Cards Limited). Компания Octopus Cards Limited имеет разрешение на работу в качестве депозитной организации в соответствии с Банковскими правилами. Выпускаемые ею карты предназначены для небольших платежей при покупке товаров в розницу, а максимальная сумма для одной карты составляет 1000 гонконгских долларов.

102. Поставщики услуг Интернет-платежей в Гонконге имеют в своем распоряжении всего лишь базовые инструменты, с помощью которых их пользователи совершают платежи разных типов, перечисляя деньги со своих банковских счетов на счета продавца товаров или услуг. Тем не менее, если какое-либо Гонконге захочет оказывать услуги подобного типа, ему нужно будет сначала получить лицензию ВУГ для осуществления деятельности в качестве УП.

103. ВУГ разработало различные стратегии и требования, подлежащие выполнению УП, и изложило их в виде контрольных директив. Контрольные директивы по борьбе с отмыванием денег и финансированием терроризма, разработанные ВУГ, называются «Директивы по предупреждению случаев отмывания денежных средств» и «ДСПОлнение к Директивам по предупреждению случаев отмывания денежных средств». Данные директивы были разработаны в виде законодательных требований в соответствии с разделом 7(3) Банковских правил. Контрольные директивы предусматривают обязательное внедрение уполномоченными предприятиями эффективных систем и процедур борьбы с отмыванием денег и финансированием терроризма, и разработаны на основе современных международных стандартов, включая 40 рекомендаций ФАТФ по борьбе с отмыванием денег и 9 специальных рекомендаций ФАТФ по борьбе с финансированием терроризма. Требования, изложенные в указанных директивах, относятся к УП, выпускающим многофункциональные карты с хранимой стоимостью.

104. В соответствии с директивами ПОД/ФТ, УП обязаны *i)* обеспечить надлежащую проверку клиентов для идентификации и проверки их личности и личности бенефициарных владельцев клиентов с помощью надежного, независимого источника информации; *ii)* получить информацию о цели и предполагаемом характере деловых отношений; *iii)* осуществлять проверку юридической чистоты операций на протяжении всего периода деловых отношений. Надлежащая проверка клиентов должна осуществляться УП с использованием подхода, основанного на оценке рисков. УП обязаны разработать стратегии и процедуры начала работы с клиентами, с помощью которых можно было бы определять тех клиентов, с которыми связаны наибольшие риски ОД/ФТ. Для таких клиентов УП должны разработать более тщательную процедуру надлежащей проверки и вести тщательный мониторинг совершаемых ими операций. Для обеспечения надлежащей проверки УП должны, по возможности, проводить личное собеседование с каждым новым клиентом для того, чтобы установить его личность и получить иные важные сведения о нем. Если личное собеседование с новым клиентом провести нельзя, для снижения возможных рисков УП обязаны применять не менее эффективные методы заочной идентификации и постоянного мониторинга. В соответствии с требованиями директив ПОД/ФТ, УП также обязаны вести надлежащий учет операций.

105. В разделе 25A главы 455 Закона об организованной преступности и тяжких преступлениях (а также в аналогичных положениях гонконгских законов о противодействии финансированию терроризма) говориться о том, что все лица, проживающие в Гонконге, обязаны уведомлять Объединенное управление финансовой разведки Гонконга (ОПФР) о подозрительных операциях. Неуведомление о подозрительной операции является уголовным преступлением. Все стороны, участвующие в финансовых операциях любого типа, для соблюдения указанного Закона обязаны использовать средства, позволяющие обнаружить подозрительные операции, при этом каждая компания самостоятельно решает, какие именно средства использовать, и самостоятельно несет за них ответственность. Кроме того, в соответствии с контрольными директивами ПОД/ФТ, разработанным ВУГ, для того, чтобы иметь возможность обнаружить и сообщить о подозрительных операциях, УП следует использовать эффективные информационно-управляющие системы. В Законе об организованной преступности и тяжких преступлениях, а также в Законе о

незаконном обороте наркотиков (возврат дохода) (и в аналогичных положениях гонконгских законов о противодействии финансированию терроризма) предусмотрено предоставление в ОПФР отчетов о подозрительных операциях. Требования об уведомлении относятся к любому лицу, знающему или подозревающему о том, что какое-либо имущество является доходом, полученным в результате совершения уголовного преступления, или что это имущество использовалось в связи, или должно быть использовано в связи с совершением уголовного преступления. В этом случае такое лицо обязано при первой возможности сообщить об имеющейся у него информации или подозрении уполномоченному лицу (напр., служащему ОПФР).

106. ОПФР обеспечивает соблюдение требований, содержащихся в директивах ПОД/ФТ, за счет постоянного контроля. Если какое-либо УП оказывается не в состоянии выполнить какое-либо требование директив ПОД/ФТ, ОПФР требует от этого УП принятия мер, необходимых для исправления нарушения. При этом ОПФР проследит за тем, чтобы нарушение было надлежащим образом исправлено УП. В тех случаях, когда нарушение является серьезным, ОПФР использует имеющиеся в ее распоряжении средства контроля за деятельностью данного УП.[32]

Австралия

107. В Австралии осуществление платежей регулируются, в основном, Законом (положением) о платежных системах 1998 года, Законом о платежных системах и неттинге 1998 года и Правилами электронных переводов платежей (ЭПП). Резервный банк Австралии (РБА) следит за выполнением Закона (положения) о платежных системах 1998 года и *Закона о платежных системах и неттинге 1998 года* для обеспечения эффективности, конкурентности и стабильности. Австралийская комиссия по ценным бумагам и инвестициям следит за выполнением Правил ЭПП для защиты прав потребителей.

108. В Австралии основными законами, нацеленными на борьбу с отмыванием денег и финансированием терроризма (ПОД/ФТ), являются Закон о борьбе с отмыванием денег и финансированием терроризма (Закон ПОД/ФТ) и Правила борьбы с отмыванием денег и финансированием терроризма. В Законе ПОД/ФТ изложены общие принципы и обязательства по ПОД/ФТ. Порядок выполнения указанных обязательств подробно оговаривается в подзаконных нормативных актах, а именно, в Правилах ПОД/ФТ.

109. Закон ПОД/ФТ охватывает финансовый сектор, игорный бизнес, торговлю драгоценными металлами и любые другие компании и специалистов, оказывающих обособленные услуги (т.е. несущие в себе риски ОД/ФТ). Так как в соответствии с

---

[32] У ОПФР имеется большое количество средств контроля за деятельностью УП. Такие меры включают в себя, например, направление высшему руководству УП письменного предупреждения, введение ограничений на деятельность данного УП, понижение контрольных рейтингов УП и направление независимого ревизора для изучения средств и методов ПОД/ФТ, использующихся данным УП. Если какое-либо УП окажется не в состоянии принять меры, необходимые для исправления нарушения, ОПФР может прибегнуть к использованию официальных полномочий, имеющихся у него в соответствии с Банковских правилами, которые предусматривают, среди прочего, отзыв разрешения, предоставленного ответственным директорам и руководителям компании, выдвижение определенных условий, на которых УП может получить разрешение, выдвижение требования к УП о проведении консультаций с консультантом, назначенным ОПФР, а также приостановка действия или отзыв разрешения, выданного УП. Меры по контролю за деятельностью УП в каждом случае зависят от тяжести обнаруженных нарушений и должны быть эффективными, соразмерными проблеме и нацеленными на недопущение таких нарушений в будущем.

законодательством ПОД/ФТ такие услуги категоризируются в соответствии с видами деятельности, могущими быть связанными с отмыванием денег или финансированием терроризма, форма их оказания (электронная, бумажная, личное общение) значения не имеет.

110. Закон ПОД/ФТ налагает на предприятия, оказывающие обособленные услуги (т.н. *подотчетные организации*), определенные обязательства. Эти обязательства включают в себя меры по надлежащей проверке клиентов (идентификация, проверка личности и постоянный мониторинг операций), отчетность (подозрительные моменты, операции, превышающие установленный порог, поручения о перечисление денежных средств заграницу), ведение учетной документации, разработка и выполнение программы ПОД/ФТ.

111. Закон ПОД/ФТ предполагает использование подхода, основанного на оценке риска. Компании, для того чтобы узнать, выполняет ли она свои обязательства, нужно определить, насколько велик риск того, что обособленная услуга, оказываемая ею клиенту, может способствовать отмыванию денег или финансированию терроризма. В Правилах ПОД/ФТ указано, как именно подотчетная организация может обеспечить соблюдение своих обязательств, используя методы и средства контроля на основе оценки рисков. При выборе и внедрении необходимых методов и средств контроля подотчетная организация должна учитывать характер, размер и сложность осуществляемой ею деятельности, а также тип ОД/ФТ рисков, с которыми она может столкнуться. При определении рисков ОД/ФТ подотчетная организация также должна учитывать риск, обусловленный следующими факторами: тип клиентов (в том числе обращая внимание на то, имеются ли среди них лица, имеющие отношение к политике), тип оказываемых ею обособленных услуг, методы, используемые для их оказания, а также иностранные юрисдикции, с которыми она имеет дело.[33]

112. Австралийское управление пруденциального регулирования (АУПР) позволяет использовать для оплаты покупок через Интернет предоплаченные платежные инструменты (ППИ). ППИ, такие как, например, смарт-карты, электронные деньги, представляют собой платежные инструменты, на которые пользователи вносят деньги, чтобы потом использовать их для совершения различных платежей. Держатель хранимой денежной стоимости возвращает ее покупателям по требованию.

113. Пруденциальный норматив АУПР по ППИ предусматривает выполнение поставщиками услуг ППИ пруденциальных требований соразмерно степени риска, присущей их деятельности. Поставщик услуг ППИ не имеет права заниматься обычными банковскими операциями. В соответствии с пруденциальным нормативом, поставщик услуг ППИ обязан выполнять требования ПОД/ФТ под контролем Австралийского центра отчетов об операциях и их анализа (в соответствии с Законом по борьбе с отмыванием денег и финансированием терроризма 2006 года).

114. Организациям, занимающимся выпуском/эквайрингом (обслуживанием) кредитных карт, АУПР выдает разрешения на осуществление деятельности в качестве «специального учреждения по работе с кредитными картами» (СУРКК). СУРКК составляют отдельную категорию депозитных учреждений (ДУ), имеющих разрешение на осуществление ограниченного количества банковских операций. СУРКК могут заниматься только выпуском и/или эквайрингом кредитных карт, а также оказывать любые иные услуги, связанные с выпуском и/или эквайрингом кредитных карт. СУРКК

[33] Генеральная прокуратура [Австралии] (2007).

не имеют права принимать на хранение денежные средства (за исключением небольших остатков на счетах кредитных карт).

МЕРЫ ПО УПРАВЛЕНИЮ РИСКАМИ, ПРЕДПРИНИМАЕМЫЕ ПРЕДСТАВИТЕЛЯМИ ДАННОГО СЕКТОРА

Введение

115. Точно так же, как любым другим видам бизнеса, коммерческим Интернет-сайтам и системам Интернет-платежей присущи различные риски – начиная с рисков, связанных с защитой Интернет-сайтов от хакеров и вирусов, и заканчивая намеренным использованием Интернет-сайтов преступниками для осуществления мошеннических действий, и систем Интернет-платежей для отмывания денег и других финансовых преступлений. Соответственно, управление рисками – процесс постоянный, корректируемый поставщиками услуг коммерческих Интернет-сайтов и Интернет-платежей для минимизации текущих рисков. Для этого компании могут заключать соглашения с клиентами-пользователями, четко оговаривающих правила и политику использования клиентами соответствующих систем. Кроме того, поставщики услуг Интернет-сайтов и Интернет-платежей могут разрабатывать и внедрять передовые методы работы, определяя собственные стандарты безопасной работы и эффективного оказания услуг своим пользователям. Управление рисками также может включать в себя программы по борьбе с отмыванием денег/финансированием терроризма (программы ПОД/ФТ) – возможно, некоторые поставщики услуг Интернет-сайтов и поставщики услуг Интернет-платежей уже разработали и используют такие программы. И наконец, подход на основе риска может включать в себя и другие методы управления рисками, применение которых обусловлено законодательством какой-либо отдельной страны или юрисдикции, в которых поставщики услуг Интернет-сайтов и поставщики услуг Интернет-платежей оказывают свои услуги. Сюда, например, могут относиться требования к предоставлению отчетности (системы Интернет-платежей) и т.д. Другие заинтересованные стороны (например, налоговые органы, органы по надзору за платежами) также участвуют или должны участвовать в борьбе с отмыванием денег и финансированием терроризма и снижению рисков ОД или ФТ. Если поставщики услуг коммерческих Интернет-сайтов не имеют обязательств по предоставлению отчетности, их деятельность контролируется такими заинтересованными сторонами.

Механизмы ПОД/ФТ, используемые для снижения рисков мошеннических действий, отмывания денег и финансирования терроризма

116. Для снижения рисков ОД/ФТ поставщики услуг Интернет-платежей используют (с соблюдением требований соответствующих надзорных органов) различные механизмы. Как уже говорилось, при проведении исследования авторы настоящего отчета получили информацию об использовании таких механизмов от одного из крупнейших поставщиков услуг коммерческих сайтов-посредников в продажах от потребителя к потребителю, от одного из крупнейших поставщиков услуг Интернет-платежей, от достаточно крупной компании-эмитента электронных денег, а также от ассоциации Electronic Money Association, представляющей группу из 33 эмитентов электронных денег и поставщиков услуг Интернет-платежей. Авторы настоящего отчета также получили подтверждение тому, что нормы ПОД/ФТ, предусматривающие использование аналогичных механизмов, обязательны для исполнения поставщиками услуг Интернет-платежей в наиболее промышленно развитых странах.

117. Ниже представлен неполный список таких механизмов:

- Создание международных служб безопасности, осуществляющих надзор за сайтами для обнаружения случаев мошенничества и злоупотреблений;
- Надлежащая проверка клиентов с использованием подхода на основе оценки рисков (упрощенный/расширенный порядок надлежащей проверки клиентов);

- Оценка риска, связанного с клиентом, при открытии счета;
- Проверка предоставленной клиентами информации на основе оценки рисков (адрес электронной почты/IP-адрес, личность владельца кредитной карты, похищенные кредитные карты и т.д.);
- Звонки в автоматическом режиме, контрольное снятие средств со счета для проверки личности клиента;
- Отправка писем на адрес клиента для его проверки;
- Проверка адреса при приеме кредитных карт к оплате;
- Проверка информации, полученной от клиентов, в коммерческих базах данных;
- Ограничения по операциям, ограничения по отправке и снятию средств;
- Проверка источника финансирования;
- Проверка клиентов, их действий и продаваемых ими вещей в режиме реального времени;
- Мониторинг (с использованием разработанных моделей риска) для обнаружения противоправных действий, а также информации:
  - полученной от клиентов (личность, используемый почтовый адрес, адрес электронной почты/IP-адрес, информация на странице «Личная информация» и т.д.);
  - полученной от клиентов (звонки по телефону продавцам и т.д.);
  - полученной из собственных источников (на основании предыдущих операций, страна товара, страна клиента, используемые методы доставки, поведение клиентов во время аукциона, методы приема платежей и т.д.);
  - полученной из внешних источников (страны, характеризующиеся повышенным уровнем некоторых видов преступности, проверка списков лиц или групп лиц, могущих заниматься террористической деятельностью, и т.д.);
- Использование моделей риска для обнаружения нетипичных (по сравнению с предыдущими операциями) или масштабных операций;
- Использование моделей/программного обеспечения, позволяющего обнаружить подозрительную деятельность (с использованием различных сигналов (признаков) опасности);
- Исследование нетипичных операций и счетов с повышенной активностью в индивидуальном порядке;
- Обнаружение нетипичной или подозрительной деятельности, связанной со снятием средств со счета;
- Отказ от операций, связанных с запрещенными товарами (наркотики, огнестрельное оружие, контрафактные товары и т.д.);
- Снятие с продажи противозаконных товаров, представленных на сайте;
- Сотрудничество коммерческими компаниями для обнаружения контрафактных товаров и снятия их с продажи;
- Анализ физических и электронных улик, оставленных преступниками в сети;
- Приостановка операций;
- Ознакомление клиентов с правилами, применимыми к некоторым странам и операциям;
- Поощрение уведомлений о подозрительных товарах, выставленных на продажу, подозрительных аукционах или о подозрительном поведении клиентов (продавцов или покупателей), использование рейтингов (покупатели и продавцы выставляют друг другу оценки);
- Отказ от приема и распределения наличных;
- Ведение журналов контроля коммерческих операций и платежей.

118. Наиболее предусмотрительные поставщики услуг Интернет-платежей собирают данные и информацию о движении средств между покупателями и продавцами, находящимися в разных странах мира, но являющихся клиентами одного и того же поставщика услуг Интернет-платежей, о коммерческих операциях между покупателями и продавцами, данные и информацию за длительный период времени, которую можно получить из центральных источников.

119. Следовательно, они имеют в своем распоряжении всю информацию о движении денежных средств и о коммерческих операциях между покупателями и продавцами, в том числе в какие страны попадают перечисляемые средства, информацию, которой у банков покупателей и продавцов нет. Они легко могут восстановить порядок коммерческих операций и движения денежных средств между различными странами и лицами по всему миру.

120. Некоторые поставщики услуг Интернет-платежей имеют доступ к данным и информации о коммерческой операции, являющейся причиной движения средств, так как они предоставляют средства платежа коммерческим Интернет-сайтам, входящим в одну и ту же финансовую группу. Тем не менее, некоторые поставщики услуг Интернет-платежей, предоставляющие средства платежа коммерческим Интернет-сайтам, не входящим в одну и ту же финансовую группу, также могут получить информацию, хотя и несколько ограниченную, о сделках, лежащих в основе движения денежных средств.

121. Простота обмена информацией с коммерческими Интернет-сайтами снижает риски злоупотреблений и риски ОД/ФТ.

122. Если поставщики услуг Интернет-платежей обеспечат надлежащий мониторинг финансовых операций своих клиентов, реагируя на отклонения от сложившейся модели поведения клиента, то недостаток личного контакта, имеющийся в начале взаимоотношений с поставщиком услуг коммерческого Интернет-сайта и поставщиком услуг Интернет-платежей, может перестать быть проблемой.

123. Стоит, тем не менее, заметить, что поставщик услуг Интернет-платежей, сможет создать гораздо более точную модель операций клиента, если количество таких операций будет достаточно большим.

124. Обмену информацией между поставщиками услуг коммерческих Интернет-сайтов и поставщиками услуг Интернет-платежей из разных стран иногда препятствуют различия в законах, защищающих частную жизнь граждан.

125. Как уже говорилось в разделе о нормативно-правовом регулировании, обязательства по предоставлению отчетности ПОД/ФТ поставщиками услуг Интернет-сайтов и поставщиками услуг Интернет-платежей зависят от того, в какой стране они находятся физически. Некоторые поставщики услуг Интернет-сайтов и поставщики услуг Интернет-платежей тесно сотрудничают с правоохранительными органами. Они способствуют вовлечению регуляторных и правоохранительных органов в активную борьбу с использованием коммерческих Интернет-сайтов и систем Интернет-платежей в преступных целях.

НЕКОТОРЫЕ ЗАМЕЧАНИЯ О СРЕДСТВАХ КОНТРОЛЯ ВТОРОГО И ТРЕТЬЕГО УРОВНЕЙ

126. Поставщики услуг Интернет-сайтов и поставщики услуг Интернет-платежей, имеющие лицензию на работу в качестве банка или поставщиков услуг электронных денег, имеют несколько обязательств, связанных с идентификацией клиентов, обнаружением, мониторингом и уведомлением о подозрительных финансовых операциях. Как говорилось в предыдущем разделе, у них есть возможность доступа к большому количеству информации для мониторинга операций своих клиентов, и некоторые поставщики услуг Интернет-платежей внедрили механизмы надлежащей проверки клиентов, применяющиеся на постоянной основе и предполагающие тщательную проверку операций клиента на протяжении всего периода работы с ним на соответствие сложившейся модели его поведения. Во многих случаях модель поведения клиента можно создать только на основе предшествующих операций с поставщиком услуг Интернет-платежей.

127. Банки покупателей и продавцов, пользующиеся услугами поставщиками услуг Интернет-платежей, не видят всей картины движения средств между покупателем и продавцом, так как соответствующая информация известна только поставщику услуг Интернет-платежей. Клиент банка может попросить свой банк перевести средства с его банковского счета на его счет у поставщика услуг Интернет-платежей. После этого клиент попросит поставщика услуг Интернет-платежей перевести эти средства на коммерческий Интернет-сайт для оплаты товара. Банк может не иметь абсолютно никакой информации об этой покупке и о причинах перевода средств на счет поставщика услуг Интернет-платежей. Установлено, что подобные случаи происходили в США: клиенты поручали своим банкам перечислить средства поставщику услуг Интернет-платежей, после чего использовали эти средства на игорных сайтах, оставляя таким образом банк в неведении относительно того, что средства были использованы в США в нарушение законов страны.

128. Однако банки по-прежнему играют важную роль в процессе мониторинга и обнаружения подозрительных сделок – даже в тех случаях, когда средства перечисляются поставщику услуг Интернет-платежей или самим поставщиком услуг Интернет-платежей. Например, банки в состоянии определить, что та или иная операция является нетипичной или несоразмерной сложившейся модели поведения клиента (профессиональная деятельность, доходы от профессиональной деятельности, типичные банковские операции).

129. Также важно и то, что финансовые учреждения, такие как, например, банки, не пытаются уйти от своих обязательств по ПОД/ФТ, в частности, от обязательств по обнаружению подозрительных финансовых операций с перечислением средств от поставщика услуг Интернет-платежей – даже если перечисляемые суммы относительно невелики. Выписка или распечатка с экрана монитора с изображением коммерческого Интернет-сайта, на котором, например, изображен выставленный на продажу товар, не должна немедленно и безоговорочно рассматриваться как счет-фактура или документ, объясняющий происхождение средств, перечисленных на банковский счет клиента. И наоборот - если для того, чтобы объяснить происхождение средств, представлен такой документ, то финансовое учреждение может рассматривать его в качестве сигнала (признака) опасности.

ВЫВОДЫ, КОТОРЫЕ ДОЛЖНЫ БЫТЬ УЧТЕНЫ ПРИ РАЗРАБОТКЕ НЕОБХОДИМЫХ СТРАТЕГИЙ

130. В данном отчете был сделан анализ рисков ОД/ФТ, связанных с коммерческими Интернет-сайтами и системами Интернет-платежей, при этом основное внимание было уделено такому виду электронной торговли, который, по различным причинам (растущая популярность, легкость доступа, доступность для широкой публики, большой объем трансграничных торговых сделок и т.д.), считается самым уязвимым для преступной деятельности, связанной с ОД/ФТ, а именно, торговле через сайты-посредники в продажах от потребителя к потребителю.

Основные выводы

131. Преступные элементы успешно находят новые каналы для финансирования терроризма и отмывания денежных средств, получаемых ими в результате незаконной деятельности. По мере распространения Интернета по миру выясняется, что коммерческим Интернет-сайтам и системам Интернет-платежей присущи многие риски и что они имеют множество уязвимых мест, позволяющих преступным организациям и террористическим группировкам использовать их в своих целях.

132. Были рассмотрены различные уязвимые места коммерческих Интернет-сайтов и систем Интернет-платежей: заочная регистрация, могущая стать причиной проблем с идентификацией клиента, скорость совершения сделок, меньший объем и большое количество сделок, что может привести к проблемам с отслеживанием, мониторингом и обнаружением операций; глобальный характер сети Интернет, в результате чего могут возникать проблемы с подсудностью; сложность мониторинга и обнаружения подозрительных финансовых операций традиционными финансовыми учреждениями, которые могут оказаться не столь эффективными в тех случаях, когда сделка осуществляется с участием поставщика услуг Интернет-платежей.

133. Некоторые риски ОД/ФТ, связанные с отмыванием денег с помощью торговых операций и заочными коммерческими и финансовыми сделками, также присущи коммерческим Интернет-сайтам и системам Интернет-платежей. Финансовые операции, осуществляемые через банковский счет или кредитную карту (два наиболее распространенные метода Интернет-платежей) предусматривают удостоверение личности клиента, сохранение информации об операциях и предоставление отчетности. Риск, связанный с операциями на небольшие суммы, далеко не всегда бывает небольшим, поэтому для снижения риска к таким операциям должны применяться регулятивные меры, которые используются в финансовом секторе. В той части исследования, которая относится к рискам, связанным с заочной регистрацией и анонимностью пользователей, говорится о необходимости поиска решений, обеспечивающих удостоверение личности в режиме онлайн (например, с помощью электронных карт-удостоверений личности, использующихся в некоторых странах), позволяющих снизить риски преступной деятельности, которым подвержены поставщики услуг Интернет-сайтов и поставщики услуг Интернет-платежей. В отчете также говорится о том, что если поставщики услуг Интернет-платежей обеспечат надлежащий мониторинг финансовых операций своих клиентов, следя за отклонениями от сложившейся модели поведения клиента и адекватно на них реагируя, то недостаток личного контакта, имеющийся в начале взаимоотношений с поставщиком услуг коммерческого Интернет-сайта и поставщиком услуг Интернет-платежей, может

перестать быть проблемой. Лица, осуществляющие торговые операции через Интернет, и лица, осуществляющие такие торговые операции традиционными методами, должны иметь сопоставимые объемы обязательств по ПОД/БФ.

134. Также важно добиться того, чтобы у поставщиков услуг коммерческих Интернет-сайтов и у поставщиков услуг Интернет-платежей из разных стран, противодействующих мошенничеству и ОД/ФТ, не возникало сложностей из-за несогласованности законов о защите частной жизни, ограничивающих объемы информации о клиентах, которой могут обмениваться поставщики услуг по операциям, могущим быть связанными с ОД/ФТ.

135. Требования по обнаружению операций, связанных с финансированием терроризма (в основном, с помощью сопоставления имен клиентов с именами, предоставленными компетентными органами), предъявляются ко всем системам Интернет-платежей в равной мере, при этом поставщики услуг Интернет-платежей, в своих сообщениях о подозрительных операциях (СПО), предоставляемых в рамках содействия борьбе с финансированием терроризма, не всегда обязаны указывать, что та или иная деятельность, по их мнению, связана с финансированием терроризма. Важно сообщать о любой подозрительной деятельности независимо от ее типа. Некоторые поставщики услуг Интернет-платежей начали внедрять и использовать системы обнаружения, мониторинга и анализа подозрительных операций, в том числе операций с небольшими суммами денег.

136. Говоря о подходе к борьбе с ОД/ФТ, основанном на оценке рисков, следует упомянуть Рекомендации ФАТФ (июнь 2007 года), в которых сказано следующее: «При использовании подхода на основе оценки рисков компетентные органы и финансовые учреждения смогут обеспечить соразмерность мер, предпринимаемых для профилактики или снижения объемов отмывания денег и финансирования терроризма, тем рискам, которые были определены. Это позволит распределять имеющиеся ресурсы наиболее эффективным способом. Принцип наиболее эффективного распределения ресурсов предполагает распределение на основе приоритетности – наибольшее внимание должно уделяться наибольшим рискам». Применяя данный принцип к операциям, осуществляемым через Интернет, представители частного сектора будут рассматривать мелкие платежи, совершаемые через финансовые учреждения или счета кредитных карт (что предполагает идентификацию и проверку личности клиента, а также учет и отчетность) в качестве операций, риск по которым будет меньше, чем по операциям, осуществляемым с помощью поставщиков услуг, не имеющих обязательств по борьбе с отмыванием денег и с финансированием терроризма (ПОД/ФТ).

137. Риск мошенничества и продаж незаконных товаров являются для поставщиков услуг коммерческих Интернет-сайтов и поставщиков услуг Интернет-платежей еще одним поводом для беспокойства, заставляющим их принимать меры для защиты передаваемой ими информации, имеющихся у них Интернет-сайтов и систем Интернет-платежей. В некоторых странах никаких официальных требований, связанных с обнаружением и борьбой с ОД/ФТ, поставщикам услуг коммерческих Интернет-сайтов не предъявляется – для этого используются рыночные стимулы.

138. Некоторые поставщики услуг коммерческих Интернет-сайтов и поставщики услуг Интернет-платежей, знающие о рисках, связанных с возможностью использования имеющихся у них ресурсов для незаконной деятельности, открыли специальные подразделения, занимающиеся мониторингом и анализом операций своих клиентов на основе подхода, предполагающего оценку рисков. Некоторые поставщики услуг Интернет-сайтов и поставщики услуг Интернет-платежей, в дополнение к использующимися ими средствами мониторинга случаев мошенничества, также

внедрили механизмы ПОД/ФТ. Использование передовых методов работы (таких как, например, методы надлежащей проверки клиентов, мониторинг операций, отказ от анонимных платежей (например, платежей наличными), введение ограничений на размер операций, ведение учетной документации по осуществляемым операциям, уведомление компетентных органов о крупных или подозрительных операциях) также может оказаться эффективным средством противодействия ОД/ФТ.

139. Сотрудничество между поставщиками услуг коммерческих Интернет-сайтов и поставщиками услуг Интернет-платежей с целью обмена информацией о коммерческих операциях, являющихся причиной финансовых сделок, позволяет снизить риски ОД/ФТ и мошенничества. Правовое стимулирование обмена такой информацией может оказаться весьма полезным.

140. В настоящем отчете сделан следующий вывод: до тех пор, пока представители данного сектора и соответствующие компетентные органы знают и понимают, какие составляющие коммерческих Интернет-сайтов и систем Интернет-платежей являются потенциально уязвимыми, и какие меры (с учтем возможных рисков) необходимо принять для обеспечения идентификации клиента, ведения учетной документации и предоставления необходимой отчетности, риски, связанные с операциям через Интернет, не обязательно будут превышать риски, связанные с традиционными (несетевыми) финансовыми операциями.

141. Составители отчета полагают, что, несмотря на то, что благодаря усилиям регулятивных органов и профессиональных объединений уровень осведомленности об ОД/ФТ среди ключевых игроков в сфере Интернет-бизнеса постоянно повышается, необходимо принимать дальнейшие меры по повышению уровня осведомленности, особенно в отношении того, что касается механизмов борьбы с ОД/ФТ.

142. Учитывая глобальный характер коммерческих Интернет-сайтов, международное сотрудничество является залогом успешной борьбы с отмыванием денег и финансированием терроризма. Поэтому важно наладить сотрудничество между ПФР, правоохранительными органами и другими заинтересованными сторонами. Поставщики услуг Интернет-платежей предоставляют отчетность в той стране, в которой была учреждена их компания (в которой они получили лицензию), а не в странах, в которых проживают лица, имеющие отношение к подозрительным операциям. А это может создавать для ПФР и правоохранительных органов сложности, связанные с идентификацией и последующим контролем таких лиц (сложно установить истинные личности сторон, участвующих в операциях в стране предоставления отчетности, учитывая, что эти лица в этой стране не живут, а сами операции трудно объяснить/обосновать, так как они осуществляются за пределами страны, в которой находится и предоставляет отчетность поставщик услуг Интернет-платежей).

Задачи, на решение которых необходимо обратить внимание

143. В настоящем исследовании определены некоторые задачи, решение которых позволит усовершенствовать механизмы снижения рисков ОД/ФТ, присущих коммерческим Интернет-сайтам и системам Интернет-платежей.

144. **Повышение уровня осведомленности:** Повышение уровня осведомленности представителей государственных органов и частного сектора о рисках ОД/ФТ имеет первостепенное значение. Также важно объяснить традиционным финансовым учреждениям ту роль, которую они играют в обнаружении и мониторинге подозрительных финансовых операций. Для этого они должны уметь использовать сигналы (признаки) опасности и знать о существующих способах ОД/ФТ. Уровень осведомленности также можно повышать с помощью учебных программ и специальных занятий с представителями частного сектора. Регулятивные органы и профессиональные объединения, занимавшиеся разработкой рекомендаций по ПОД/ФТ и типизацией способов ОД/ФТ, также могут оказать большую помощь.

145. **Внедрение единообразных законов**: Учитывая глобальный характер сети Интернет и его доступность, сложно определить, в каком месте или стране находится регулятивный орган, имеющий право регламентировать деятельность поставщиков услуг Интернет-платежей, и каким образом осуществлять принудительное обеспечение правопорядка в случае возможных нарушений. Поставщики услуг Интернет-платежей, осуществляющие свою деятельность в глобальном масштабе, расположены и имеют лицензии, выданные в разных странах и регионах. Поэтому важно, чтобы во всех странах принимались схожие законы, предусматривающие обязательную идентификацию клиента, надлежащую проверку клиента, ведение учетной документации и предоставление отчетности – в противном случае некоторые поставщики услуг Интернет-платежей могут выбрать страну с самым несовершенным законодательством или страну, в которой такая деятельность вообще не регламентируется.

146. **Изучение передовых методов работы:** Информация о стандартах надлежащей проверки клиентов и передовых методов работы (мониторинг операций, отказ от некоторых видов платежей (например, платежей наличными), считающихся высокорисковыми с точки зрения ОД/ФТ, введение ограничений на размер операций и т.д.), определенных участниками семинара и представленных в настоящем отчете, может оказаться полезной для других представителей частного сектора и может использоваться в качестве одной из основных составляющих учебных программ и специальных занятий с представителями частного сектора.

147. **Значение международного сотрудничества**: Учитывая глобальный характер деятельности, связанной с использованием сети Интернет и коммерческих Интернет-сайтов, международное сотрудничество является ключевым условием успешной борьбы с ОД и ФТ. Борьба с использованием коммерческих Интернет-сайтов для ОД/ФТ должна вестись компаниями сообща. Международное сотрудничество в части обеспечения надлежащего регулирования и мониторинга деятельности компаний, работающих в нескольких юрисдикциях, также очень важно.

148. Необходимо обратиться в Международную организацию органов финансовой разведки «Эгмонт» для обсуждения мер по повышению уровня осведомленности ПФР о методах борьбы с использованием коммерческих Интернет-сайтов и систем Интернет-платежей для отмывания денег и финансирования терроризма и заявить о необходимости поиска способов, с помощью которых ПФР смогут увеличить объемы обмена информацией и данными об использовании коммерческих Интернет-сайтов и систем Интернет-платежей в преступных целях.

СПИСОК ЛИТЕРАТУРЫ

[Australian] Attorney-General's Department (2007), *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)*, accessed through: www.comlaw.gov.au

FATF (2006a), *Report on New Payments Methods*, FATF, Paris, www.fatf-gafi.org

FATF (2006b), *Trade-based Money Laundering*, FATF, Paris, www.fatf-gafi.org

FATF (2007), Guidance on the Risk-Base Approach to Combating Money Laundering and Terrorist Financing, High Level Principles and Procedures, FATF, Paris, www.fatf-gafi.org

Federal Trade Commission (2007a), "*About the Bureau of Consumer Protection*", Federal Trade Commission web site, www.ftc.gov/bcp/about.shtm

Federal Trade Commission (2007b), "*Division of Enforcement*", Federal Trade Commission web site, www.ftc.gov/bcp/about.shtm

Monetary Authority of Singapore, (2006), "*Stored Value Facilities Guidelines"*, accessed at: www.mas.gov.sg/resource/legislation_guidelines

Monetary Authority of Singapore (2007), *Prevention of Money Laundering and Countering of Terrorism – Holders of Stored Value Facilities,* Notice PSOA-No.2, Singapore, accessed at: www.mas.gov.sg/resource/legislation_guidelines

Monetary Authority of Singapore Act (Chapter 186), http://agcvldb4.agc.gov.sg/non_version/cgi-bin/cgi_retrieve.pl?actno=REVED-186&doctitle=MONETARY%20AUTHORITY%20OF%20SINGAPORE%20ACT%0a&date=latest&method=part

Munro, Neil (2001), "*Internet-Based Financial Services: A New Laundry?", Journal of Financial Crime*, Henry Stewart Publications, Vol. 9, No. 2, pp. 134-152, Henry Stewart Publications

Philippsohn, Steve (2001), "*The Dangers of New Technology – Laundering on the Internet", Journal of Money Laundering Control*, Henry Stewart Publications, Vol. 5, No. 1, pp. 87-95

[Singapore] *Payment Systems (Oversight) Act 2006 (PS(O)A)* accessed at: *www.mas.gov.sg/legislation_guidelines/payment_system/payment_act2006/Payment_Systems_Oversight_Act_2006.html.*