



РУКОВОДСТВО ФАТФ

ОБМЕН ИНФОРМАЦИЕЙ В ЧАСТНОМ СЕКТОРЕ

НОЯБРЬ 2017





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

Подробная информация о ФАТФ размещена на сайте: www.fatf-gafi.org

Данный документ и любые прилагаемые схемы не ограничивают статус или суверенитет никаких территорий, не противоречат определению межгосударственных границ и наименований любых территорий, городов или областей.

© FATF/OECD. All rights reserved, 2017

© ФАТФ/ОЭСР. Все права защищены, 2017

Неофициальный перевод подготовлен и опубликован ЕАГ совместно с
Международным учебно-методическим центром финансового
мониторинга согласно письменному разрешению ФАТФ

Оригинал документа опубликован по ссылке:
www.fatf-gafi.org/media/fatf/documents/recommendations/Private-Sector-Information-Sharing.pdf

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

Photocredits coverphoto: ©Thinkstock

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	4
ПРЕДПОСЫЛКИ И КОНТЕКСТ	4
НАЗНАЧЕНИЕ, ЦЕЛЕВАЯ АУДИТОРИЯ, СОДЕРЖАНИЕ И СТАТУС ДАННОГО РУКОВОДСТВА	5
ОБЩИЕ ВОПРОСЫ ОБМЕНА ИНФОРМАЦИЕЙ.....	7
А. Юридические вопросы	7
В. Операционные препятствия.....	9
С. Вызовы для надзорных органов	10
ОБМЕН ИНФОРМАЦИЕЙ В СООТВЕТСТВИИ С РЕКОМЕНДАЦИЯМИ ФАТФ	11
А. Обмен информацией в рамках финансовых групп	11
В. Обмен информацией о подозрении в незаконном происхождении денежных средств или их связи с финансированием терроризма в рамках финансовой группы	19
С. Конфиденциальность и разглашение СПО, а также их влияние на обмен информацией в группе.....	21
ИНФОРМАЦИОННЫЙ ОБМЕН МЕЖДУ КРЕДИТНО- ФИНАНСОВЫМИ УЧРЕЖДЕНИЯМИ, ОТНОСЯЩИМИСЯ К РАЗНЫМ ГРУППАМ	27
А. Информационный обмен в соответствии с Рекомендациями ФАТФ ..	27
НОВОЕ В ИНФОРМАЦИОННОМ ОБМЕНЕ	32
Информационный обмен, выходящий за рамки Рекомендаций ФАТФ.....	32
РУКОВОДЯЩИЕ УКАЗАНИЯ И ОБРАТНАЯ СВЯЗЬ.....	38
ВЫВОДЫ	39
ПРИЛОЖЕНИЕ 1. РАЗЛИЧИЯ РЕЖИМОВ DRR И ИХ ПРИМЕНЕНИЕ.....	41
ПРИЛОЖЕНИЕ 2 – ПОКАЗАТЕЛЬНЫЕ ПРИМЕРЫ ИЗ ПРАКТИКИ	45

ВВЕДЕНИЕ

ПРЕДПОСЫЛКИ И КОНТЕКСТ

1. Эффективный обмен информацией – один из фундаментальных компонентов отлаженной системы ПОД/ФТ. Конструктивный и своевременный обмен информацией является ключевым требованием стандартов ФАТФ, которое фигурирует сразу в нескольких Рекомендациях и Непосредственных результатах. Финансовым учреждениям не должно необоснованно создаваться препятствий для обмена информацией в контексте управления рисками ОД/ФТ.
2. Обмен информацией в сфере ПОД/ФТ в таких финансовых учреждениях как банки может происходить на различных уровнях одной и той же группы. Другие финансовые учреждения, такие как поставщики услуг по переводу денег и ценностей (действующие преимущественно через агентов или иные каналы сбыта), могут иметь иные бизнес-модели и структуры. Основная задача эффективного обмена информацией относится ко всем таким финансовым учреждениям, действующим в различных структурах.
3. Обмен информацией происходит также между различными организациями и секторами, например, между финансовыми учреждениями, не входящими в одну и ту же группу, и государственными секторами, и наоборот. Поток информации может существовать в пределах страны или выходить за ее границы. Обмен информацией между государственными организациями не менее важен и является значимым фактором эффективности внутреннего режима координации и сотрудничества.
4. Обмен информацией крайне важен для противодействия отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения. В транснациональных схемах отмывания денег государственные границы не соблюдаются. Препятствия для обмена информацией могут негативно отразиться на эффективности мер ПОД/ФТ и даже облегчить деятельность преступных сетей. Это еще раз говорит о важности быстрого, значимого и комплексного обмена информацией из самых разных источников как в пределах страны, так и в международном масштабе.
5. Обмен информацией играет ключевую роль в обеспечении финансовой прозрачности и добросовестности финансовой системы за счет предоставления финансовым учреждениям и соответствующим компетентным органам информации и аналитических данных, необходимых для предотвращения и пресечения ОД/ФТ. В свою очередь, финансовым учреждениям пригодится информация государственного сектора об анализе тенденций, моделях поведения,

подозрительных лицах или географических уязвимостях — она поможет им лучше управлять рисками, контролировать свои потоки транзакций и передавать более полезные данные правоохранительным органам. Учреждения государственного и частного секторов могут быть как источником, так и получателем информации. Подобное использование данных подчеркивает важность непрерывного диалога между государственным и частным сектором. Кроме того, зависимость от такой информации указывает на повышение внимания международных мер к выявлению потенциальных препятствий для обмена информацией, способных негативно отразиться на эффективности системы, и поиску возможных политических и операционных решений для их устранения.

6. В июне 2016 года ФАТФ опубликовала Консолидированные стандарты по обмену информацией¹, которые содержат выдержки из Рекомендаций ФАТФ и Пояснительных примечаний, относящиеся к обмену информацией. Консолидация действующих стандартов без каких-либо поправок была сделана для экономии времени и сил и для разъяснения требований в отношении обмена информацией, рассредоточенных между 25 из Рекомендаций ФАТФ и затрагивающих 7 Непосредственных результатов в Методологии ФАТФ по оценке эффективности. Этот документ служит отправной точкой для решения вопросов, рассматриваемых в данном документе.

НАЗНАЧЕНИЕ, ЦЕЛЕВАЯ АУДИТОРИЯ, СОДЕРЖАНИЕ И СТАТУС ДАННОГО РУКОВОДСТВА

7. Назначение данного Руководства:

- i. указать на пользу обмена информацией между организациями частного сектора (в частности, финансовыми учреждениями) для повышения эффективности предпринимаемых ими мер по предотвращению ОД/ФТ;
- ii. выделить основные препятствия для обмена информацией в пределах группы компаний и между финансовыми учреждениями, не входящими в одну и ту же группу;
- iii. разъяснить стандарты ФАТФ по обмену информацией: а) в отношении и в контексте программ ПОД/ФТ – обмен информацией о подозрительных транзакциях в рамках группы и влияние положений о конфиденциальности ОПТ и разглашении на такой обмен; б) между финансовыми учреждениями, не входящими в одну и ту же группу;
- iv. продемонстрировать примеры сотрудничества между органами по защите данных и конфиденциальности и по ПОД/ФТ с целью решения взаимоисключающих задач в разных странах;

¹ Единые стандарты ФАТФ по обмену информацией

Руководство ФАТФ

v. привести примеры содействия обмену информацией в рамках группы и между финансовыми учреждениями, не входящими в одну и ту же группу, и конструктивного взаимодействия между государственным и частным секторами в разных странах;

vi. поддержать эффективную реализацию ПОД/ФТ за счет обмена информацией как в государственном, так и в международном контексте.

8. Целевая аудитория данного Руководства:

i. страны и их государственные компетентные органы, ответственные за ПОД/ФТ;

ii. организации частного сектора, включая финансовые учреждения, имеющие обязательства по программам ПОД/ФТ в рамках группы или осуществляющие клиентские транзакции с другими учреждениями;

iii. государственные и наднациональные органы защиты данных и конфиденциальности (data protection and privacy, DPP).

9. В данном документе описываются проблемы обмена информацией и приводятся рекомендации по обмену информацией в контексте группы и между финансовыми учреждениями, не входящими в одну и ту же группу. В Приложении 1 показано, как различия в режимах DPP и их применении могут влиять на поток информации. В Приложении 2 приводятся примеры и принятые в разных странах подходы к решению некоторых из этих проблем, включая совместную работу государственных органов DPP и ПОД для решения их соответствующих задач. Там же представлены инновационные разработки, принятые странами для содействия обмену информацией в рамках группы и между финансовыми учреждениями, не входящими в одну и ту же группу. Кроме того, в этом разделе приводятся примеры устоявшихся механизмов и процессов по инструктированию и получению обратной связи от частного сектора, упрощающих обмен информацией между всеми заинтересованными лицами. Следует отметить, что эти примеры приводятся только для справки. Они имеют сугубо иллюстративный характер и не могут считаться рекомендованными ФАТФ. В примерах содержатся перекрестные ссылки на соответствующие разделы данного Руководства. Рассматривая общие принципы, изложенные в Руководстве, государственные органы власти должны принимать во внимание национальные особенности и нормативно-правовую базу своей страны. Данное Руководство не имеет обязательной силы, но опирается на опыт стран и частного сектора и может помочь компетентным органам и финансовым учреждениям в эффективной реализации некоторых из Рекомендаций ФАТФ.

ОБЩИЕ ВОПРОСЫ ОБМЕНА ИНФОРМАЦИЕЙ

10. Обмен информацией крайне важен для того, чтобы финансовые учреждения, а также надзорные и правоохранительные органы могли лучше распределять ресурсы в риск-ориентированном подходе и внедрять инновационные методы противодействия ОД/ФТ. С учетом размеров и географического охвата международной финансовой системы успешная реализация мер по выявлению и предотвращению ОД/ФТ невозможна без усовершенствования координации и сотрудничества между всеми заинтересованными лицами. Улучшение обмена информацией – ключевой элемент сотрудничества между странами, между членами одной и той же финансовой группы, между различными финансовыми группами и между частным и государственным секторами.

11. Усовершенствования в обмене информацией также важны для того, чтобы в полной мере применить все возможные улучшения в средствах защиты ПОД/ФТ и получить доступ к финансовым услугам, обусловленным новыми технологиями и бизнес-моделями. При этом сохраняются препятствия для эффективного обмена информацией, которые могут задержать прогресс и создать правовые и нормативные неопределенности. Обнаруженные проблемы обсуждаются ниже.

А. Юридические вопросы

12. Юридические ограничения могут препятствовать доступности, предоставлению, получению и обработке информации для целей ПОД/ФТ. Это может быть связано с различными политическими задачами, сохранением конфиденциальности клиентских данных и требованиями о хранении документации. В некоторых случаях регулируемые организации не понимают, разрешен ли обмен информацией соответствующим правовым режимом, что ее затрудняет. В связи с этим странам необходимо решить эти вопросы и внедрить эффективный режим обмена информацией, определяющий применение различных правовых норм в данном контексте, предоставив соответствующее разъяснительное руководство к своим законам и положениям и устранив, таким образом, все неясности в этой сфере.

13. Проблемы могут быть в частности вызваны следующими моментами:

i. Различные правовые системы защиты данных и конфиденциальности (DPP) и их реализация

14. В любой юрисдикции законы и положения о ПОД/ФТ принимаются с целью предотвращения, обнаружения, пресечения, расследования и уголовного преследования ОД/ФТ. Каждый человек имеет право на конфиденциальность и

Руководство ФАТФ

защиту его персональных данных². Это право является фундаментальным во многих юрисдикциях и представляет собой важную политическую задачу в соответствии с фундаментальными принципами внутреннего права. Цели ПОД/ФТ также служат решению важных задач национальной безопасности и государственных интересов и должны выполняться тщательно, но без ущемления права граждан на защиту их персональных данных и конфиденциальности. Цели политик ПОД/ФТ и DPP не являются взаимоисключающими и должны признавать, поддерживать друг друга и находиться в балансе.

15. Различия в законах юрисдикций о DPP могут создавать сложности, в частности, затруднять обмен информацией для частного сектора. Ситуация усугубляется, если в стране отсутствуют методические рекомендации или нет единообразия в соблюдении требований о ПОД/ФТ и исполнении обязательств по DPP. Презюмированный конфликт между задачами ПОД/ФТ и DPP может быть связан с отсутствием адекватной координации между различными органами власти на этапе нормотворчества, а значит и необходимого баланса между защитой данных с одной стороны и предотвращением или пресечением преступлений с другой. Видимая сложность различных методов DPP, боязнь штрафных санкций и избегание риска в значительной мере уменьшают доступность, предоставление и получение информации частным сектором даже в тех случаях, когда обмен информацией разрешен.

16. Несмотря на то, что в некоторых ситуациях органы защиты данных стараются оказывать поддержку государственным органам власти и заинтересованным лицам из частного сектора, во множестве случаев пригодились бы более ясные инструкции национальных регулирующих органов и государственных органов власти по эффективной работе с различными нормативными требованиями. Например, международным финансовым учреждениям, функционирующим в различных юрисдикциях, пригодились бы четкие инструкции и руководства от органов защиты данных о том, какая степень международного обмена персональными данными для целей ПОД/ФТ допускается в соответствии с государственными интересами или иными условиями различных положений о защите передаваемых данных (например, в какой степени допустима передача данных в целях соблюдения требований ПОД/ФТ).

17. Страны должны изучить свое национальное законодательство и, если это необходимо для достижения баланса, внести в него поправки и (или) разъяснения. Будет хорошо, если государственные органы власти, ответственные за защиту

² Под персональными данными понимается любая информация, связанная с физическим лицом, которого можно прямо или косвенно идентифицировать по таким признакам, как имя, идентификационный номер, данные о местонахождении, онлайн-идентификатор или один или несколько факторов, характерных для физической, психологической, генетической, психической, экономической, культурной или социальной идентичности этого физического лица.

данных и конфиденциальность и за ПОД/ФТ, вступят в диалог и примут совместимые последовательные политики, позволяющие финансовым учреждениям соблюдать законодательные требования. Кроме того, государственные органы власти могут рассмотреть возможность проведения анализа национальных законов и положений с целью повышения эффективности обмена информацией и распространения результатов такого анализа (*пункты 3-7 и Приложение 2*).

ii. Положения о защите тайны финансовых учреждений

18. Препятствовать обмену информацией могут законы о защите тайны финансовых учреждений. Например, тайну финансовых учреждений, в зависимости от национального законодательства, могут не отменять «законный интерес» или соображения безопасности. В этом отношении следует отметить, что по Рекомендации 9 страны должны следить за тем, чтобы законы о тайне финансовых учреждений не препятствовали выполнению Рекомендаций ФАТФ.

В. Операционные препятствия

19. Операционные препятствия могут возникать на институциональном и (или) на государственном уровне. Своевременный обмен информацией может затрудняться возможностями ИТ и процедурами ведения документации в финансовых учреждениях. Например, некоторые сведения о клиентах, необходимые для проведения НПК, могут отсутствовать в системах ПОД/ФТ финансовых учреждений из-за того, что собирались для другой цели. Правила аутсорсинга, регулирующие объем работ, который может быть централизован за рубежом, и наоборот, данные или требующие этих данных правила о выполнении работ и сохранении ИТ-системы и операционных процессов внутри страны могут создавать ограничения, усложняющие работу и вызывающие фрагментацию процессов.

20. Препятствовать обмену информацией, даже если она доступна, могут неподходящие средства ИТ, различные форматы данных, отсутствие политик и процедур по работе с доступной информацией и общее непонимание ее ценности как в государственном, так и в частном секторе. Проблемы возможностей и интеграции ИТ могут также возникать, когда финансовые учреждения расширяются, приобретая новые предприятия, и должны интегрировать различные ИТ-системы в уже существующие организации.

21. В некоторых случаях обмен информацией между государственным и частным секторами, а также между частными организациями происходит по установленным шаблонам, позволяющим использовать автоматический анализ и сбор информации. Шаблоны могут быть достаточно гибкими для того, чтобы

Руководство ФАТФ

принимать во внимание и другие релевантные данные (такие как IP-адреса, номера телефонов, имена пользователей, должности, организации и т. д.), доступные финансовым учреждениям. Стандартизация форматов данных способствует интеграции и, таким образом, способствует обмену данными.

С. Вызовы для надзорных органов

22. Для надзорных органов недостаточный обмен информацией может затруднять осуществление консолидированного надзора в целях ПОД/ФТ (к примеру, в соответствии с требованиями Рекомендации 26). Например, в случае, если финансовое учреждение имеет сеть филиалов или подразделений в нескольких странах, законы принимающей страны (применимые к таким филиалам или подразделениям) могут не разрешать надзорным органам страны происхождения доступ ко всей информации о клиентах, хранящейся в таких филиалах или подразделениях. В связи с этим может возникнуть необходимость в отдельных соглашениях между надзорными органами страны происхождения и принимающей страны, по которым первые смогут проверять данные клиентов от имени вторых. Это может препятствовать своевременному, всестороннему анализу документации и эффективному применению надзора за группой компаний в целях ПОД/ФТ³.

23. Таким образом, надзорные органы должны стимулировать заключение двусторонних и многосторонних соглашений, поддерживающих обмен информацией для целей ПОД/ФТ и определяющих, какая информация должна предоставляться в процессе консолидированного надзора или надзора за группой компаний, и в какие сроки. Несмотря на то, что подобные соглашения не устраняют юридические преграды для обмена информацией, в случае, если консолидированный надзор за деятельностью группы затруднен по каким-либо причинам (включая отсутствие доступа к необходимой информации) или группа подвергается чрезмерным рискам, а надлежащее управление этими рисками не производится, надзорный орган страны происхождения может ограничить виды деятельности, которыми имеет право заниматься эта группа, и подвергнуть ее расширенным надзорным мероприятиям, в т. ч. потребовать от финансовой группы закрытия зарубежных предприятий в экстренных случаях.

³ Обязательный критерий 8 Основного принципа 13 БКБН (взаимоотношения между страной происхождения и принимающей страной) гласит, что надзорным органам страны происхождения должен быть предоставлен непосредственный доступ к местным представительствам и подразделениям банковской группы, позволяющий им оценить безопасность и надежность этой группы, а также соблюдение требований о надлежащей проверке клиентов.

**ОБМЕН ИНФОРМАЦИЕЙ В СООТВЕТСТВИИ С РЕКОМЕНДАЦИЯМИ
ФАТФ**

24. В этом разделе изложены основные Рекомендации ФАТФ (Рекомендации 18, 20 и 21) и их требования в контексте обмена информацией в рамках финансовой группы. Здесь же рассматривается обмен информацией между финансовыми учреждениями, не входящими в одну и ту же финансовую группу, в соответствии с Рекомендациями ФАТФ.

А. Обмен информацией в рамках финансовых групп**Рекомендация 18. Внутренний контроль, зарубежные филиалы и дочерние компании**

Финансовые учреждения обязаны применять программы по борьбе с отмыванием денег и финансированием терроризма. Финансовые группы должны быть обязаны применять групповые программы противодействия отмыванию денег и финансированию терроризма, включая принципы политики и процедуры по обмену информацией внутри группы для целей ПОД/ФТ.

Финансовые учреждения должны быть обязаны обеспечить применение мер ПОД/ФТ через групповые программы по борьбе с отмыванием денег и финансированием терроризма зарубежными филиалами и дочерними компаниями с их контролирующим участием в соответствии с требованиями страны расположения по применению Рекомендаций ФАТФ.

і. Значение понятий «финансовая группа» и «в рамках группы» в контексте обмена информацией

25. Программы финансовой группы по противодействию отмыванию денег и финансированию терроризма должны быть применимы ко всем филиалам и дочерним компаниям с контролирующим участием этой финансовой группы⁴. Такие программы должны включать политики и процедуры по обмену информацией, необходимой для проведения НПК и управления рисками ОД/ФТ. Филиалы и подразделения обязаны предоставлять сотрудникам финансовой группы, отвечающим за контроль соблюдения требований, аудит, ПОД/ФТ и другие функции и участвующим в контроле и (или) смягчении рисков ОД/ФТ на уровне группы информацию о клиентах, счетах и транзакциях, если это необходимо для ПОД/ФТ⁵. При этом должны применяться средства защиты,

⁴ Пояснительное примечание к Рекомендации 18, пункт 4.

⁵ Пояснительное примечание к Рекомендации 18, пункт 4.

Руководство ФАТФ

достаточные для обеспечения конфиденциальности и использования такой информации только в тех целях, для которых она предназначена.

26. Термин «в рамках группы» (или «в рамках предприятия») в контексте требований о программах по ПОД/ФТ, предъявляемых к финансовой группе по Рекомендации 18, включает все предприятия (как в стране, так и за рубежом), подпадающие под определение финансовой группы в Глоссарии ФАТФ. Это соответствует тому принципу, что финансовая группа в целом может подвергаться риску ОД/ФТ в связи с деятельностью входящих в нее организаций, охваченных Рекомендациями ФАТФ, а значит, этот риск требует идентификации, управления и смягчения на уровне группы.

27. Согласно Глоссарию ФАТФ, «Термин финансовая группа означает группу, которая включает родительскую компанию или юридическое лицо любого другого типа, выполняющее функции контроля и координации в отношении остальной части группы по осуществлению группового надзора согласно Основным принципам, а также филиалы и (или) подразделения, на которые распространяются политики и процедуры группы в области ПОД/ФТ».

ii. Информация, обмена которой требуют программы в рамках группы

28. Обмен информацией в финансовой группе предназначен для эффективной идентификации рисков, управления ими и смягчения этих рисков. Должна быть включена информация и анализ операций или деятельности, которые кажутся необычными (если подобный анализ проводился); может быть включено СПО, лежащая в его основе информация или факт направления СПО. Страны могут определять охват, масштаб и механизмы информационного обмена на основе чувствительности информации и ее актуальности для управления рисками ОД/ФТ (дополнительные сведения см. ниже в пунктах 50-54). Он должен соответствовать законодательной базе (как страны происхождения, так и принимающих стран), определяющей объем, степень и механизм такого обмена информацией.

29. В представленной ниже таблице показаны широкие цели ПОД/ФТ, которым должен служить такой обмен информацией. Это подтверждает тот факт, что обмен информацией в целях соблюдения требований на уровне группы необходим для комплексного и эффективного управления рисками ОД/ФТ и соблюдения требований. Информация, указанная в приведенной ниже таблице, может быть доступна, собирается или требуется не во всех случаях. Это зависит от предоставляемых клиентам продуктов и услуг, географического местонахождения, действующей правовой системы, а также рисков и контекста. Тем не менее, обмен информацией в рамках группы может обеспечить эффективность комплаенс-программы в рамках группы.

Таблица 1. Цели ПОД/ФТ для обмена информацией

Типы информации	Примеры элементов информации (если доступны и при необходимости)	Цели ПОД/ФТ для обмена информацией в группе
Информация о клиенте	Идентификационные и контактные данные клиента (имя и идентификатор); в случае юридических лиц и образований – информация о характере деятельности, владельцах и структуре управления; организационно-правовая форма и подтверждающие документы; юридический адрес и основное место ведения бизнеса; идентификатор юридического лица (LEI), финансовая и налоговая отчетность, недвижимость, информация об источниках средств и благосостояния, экономической и (или) профессиональной деятельности и бухгалтерском учете, является ли клиент ПДЛ (включая близких родственников и членов семьи), и другие важные данные из документов, полученных при регистрации клиента или внесении изменений; информация об адресных финансовых санкциях и любые иные сведения, полученные как из открытых источников, так и в процессе внутреннего расследования в отношении ОД/ФТ, категоризации рисков клиента и т. д.	Управление клиентскими и географическими рисками, определение общей подверженности рискам в связи с регистрацией одного и того же клиента сразу в нескольких организациях группы, более эффективная документация сведений о клиенте.
Информация о бенефициарных владельцах	Идентификационные и контактные данные бенефициарного владельца, принадлежащая ему недвижимость, информация об источниках средств и благосостояния, экономической и (или) профессиональной деятельности и бухгалтерском учете, является ли бенефициарный владелец ПДЛ (включая близких родственников и	Управление рисками бенефициарных владельцев и географическими рисками, обнаружение одного и того же бенефициарного владельца сразу в нескольких

Типы информации	Примеры элементов информации (если доступны и при необходимости)	Цели ПОД/ФТ для обмена информацией в группе
	членов семьи), и другие важные данные из документов, полученных при регистрации клиента или внесении изменений.	организациях группы, более эффективная документация сведений о бенефициарных владельцах.
Информация о счетах	Сведения о банковских и других счетах, включая назначение счета, ожидаемое место осуществления транзакций или деятельности по данным клиента и указываемое в деловой корреспонденции, и т. д.	Эффективное проведение надлежащей проверки и мониторинг транзакций на уровне групп, сопоставление характера транзакций с финансовым профилем, анализ сигналов или нестандартной структуры операций в рамках группы.
Информация о транзакциях	Записи о транзакциях, кредит и дебет, а также использование платежных карт, кредитная история, цифровой след (IP-адрес, информация об использовании банкомата и т. д.), информация о неудачных попытках осуществления транзакций, отчеты о валютных транзакциях, информация о закрытии счета или прекращении деловых отношений в связи с подозрениями, анализ, проведенный для выявления необычных или подозрительных транзакций, и т. д.	Общий мониторинг транзакций, обработка поступивших сигналов и выявление подозрительных транзакций, маркировка и проверка наличия подобного поведения в других структурных подразделениях финансовой группы.

iii. Важность обмена информацией для программ на уровне группы

30. В более широком контексте обмен информацией о соблюдении требований на уровне группы необходим для эффективной идентификации и смягчения рисков ОД/ФТ финансовой группой, а также управления этими рисками. Кроме того, он позволит группе реализовать более качественную систему внутреннего контроля и повысить качество принятия решений о надлежащей проверке, мониторинге транзакций и отчетах о подозрительных транзакциях. Обмен информацией между

предприятиями финансовой группы, включая подразделения и филиалы, и головным офисом обеспечит соблюдение требований на уровне группы и позволит внедрить комплексные процессы управления рисками. Консолидированная проверка и мониторинг клиентов и транзакций на предмет возможных нарушений адресных финансовых санкций также требуют информации о деятельности предприятий и клиентов, включенных в санкционный список, в различных организациях группы.

31. Рекомендации БКБН 2017 года⁶ *по рациональному управлению рисками, связанными с отмыванием денег и финансированием терроризма*, также содержат комплексные рекомендации для банков по эффективному управлению рисками ОД/ФТ в рамках группы и в международном контексте. Они разъясняют предпосылки и принципы консолидированного управления рисками, показывают, как обеспечить согласованное применение групповых политик и процедур ПОД/ФТ в рамках группы, в каких случаях особенности локальных организаций и требования юрисдикции происхождения должны быть согласованы и приведены в соответствие с более широкими политиками и процедурами группы и каким образом банки должны работать с расхождениями в требованиях страны происхождения и принимающих стран. Кроме того, в них говорится о том, каким образом банки, входящие в финансовую группу, должны делиться информацией с другими членами группы в целях информирования, улучшения оценки рисков на уровне группы и реализации эффективных политик и процедур ПОД/ФТ в рамках группы⁷.

32. Ниже перечислены основные результаты, ожидаемые от программ обмена информацией в рамках группы:

а) *Глобальная оценка рисков*

33. Для того чтобы комплаенс-программа в рамках группы была эффективной, финансовые учреждения должны понимать, каким рискам ОД/ФТ они подвергаются в глобальном масштабе. Такие риски могут быть связаны с клиентами, продуктами, географическим профилем операций, характером транзакций или иными особенностями каждого предприятия, входящего в одну и ту же группу. Комплексное понимание и идентификация этих рисков позволят финансовым учреждениям лучше структурировать свой профиль рисков и принимать соответствующие меры. Информация от филиалов, подразделений и

⁶ См. Рекомендации БКНБ *по рациональному управлению рисками, связанными с отмыванием денег и финансированием терроризма*.

⁷ «Вне зависимости от его расположения, каждое отделение должно разработать и осуществлять эффективный мониторинг политик и процедур, соответствующих рискам, присутствующим в данной юрисдикции и в банке. Такой мониторинг на местном уровне должен дополняться четким процессом по обмену информацией с головным офисом» (пункт 72).

Руководство ФАТФ

других членов группы должна применяться в ходе общей оценки рисков. Это поможет выявлять и определять характер и уровень риска ОД/ФТ для каждой входящей в группу организации, а также уровень риска ОД/ФТ для группы в глобальном масштабе, в частности связь предоставляемой информации с международными отношениями. Вот почему необходимо, чтобы специалисты по контролю соблюдения требований могли иметь доступ к такой информации, в том числе к информации о зарубежной деятельности, если она потребуется. Например, если Банк А, расположенный в стране X, обнаружит отмывающее деньги лицо и закроет его счета, однако при этом у того же лица будет счет в подразделении Банка А в стране Y, это подразделение продолжит оказывать банковские услуги отмывающему деньги лицу, поскольку не будет знать о его деятельности и действиях банка в Стране X. Кроме того, при оценке рисков ОД/ФТ, которым они подвергаются в международном масштабе, финансовые учреждения должны считать барьеры для обязательного обмена информацией, способные препятствовать эффективной реализации Рекомендаций ФАТФ, автономным риском и принимать соответствующие меры по его смягчению.

34. Обмен информацией со специалистами группы по контролю соблюдения требований (т. е. на уровне головного офиса) не означает, что только они должны оценивать соблюдение требований всеми членами группы во всех местах, где она осуществляет свою деятельность. Каждое отделение в каждом конкретном месте обязано проводить самостоятельную оценку своих рисков ОД/ФТ и располагать информацией, необходимой для собственной оценки риска. Для этой цели местному отделению многонациональной финансовой группы в отдельной юрисдикции требуется такой же доступ к информации специалистов группы по контролю соблюдения требований и других членов группы, необходимой для проведения собственной оценки рисков. В связи с этим многонациональная группа должна включать в свою систему оценки рисков и управления ими механизм, позволяющий определять, в каких случаях местным отделениям потребуется доступ к данным о международных рисках, связанных с работой с клиентами, и в каких случаях разумно или действительно необходимо предоставлять информацию о клиентах или транзакциях сразу в несколько географических регионов.

35. Более того, централизованное хранилище документации не может приравниваться к обмену содержащейся в ней информации в рамках группы. Управление доступом к электронному/централизованному хранилищу документации должно осуществляться в соответствии с требованиями о конфиденциальности и другими обязательствами. Порядок глобального мониторинга транзакций должен только повышать соблюдение требований об управлении рисками и исполнении обязательств по подаче отчетов во всех местах, где осуществляет свою деятельность многонациональная группа. Таким образом,

мониторинг в одном месте не должен препятствовать исполнению этих обязательств в других местах, где работает группа. Необходимо учитывать местные юридические ограничения на доступ к конфиденциальной информации и внедрять в глобальную оценку рисков соответствующие меры на уровне группы.

б) Эффективное смягчение рисков, связанных с клиентами, продуктами, услугами и географическим местонахождением

36. Разработка соответствующих мер по смягчению рисков, связанных с клиентами, продуктами, услугами и географическим местонахождением, требует адекватной информации о клиентах, характере их транзакций, указанном клиентом предполагаемом месте осуществления транзакций и (или) деятельности, используемых им продуктах и услугах и, если необходимо, источниках и (или) назначении денежных средств. Информация, полученная таким образом финансовой группой, поможет найти соответствующие решения по управлению рисками и их смягчению. Например, на основе общей оценки клиентов или категорий клиентов финансовые учреждения могут разработать политики по дополнительным или усиленным мерам надлежащей проверки, более строгим процедурам мониторинга транзакций, личному общению с определенными клиентами, более частым просмотром данных клиентов и т. д.

37. Точно так же информация, предоставленная финансовым учреждением специалистам группы по контролю соблюдения требований в связи с обнаруженным злоупотреблением новыми или уже существующими продуктами и услугами и предпринятыми мерами по смягчению рисков, может помочь финансовой группе реализовать последовательный подход в многонациональной среде. Процедуры по смягчению рисков на уровне группы могут быть эффективно реализованы только в том случае, если специалисты группы по контролю соблюдения требований будут располагать адекватной информацией о клиентах, их транзакциях и уровне деятельности, а также обо всех аномалиях, обнаруженных на основе доступной информации о клиентах. Например, публичное должностное лицо (ПДЛ), расположенное в Стране X – юрисдикции с высоким уровнем риска коррупции – совершает электронный денежный перевод на крупную сумму, не соответствующий его профилю, и не дает пояснений в ответ на запросы банка; в результате банк закрывает счет этого ПДЛ. То же ПДЛ отправляет структурированный электронный перевод со счета в другой организации той же банковской группы, расположенной в Стране Y, и сообщает ложные сведения об источнике и назначении этих средств. Подразделение в Стране Y не знает о закрытии счета подразделением в Стране X, а значит – не может надлежащим образом урегулировать риск, связанный с данным клиентом. Это может помешать обнаружению возможных ОПТ в международном контексте на основе информации, полученной из различных источников в рамках группы.

Руководство ФАТФ

с) *Согласованное применение систем контроля*

38. Местные операции международной компании должны осуществляться в соответствии с местными законами и положениями. В то же время должны выполняться комплаенс-программы на уровне группы, чтобы во всех организациях группы системы контроля применялись согласованно. Для применения систем контроля и процедур в масштабах группы требуется обмен релевантной информацией между финансовыми учреждениями и специалистами группы по контролю соблюдения требований. Если финансовое учреждение работает за рубежом и минимальные требования принимающей страны в отношении ПОД/ФТ ниже требований страны происхождения, оно должно следить за тем, чтобы его филиалы и дочерние компании с его контролирующим участием в принимающих странах выполняли требования страны происхождения настолько, насколько это допускают законы и положения принимающей страны. Если принимающая страна не разрешает надлежащую реализацию систем внутреннего контроля (включая обмен информацией в соответствии с Рекомендациями ФАТФ), финансовым группам следует применять соответствующие дополнительные меры по управлению рисками ОД/ФТ и информировать об этом надзорные органы своей страны происхождения. Если таких дополнительных мер недостаточно, компетентным органам в стране происхождения следует рассмотреть возможность применения дополнительных мер надзорного характера, включая установку дополнительного контроля над финансовой группой и, в соответствующих случаях, предъявления финансовой группе требования о прекращении ее отношений с принимающей страной⁸. Это может потребоваться, например, в случае, если риски перевешивают способность учреждения управлять ими с помощью соответствующих мер.

39. Информация о политиках идентификации клиентов и установления деловых отношений, отчеты внутренних и внешних аудиторов, отчеты надзорных органов о выездных проверках и наложенные ими санкции или дисциплинарные меры, а также примеры документов, подтверждающие применение мер надлежащей проверки, составления отчетов и выполнения требований о ведении документации, предоставляемые специалистам группы по соблюдению требований в соответствующих ситуациях, помогают оценивать выполнение требований. Подобная оценка позволит компании усилить свои международные системы контроля с учетом специфики каждой страны и региона. Например, тот факт, что подразделение Банка А в Стране Х не применило меры по НПК и ведению документации, может ослабить общую эффективность групповых систем контроля этого банка. Финансовое учреждение может проверить применение этих мер на международном уровне, если его специалисты по соблюдению требований имеют

⁸INR 18.5.

доступ к таким документам на выборочной основе.

d) *Обычные методы работы финансовых конгломератов, состоящих из нескольких организаций*

40. Довольно часто финансовые группы осуществляют свою деятельность сразу в нескольких направлениях (банки, ценные бумаги, страхование, сырье и т. д.). Соблюдение требований в масштабах группы означает, что такие финансовые конгломераты должны иметь возможность отслеживать и предоставлять информацию о личностях своих клиентов, их транзакциях и движении средств по счетам в масштабах всей группы. Различия в требованиях по ПОД/ФТ для каждого сектора могут потребовать определенных корректировок, однако в целом обмен информацией обеспечивает комплексный подход к управлению рисками на консолидированной основе. Например, если финансовая группа А представлена в банковском секторе, секторе ценных бумаг и секторе страхования в рамках одной и той же группы, необъясненное внесение денежных средств на банковский счет Клиента X с высокой степенью риска должно вызвать передачу сигнала о транзакциях этого клиента в другие направления деятельности этой группы. Отсутствие такой информации позволит клиенту продолжать свои транзакции в других секторах, где нет подобного мониторинга или дополнительных мер по проверке клиентов.

В. Обмен информацией о подозрении в незаконном происхождении денежных средств или их связи с финансированием терроризма в рамках финансовой группы

Рекомендация 20. Подача отчетов о подозрительных транзакциях

Если финансовое учреждение подозревает или имеет разумные основания подозревать, что средства являются доходом от преступной деятельности или связаны с финансированием терроризма, оно должно быть обязано законом незамедлительно сообщать о своих подозрениях в подразделение финансовой разведки (ПФР).

41. Рекомендация 20 ФАТФ требует от финансовых учреждений сообщения о подозрительных транзакциях, если они подозревают или имеют разумные основания подозревать, что средства являются доходом от преступной деятельности или связаны с финансированием терроризма. В Рекомендации 20 говорится только о необходимости сообщать о подозрительной деятельности и не предусматривается никакой уголовной ответственности. Этот вопрос отдается на усмотрение государственных органов власти (например, правоохранительных органов).

42. Технологические достижения последних лет расширили способности

Руководство ФАТФ

финансовых учреждений по аналитике и обработке данных и дали им возможность более глубоко изучать транзакции и выявлять тенденции и типологии, используя поток информации от различных источников, продуктов, услуг и секторов. Достижения в области анализа и обработки данных позволяют финансовым учреждениям выявлять шаблоны и тенденции, просеивая большие объемы структурированных и неструктурированных данных. Реализация этого потенциала требует аккумулирования (часто в централизованном пуле) как можно большего объема информации и выгодна как государственному, так и частному сектору.

43. Обмен информацией и анализом транзакций или деятельности, вызывающих подозрения (если такой анализ проводился), включая СПО, информацию, лежащую в основе СПО, или тот факт, что СПО был направлен филиалами или дочерними компаниями в рамках группового комплаенс, способствует развитию комплаенс-программ в группе⁹. Аналогичным образом филиалы и дочерние компании должны получать такую информацию от ответственных лиц на уровне группы, когда это уместно и целесообразно для управления рисками. Это относится и к внутренней, и к международной среде, поскольку клиенты могут взаимодействовать с различными организациями в составе финансовой группы и в различных географических регионах. Обмен информацией позволяет финансовым учреждениям выявлять клиентов с повышенным риском в различных организациях группы и применять соответствующие механизмы мониторинга или усиленные меры. Кроме того, он позволяет составить общую картину рисков, которым подвергается финансовое учреждение со стороны таких клиентов, а значит, способствует реализации эффективного риск-ориентированного подхода. Подобный обмен информацией, который может происходить до или после подачи необходимых ОПТ финансовыми учреждениями, позволит специалистам по комплаенс-контролю изучить действия и транзакции подозрительного клиента по различным вертикалям, направлениям деятельности и юрисдикциям, а затем провести тщательный анализ подозрительной деятельности, сопоставить его результаты с клиентской базой данных и разработать сценарий развития международных операций (*пункт 8 Приложения 2*).

44. В контексте финансирования терроризма крайне важную роль играет своевременность обмена информацией. Мгновенный обмен релевантной информацией в масштабах группы может оказаться решающим, особенно если речь идет о клиентах, оцененных как связанные с повышенным риском (исходя из

⁹ В феврале 2011 года объединение подразделений финансовой разведки Группа Эгмонт опубликовало официальный документ о проблемах и принципах обмена информацией в масштабах предприятия. В нем изложены основные проблемы режима международного обмена СПО и представлены возможные пути для содействия обмену СПО в масштабах предприятия. В документе сделан вывод о том, что международный характер обмена СПО в масштабах предприятия требует, чтобы юрисдикции координировали свои действия в этой сфере.

их транзакций, истории и/или страны происхождения). Изначальное подозрение финансового учреждения о том, что транзакция имеет отношение к ФТ, может подтвердить информация о транзакциях того же клиента или получателя средств в других организациях финансовой группы. Подобную цепочку транзакций можно обнаружить, только если изначальное подозрение будет передано по финансовой группе, а клиент или получатель будут помечены как требующие особого внимания. При этом процесс обмена информацией в связи с подозрениями в ФТ и получение подтверждающей информации не должны вызывать задержку в своевременной подаче ОПТ в той юрисдикции, где возникло подозрение или имели место соответствующие транзакции.

45. Невозможность законного обмена такой информацией может привести к неравномерному применению комплаенс-программы в различных организациях финансовой группы. Например, может возникнуть ситуация, когда одно подразделение подает СПО в отношении определенного клиента или транзакции, а другая организация группы, которой об этом неизвестно, не замечает ничего подозрительного в фактах, аналогичных тем, которые послужили основанием для дальнейшего анализа или подачи СПО. Все это снижает эффективность глобальных комплаенс-программ финансовых групп. Более того, в определенных ситуациях подобный сценарий может привести к признанию организации группы, не соблюдающей требования о подаче СПО во второй юрисдикции в целом, поскольку этой организации будет вменено знание о потенциально подозрительном поведении, которым обладает первое подразделение. Однако это не означает, что финансовой группе будет приписано намеренное несоблюдение требований, если невозможность эффективного взаимодействия вызвана, прежде всего, невозможностью обмена такой информацией. Кроме того, финансовые учреждения обязаны документировать соответствующие критерии обмена информацией (в соответствии с законами и положениями принимающей страны) в поддержку комплаенс-программы управления рисками в рамках группы и обеспечивать наличие средств для защиты конфиденциальности информации и ограничения ее использования только для целей ПОД/ФТ. Если эффективное управление рисками в масштабах группы затруднено, финансовые учреждения должны принимать соответствующие дополнительные меры по управлению рисками ОД/ФТ и информировать об этом надзорные органы страны своего происхождения.

С. Конфиденциальность и разглашение СПО, а также их влияние на обмен информацией в группе

Рекомендация 21. Разглашение и конфиденциальность

Финансовые учреждения, их директора, должностные лица и сотрудники:

(а) ...

(b) по закону не имеют права разглашать информацию (предупреждать) о том, что отчет о подозрительной транзакции (СПО) или связанная с ним информация направляется в ПФР.

i. Проблемы обмена информацией о подозрительных транзакциях в рамках группы и их возможные решения

46. Одной из основных проблем, связанных с обменом СПО (либо фактом подачи СПО или лежащей в его основе информации), заключается в обеспечении их конфиденциальности, необходимой для эффективной работы режима подачи отчетов. Конфиденциальность СПО предотвращает предупреждение субъекта СПО и третьих сторон, которое может помешать сбору разведанных и расследованию и позволить соответствующим лицам скрыть или ликвидировать активы. Кроме того, конфиденциальность защищает репутацию лица, ставшего субъектом СПО. И, наконец, конфиденциальность защищает и обеспечивает безопасность лица, подающего отчет, а нарушения конфиденциальности могут разрушить всю систему подачи отчетов о подозрительных транзакциях. Во многих юрисдикциях несанкционированное разглашение СПО может также повлечь за собой уголовную ответственность для соответствующего финансового учреждения. Безусловно, эти проблемы ограничивают обмен СПО.

47. Вопрос конфиденциальности СПО дополнительно усложняется, если обмен такими отчетами носит международный характер и в игру вступают законы различных стран. Это могут быть, например, государственные нормы, связанные с открытостью и формированием документации (включая СПО, поданные в принимающей стране и предоставленные специалистам группы по контролю соблюдения требований) в судопроизводстве страны происхождения, доступ к базам данных финансовых учреждений для государственных органов власти и т. д.

48. Другая проблема в области обмена СПО связана с порядком внутреннего и международного обмена информацией. Вопросы вызывает также обработка зарубежных СПО или информации о существовании зарубежных СПО в ходе судебных разбирательств. Эти моменты неясны и трактуются по-разному как в административных, так и в уголовных делах разных стран. В некоторых странах есть положения, которые требуют уведомления регулирующих органов о судебных запросах и повестках, связанных с внутренними СПО, чтобы эти органы могли вмешаться и обеспечить конфиденциальность СПО в ходе судебных разбирательств, но при этом могут не защищать иностранные СПО, поданные в иностранное ПФР. Довольно часто вопросы конфиденциальности СПО возникают в связи с их международным обменом и включают возможность их неправомерного использования для непредусмотренных целей, утечки в средства массовой информации с целью получения политических выгод и обмена без

соблюдения соответствующих законов. С точки зрения ПФР одна из основных проблем заключается в том, чтобы не допустить получение необоснованного доступа к релевантной информации третьими сторонами (включая органы власти третьих стран), особенно если обмен СПО между юрисдикциями происходит систематически, а не при наличии межюрисдикционного характера таких отчетов. Чтобы сохранить конфиденциальность СПО, передаваемых друг другу различными юрисдикциями, страны должны рассмотреть возможность распространения на иностранные СПО такой же юридической защиты, которой пользуются в их правовой системе внутренние СПО.

49. И, наконец, существует вероятность, что обмен информацией о подозрительной деятельности в рамках группы приведет к тому, что ведущие финансовые группы будут систематически подавать СПО только в юрисдикциях своего происхождения, а не в тех юрисдикциях, где находятся соответствующие входящие в них финансовые учреждения. С этим связана и другая проблема: даже если СПО подается в соответствующих юрисдикциях, внутреннее расследование финансовой группы может проводиться только в одной юрисдикции (юрисдикции родительской компании), а значит, часть релевантной информации не подпадет под право ПФР принимающей страны запрашивать дополнительную информацию у финансовых учреждений. Сотрудничество и внутренние расследования в рамках группы должны осуществляться в оперативном порядке и не препятствовать своевременной подаче СПО в подразделение финансовой разведки принимающей юрисдикции. Для решения этих проблем необходимо, чтобы финансовые учреждения подавали отчеты о подозрительных транзакциях в подразделение финансовой разведки юрисдикции¹⁰ той страны, где они осуществляют свою деятельность, в кратчайшие сроки независимо от какого-либо обмена данными.

ii. Возможные механизмы обмена информацией о подозрительной деятельности в рамках финансовой группы

¹⁰ В рамках законодательства ЕС, финансовые учреждения обязаны сообщать о подозрительных операциях в ПФР государства-члена, на территории которого создается лицо, обязанное передавать информацию. Это означает, что в ситуациях свободного предоставления трансграничных услуг, СПО всегда должны передаваться в ПФР страны, где была создана компания; если финансовые учреждения работают в другом государстве-члене, они должны представлять СПО принимающему ПФР. В некоторых конкретных обстоятельствах и с учетом ограничительных критериев национальные законы могут выходить за рамки правил паспортизации ЕС. Европейский Суд подтвердил, что при отсутствии эффективного механизма обеспечения полного и всестороннего сотрудничества между государствами-членами, который бы позволил эффективно бороться с преступлениями в сфере ПОД/ФТ, и при условии, что законодательство является соразмерным, закон ЕС не препятствует национальному законодательству государства-члена требовать от кредитных учреждений, действующих на территории данного государства-члена без создания компании на этой территории, направлять непосредственно органам государственной власти государств-членов информацию, необходимую для борьбы с ОД/ФТ (см. C-212/11 – Решение суда (третья палата) от 25 Апреля 2013 года – Jyske Bank Gibraltar Ltd v Administración del Estado)

Руководство ФАТФ

50. Существуют различные способы обмена информацией о необычной или подозрительной деятельности в пределах финансовой группы в зависимости от национальной правовой системы соответствующей юрисдикции. Это не обязательно должен быть обмен самими СПО, который в некоторых юрисдикциях запрещен. Той же цели можно достичь, например, путем: (а) обмена информацией и аналитическими данными об операциях или деятельности, которые кажутся подозрительными, если такой анализ проводился (фактах, транзакциях, обстоятельствах и документах, включая персональные данные) и результатах внутреннего анализа или проверки. Этот список элементов информации представлен для справки и не является исчерпывающим. В подобных случаях обмен информацией может осуществляться без сообщения о факте подачи самого СПО; (б) сообщения о факте подачи СПО; (в) сообщения о факте подачи СПО и предоставления связанной с ним информации (например, о подозрениях и результатах внутреннего анализа или проверки), но не самого СПО; или (д) предоставления СПО и связанной с ним информации. Это можно проиллюстрировать следующим образом:

Таблица 2: возможные механизмы обмена информацией о подозрительной деятельности в рамках финансовой группы

Возможные пути	Информация о подозрительной деятельности, внутреннем анализе или проверке	Факт подачи СПО	Само СПО
(а)	✓		
(б)		✓	
(в)	✓	✓	
(г)	✓	✓	✓

51. В связи с этим одна из основных задач обмена информацией – улучшить соблюдение требований об управлении рисками и исполнение обязательств по подаче отчетов во всех местах, где функционирует многонациональная группа. Основопологающим принципом должно быть то, что предоставляемая информация может пригодиться специалистам группы по контролю соблюдения требований для общего анализа и управления рисками ОД/ФТ в рамках группы или в некоторых входящих в нее организациях. Таким образом, предоставляемая информация

должна содержать межюрисдикционный элемент, например, информацию о клиенте, который пользуется услугами группы в нескольких разных местах, либо аспектах потока транзакций или денежных средств, влияющих на операции в соответствующих юрисдикциях. Такой обмен информацией должен подвергаться специалистами группы по контролю соблюдения требований соответствующим средствам контроля и мониторинга для защиты конфиденциальности информации и обеспечения ее использования только для управления рисками ОД/ФТ.

iii. Критерии обмена информацией в рамках финансовой группы

52. Финансовые учреждения должны определить соответствующие критерии для обмена такой информацией для целей соблюдения требований в рамках группы. При этом необязательно применять те же критерии, что и для подачи СПО. Например, если оснований для преобразования обнаруженных предупреждающих признаков в СПО недостаточно, обмен информацией об углубленном анализе, который проводится в таких ситуациях для соблюдения требований в рамках группы, может раскрыть дополнительную информацию и помочь принять решение о необходимости подачи отчета. В зависимости от обстоятельства финансовое учреждение может прийти к решению о подаче СПО одновременно с первичным обнаружением необычной или потенциально подозрительной деятельности (в т. ч. до проведения запрашиваемой транзакции). Во многих случаях определить, достигнут ли порог подозрений, позволяет углубленный анализ. В результате такого анализа может быть принято как положительное, так и отрицательное решение о подаче СПО. Более того, сама природа транзакции или деловых отношений клиента с финансовым учреждением может сделать несущественной ту или иную информацию для целей соблюдения требований в рамках группы. Это может случиться, если транзакции локализованы и никак не могут распространиться на другие филиалы, подразделения или секторы. В подобных ситуациях финансовые учреждения должны принимать соответствующие решения с учетом контекста, сложности и серьезности обнаруженных случаев.

53. Систематический обмен такой информацией в рамках группы абсолютно по всем делам может не требоваться или не способствовать повышению уровня соблюдения требований об управлении рисками и исполнения обязательств по подаче отчетов. Финансовые учреждения могут прямо прописать в своей системе оценки рисков и управления ими, в каких случаях должна закладываться основа для определения примеров и типов информации, которая будет предоставляться в целях соблюдения требований в рамках группы. Критерии подачи отчетов о подозрительной деятельности для целей соблюдения требований в рамках группы должны подвергаться периодической переоценке с учетом соответствующих событий (таких как аудиторская или экспертная проверка группы) и подлежать изучению надзорными органами.

Руководство ФАТФ

iv. Средства защиты предоставляемой информации

54. Финансовые учреждения должны использовать достаточные средства защиты предоставляемой информации, обеспечивающие (а) защиту конфиденциальности предоставляемой информации (в т. ч. от разглашения) и (б) использование такой информации только для целей ПОД/ФТ и ни для чего иного. Сюда должны входить политики, протоколы и процедуры обмена информацией, а также настройка контроля доступа и межсетевых экранов, включая, если необходимо, условия передачи информации между различными организациями группы (например, если разные организации группы обслуживают одного и того же клиента), чтобы информация была защищена и доступна только сотрудникам, ответственным за ПОД/ФТ, и только для конкретных целей ПОД/ФТ. Более того, возникновение подозрений в отношении какого-либо клиента в одной из организаций группы не означает автоматическую и (или) систематическую подачу СПО другими организациями этой группы, но может быть важным элементом анализа и профиля рисков деловых отношений и при необходимости требовать усиленных мер НПК.

v. Устранение правовых барьеров и взаимодействие с частным сектором

55. Страны должны стараться устранять все правовые и законодательные барьеры, препятствующие потоку информации в рамках финансовой группы, а значит, и эффективной реализации Рекомендаций ФАТФ. Это может потребовать тщательной оценки действующих положений (в отношении DPP, финансовой тайны, ПОД/ФТ и другого законодательства), ограничивающих обмен информацией. Активное взаимодействие с частным сектором может также помочь в выявлении областей, в которых точки зрения государственного и частного сектора на ожидания действующих требований в значительной мере расходятся. По результатам такого взаимодействия в целях улучшения условий для обмена информацией может быть опубликовано соответствующее руководство или пояснения.

ИНФОРМАЦИОННЫЙ ОБМЕН МЕЖДУ КРЕДИТНО-ФИНАНСОВЫМИ УЧРЕЖДЕНИЯМИ, ОТНОСЯЩИМИСЯ К РАЗНЫМ ГРУППАМ

56. Эффективные системы ПОД/ФТ на национальном и международном уровнях также предполагают информационный обмен между различными кредитно-финансовыми учреждениями, не относящимися к одной и той же финансовой группе. Сюда входит обмен информацией между различными учреждениями как в пределах одной страны, так и в международном масштабе, и к нему относятся все ограничения и препятствия, указанные выше. Ключевыми Рекомендациями ФАТФ, требующими осуществления информационного обмена между кредитно-финансовыми учреждениями, не относящимися к одной и той же финансовой группе, являются Р.13 (корреспондентская банковская деятельность), Р.14 (УПДЦ), Р.16 (электронные переводы денежных средств) и Р.17 (возможность полагаться на третьи стороны). Каждая из них требует предоставления или наличия определенной информации для реализации важных предупредительных мер.

57. В разделах III и IV описывается информационный обмен между различными кредитно-финансовыми учреждениями на основе ключевых Рекомендаций ФАТФ, а также преимущества добровольного обмена дополнительной информацией и способы его упрощения.

А. Информационный обмен в соответствии с Рекомендациями ФАТФ

і. В контексте корреспондентских банковских отношений (Р.13)

58. Кредитно-финансовым учреждениям предписывается собирать достаточный объем сведений об учреждении-респонденте, чтобы в полной мере понимать характер его бизнеса, оценить меры контроля учреждения-респондента в сфере ПОД/ФТ и удостовериться, что их устраивает способ использования учреждением-респондентом сквозных счетов. Сюда входит понимание, какие типы клиентов учреждение-респондент намеревается обслуживать в ходе корреспондентских банковских отношений, предполагаемый характер операций, их размеры и т.п. В некоторых особых случаях учреждение-корреспондент может запросить у учреждения-респондента дополнительную информацию, чтобы эффективно контролировать его операции. Такой контроль может предусматривать предоставление банком-респондентом банку-корреспонденту конкретной информации об операции и клиенте, чтобы позволить ему игнорировать уведомления, сгенерированные их системой контроля операций. Однако такая проверка информации банком-корреспондентом не должна быть обусловлена и не является требованием о проведении НПК в отношении клиента банка-

Руководство ФАТФ

респондента, но является следствием контроля операций, поступающих в банк-респондент или исходящих из него¹¹.

59. Учреждения-респонденты должны быть в состоянии предоставить дополнительную конкретную информацию, запрашиваемую корреспондентом в некоторых особых случаях, о конкретных клиентах и операциях. Из-за отсутствия такой информации по причине ограничений на информационный обмен банки-корреспонденты могут оказаться не в состоянии применять надлежащие меры контроля в сфере ПОД/ФТ для управления рисками, связанными с такими отношениями¹². В таких случаях, в отсутствие дополнительной информации, у корреспондентов может не оказаться другой альтернативы, кроме как прервать коммерческие отношения. В конечном итоге это может привести к задержке обработки операций или даже к прекращению корреспондентских банковских отношений, и тем самым к усугублению феномена дерискинга (*пункт 12 Приложения 2*).

60. Чтобы избежать подобного сценария, необходимо обеспечить наличие механизмов, позволяющих кредитно-финансовым учреждениям-респондентам обмениваться запрашиваемой информацией с корреспондентами. Поэтому руководство учреждения-респондента должно понимать и четко определить, в каких случаях учреждения-корреспонденты могут запрашивать информацию, а также тип такой информации, чтобы обеспечить наличие механизмов обмена такой информацией у респондентской финансовой организации. Кроме того, страны могут рассмотреть возможность стимулирования готовности банков-респондентов отвечать на подобные информационные запросы и в явном виде определить их обязательства, связанные с обменом информацией с корреспондентами.

61. Если это оправдано, страны могут рассмотреть возможность оценки своих правовых систем для устранения препятствий к информационному обмену, чтобы убедиться, что их собственные положения о защите данных и финансовой тайны или другие подобные нормативы не заставляют кредитно-финансовые учреждения терять доступ к услугам, оказываемым в рамках корреспондентских банковских отношений. Кроме того, общение и взаимодействие государственного и частного секторов также могут помочь в выявлении конкретных областей или вопросов, по поводу которых необходимы указания.

ii. В контексте услуг перевода денег или ценностей (УПДЦ) (Р.14)

¹¹ См. Руководство ФАТФ 2016 года по услугам, оказываемым в рамках корреспондентских банковских отношений (в частности, пункты 3, 4, 5 и 18).

¹² См. Руководство ФАТФ 2016 года по услугам, оказываемым в рамках корреспондентских банковских отношений (в частности, пункты 32, 33 и 41).

62. Согласно Р.14, провайдеры УПДЦ, работающие через агентов (независимо от их местонахождения), обязаны включить их в программы ПОД/ФТ и контролировать соблюдение ими требований этих программ. Это требует информационного обмена между агентами и их провайдерами УПДЦ, позволяющего последним эффективно контролировать операции агентов, что даст возможность провайдерам УПДЦ не только выполнить свое обязательство по надзору, но и повысить эффективность механизмов контроля операций и направления отчетности, используемых агентами в рамках передачи отзывов и дополнительной информации.

63. В соответствующих случаях целенаправленный обмен информацией о подозрительных операциях может также помочь провайдерам УПДЦ более эффективно снижать риски ОД/ФТ и обеспечить выполнение обязательств по управлению существующими рисками и направлению отчетности. Странам следует рассмотреть возможность выпуска необходимых указаний в данном отношении, а также идентификации и устранения барьеров, препятствующих информационному обмену.

iii. В контексте электронных денежных переводов (Р.16)

64. Рекомендация 16 ФАТФ предписывает странам обеспечить включение финансовыми учреждениями требуемой и точной информации об отправителе и требуемой информации о получателе во внутренний или международный электронный денежный перевод и сопровождающие сообщения, и чтобы эта информация сопровождала электронный перевод или сопровождающее сообщение по всей цепочке платежа. Цель Р.16 – обеспечить незамедлительную доступность основной информации об отправителях и получателях электронных денежных переводов для ПФР/ПОО, а также для кредитно-финансовых учреждений-отправителей, посредников и получателей в целях контроля операций и направления СПО, проверки по санкционным спискам, замораживания и отслеживания электронных денежных переводов¹³.

65. На случай, когда такая информация отсутствует, кредитно-финансовые учреждения-посредники и получатели должны располагать: (а) риск-ориентированными политиками и процедурами, позволяющими определять, когда выполнять, отклонять или приостанавливать электронный денежный перевод, если информация о его отправителе или получателе отсутствует; а также (б) соответствующими последующими мерами. Например, они могут включать запросы к предыдущему кредитно-финансовому учреждению в цепочке платежа о предоставлении недостающей или неполной информации в скорейшие сроки. По большому счету, такая основная информация об

¹³ Пояснительная записка к Рекомендации ФАТФ 16, пункты 1 и 2.

Руководство ФАТФ

отправителе и получателе необходима кредитно-финансовым учреждениям для эффективного выполнения электронных денежных переводов. Соответственно, ее передача обычно разрешена правовыми системами, не связанными с ПОД.

66. Ограничения на передачу информации, мешающие кредитно-финансовым учреждениям ее осуществлять, могут привести к значительным задержкам обработки операций. Странам следует создать разрешающую нормативно-правовую базу, устраняющую барьеры информационного обмена. Надлежащие указания и обратная связь могут прояснить ожидания органов регулирования от кредитно-финансовых учреждений.

67. Далее, согласно пункту 22 Пояснительной записки к Р.16, провайдеры УПДЦ обязаны соблюдать соответствующие требования Рекомендации 16 в странах, в которых они осуществляют деятельность, напрямую или через агентов. Если провайдер УПДЦ контролирует и отправителя, и получателя перевода денежных средств, то провайдер УПДЦ: (а) должен учитывать всю информацию как от отправителя, так и от получателя перевода денежных средств, чтобы определить, имеются ли основания для подозрений; а также, (b) если необходимо, должен направить СПО в соответствующее ПФР и предоставить ему информацию об операции¹⁴. А также для этого необходима передача информации о международных операциях, осуществляемых провайдером УПДЦ. Странам следует устранить любые существующие барьеры, препятствующие информационному обмену, и рассмотреть возможность выпуска необходимых указаний, чтобы провайдеры УПДЦ могли соблюдать указанные требования.

iv. В контексте возможности полагаться на третьи стороны (Р.17)

68. Согласно Рекомендации 17, кредитно-финансовым учреждениям может быть разрешено полагаться на третьи стороны (внутри страны или за рубежом) при применении элементов (а)-(с) мер НПК, указанных в Рекомендации 10, или при привлечении клиентов. Эти элементы следующие: (а) идентификация клиента, (b) идентификация бенефициарного собственника, (с) цель и предполагаемый характер деловых отношений. Кредитно-финансовое учреждение, полагающееся на третью сторону, должно незамедлительно получить необходимую информацию, относящуюся к указанным элементам, и принимать адекватные меры, чтобы копии данных идентификации и других документов о НПК были предоставлены третьей стороной незамедлительно по соответствующему запросу.

69. Таким образом, процедуры, позволяющие полагаться на третьи стороны, обусловлены способностью кредитно-финансовых учреждений получать

¹⁴ См. пункт 67 Руководства ФАТФ о РОП для провайдеров УПДЦ, февраль 2016 года.

необходимую информацию от третьих сторон. Кроме того, необходимость понимать цель и предполагаемый характер деловых отношений может привести к необходимости передачи дополнительной информации, такой как финансовое положение клиентов. Это поможет определить, соответствуют ли совершаемые операции сведениям, имеющимся у кредитно-финансового учреждения, о клиенте, его бизнесе и профиле рисков. Ограничения на информационный обмен или нормативно-правовая неопределенность могут затруднять возможность для кредитно-финансовых учреждений полагаться на третьи стороны, особенно в контексте международных операций. Это может потребовать вмешательства со стороны органов власти принимающих государств третьих сторон для разрешения затруднений, которые мешают третьим сторонам обмениваться информацией с кредитно-финансовыми учреждениями данной страны, если такой обмен разрешен в целях обеспечения возможности полагаться на третьи стороны.

v. В контексте регулирования и надзора за кредитно-финансовыми учреждениями (Р.26)

70. В целях эффективного выполнения Рекомендаций ФАТФ, для надзора за международными операциями органы надзора принимающей юрисдикции должны иметь доступ к сведениям о клиентах, счетах и операциях, которыми располагает кредитно-финансовое учреждение принимающей юрисдикции, в той мере, в которой это разрешено правовыми системами обеих юрисдикций. К таким сведениям относятся СПО и сопутствующая информация, если необходимо оценить выполнение обязательность в сфере ПОД/ФТ и надежность процедур управления рисками. Органы надзора принимающей страны будут оценивать соблюдение местных законов и обязательств, а органы надзора данной страны должны быть способны оценить соблюдение групповых политик и процедур в сфере ПОД/ФТ. Отсутствие доступа к таким сведениям может помешать органам надзора данной страны эффективно оценить соответствие на уровне группы, что влияет на эффективное выполнение Рекомендаций ФАТФ. Если помехи для информационного обмена окажутся непреодолимыми, а удовлетворительных альтернатив нет, то органы надзора данной страны должны ясно дать понять органам надзора принимающей страны, что кредитно-финансовое учреждение может быть подвергнуто дополнительным надзорным мерам, таким как усиленный надзор в отношении группы, включая (в соответствующих случаях) требование к материнской группе свернуть операции в принимающей юрисдикции¹⁵.

¹⁵ См. также Руководство БКБН по рациональному управлению рисками, связанными с отмыванием денег и финансированием терроризма, июнь 2017 года, раздел IV.

НОВОЕ В ИНФОРМАЦИОННОМ ОБМЕНЕ

Информационный обмен, выходящий за рамки Рекомендаций ФАТФ

71. Обмен дополнительной информацией между кредитно-финансовыми учреждениями – за рамками указанных выше требований Рекомендаций ФАТФ – может иметь дополнительные преимущества за счет углубленного понимания рисков и уязвимостей. А также он может обеспечивать более полное соответствие и использование возможностей частным сектором, препятствовать злонамеренному использованию преступниками недостаточной осведомленности отдельных кредитно-финансовых учреждений об их отношениях с другими учреждениями.

72. Например, некоторые юрисдикции обнаружили, что передача оповещений или сведений о клиентах, которым было отказано в обслуживании или с которыми были прекращены отношения по причине обеспокоенности по поводу ОД/ФТ, способна предотвратить использование финансовой системы преступниками, которые могут пытаться взаимодействовать со многими учреждениями. Объединение информации о платежах различных учреждений помогает выявить структурированные платежи преступников, пользующихся услугами большого количества учреждений, чтобы избежать обнаружения другими способами.

73. Однако такой информационный обмен может также породить широкий спектр общественных опасений по поводу использования (или злонамеренного использования) информации, включая недобросовестную коммерческую практику, стимулирование дерискинга и недоступность финансовых услуг, возможное нарушение конфиденциальности СПО и повышенный риск разглашения, нарушение конфиденциальности клиентов, законов о защите данных и частной жизни, тайны финансовой организации, а также общие опасения, связанные с информационным обменом, описанные в предыдущей части данного руководства.

74. Например, передача информации о клиентах между кредитно-финансовыми учреждениями потенциально может вызвать конкуренцию в связи с избирательным обменом информацией, осуществляемым лишь с небольшой группой участников. Возможно усугубление дерискинга и «защитной отчетности», например, когда кредитно-финансовые учреждения чувствуют себя обязанными направить СПО о клиенте только потому, что им стало известно, что так поступали другие кредитно-финансовые учреждения (и без проведения собственных внутренних расследований). Чрезмерное доверие к системе обмена подозрительной информацией или общая платформа

потенциально могут привести к моральному риску, когда кредитно-финансовое учреждение считает потенциально подозрительного клиента подозрительным еще до проведения надлежащей проверки клиента и поэтому лишает этого клиента доступа ко всей финансовой системе.

75. Странам необходимо тщательно учитывать правовые, политические и операционные поводы для беспокойства, отмеченные выше, и разработать меры для их смягчения. К таким мерам относятся, например, исключение злоупотреблений информационным обменом, неразрешенного использования полученной информации и нарушений основополагающих принципов договоров об информационном обмене, а также потенциальные последствия подобного поведения.

76. Также странам следует разъяснить, какими типами информации можно обмениваться, с кем и при каких обстоятельствах, с какой целью и с какими ограничениями, в зависимости от уязвимости информации и необходимости обеспечивать ее конфиденциальность. Такие разъяснения можно задокументировать и подкрепить указаниями по информационной безопасности и протоколами доступа. Это позволит избежать неоднозначного толкования, неопределенности и непоследовательного применения, которые могут затруднить информационный обмен, осуществляемый в соответствии с такими положениями. Подходящий механизм надзора и прозрачность также обеспечат доверие и ответственное отношение заинтересованных сторон.

77. Тем не менее, в последние годы страны и частный сектор сделали большой шаг вперед в анализе данных, который помогает выявлять деятельность и тенденции ОД/ФТ. Достаточные меры безопасности и механизмы существующих правовых систем разрешают информационный обмен, что гарантирует наличие более качественной и более актуальной и действенной информации, приводя к положительным результатам. Некоторые такие механизмы и процессы описаны ниже и в Приложении 2.

А. Типы информационного обмена

78. В данном контексте возможен обмен широким спектром информации, осуществляемый разнообразными способами. Они изложены ниже.

і. Информация о рисках, преступных тенденциях и типологиях

79. Кредитно-финансовые учреждения могут сотрудничать для обмена аналитической и стратегической информацией о выявленных последних рисках и преступных тенденциях, способах, техниках, общепринятых типологиях и методах злонамеренного использования финансовой системы. Такая информация, очищенная от персональных данных, не подразумевает защиту данных и конфиденциальности, разглашение или другие меры защиты

Руководство ФАТФ

информации, позволяющей установить личность. Данный информационный обмен может обеспечить уникальные сведения, которые могут использовать в своих операциях участвующие кредитно-финансовые учреждения. Это способствует более тесному сотрудничеству между участниками, а также обеспечивает актуальность оценки рисков на основании текущих тенденций и методов.

80. Часто в таких инициативах участвуют и правоохранительные органы, которые могут предоставить более полные последние сведения об указанных преступных тенденциях и типологиях, в том числе примеры дел и конкретную информацию о рисках ОД/ФТ. Это повышает общую информированность о существующих сценариях финансовых преступлений, стратегических и операционных рисках, полученных на основе анализа таких преступлений, а также об их возможном влиянии на финансовую отрасль в целом.

ii. Информация об операциях и клиентская информация

81. Некоторые страны в своих национальных правовых системах явным образом разрешают обмен определенной информацией об операциях и другой информацией о подозрительных операциях (но не обязательно самими СПО) между кредитно-финансовыми учреждениями, не относящимися к одной и той же группе. Это может быть информация о клиентах, представителях и/или бенефициарных собственниках, связанная с двумя или более кредитно-финансовыми учреждениями или подотчетными организациями, включая сведения о физических лицах или организациях, подозреваемых в ОД/ФТ. Это относится, например, к случаям, когда финансовые организации имеют одних и тех же клиентов (*Приложение 2, пункты 10-14*).

82. Такой информационный обмен может обеспечивать дополнительные элементы для более эффективной оценки риска, связанного с клиентами, или, например, упрощать подтверждение изначального подозрения, когда на новый открытый счет с минимальным движением средств в течение нескольких месяцев неожиданно поступает крупный электронный денежный перевод, и становится необходимо запросить у банка-ремитента информацию об источнике средств и другие сопутствующие сведения. Страны могут настоятельно рекомендовать кредитно-финансовым учреждениям передавать друг другу конкретную информацию об угрозах и высокорисковых клиентах. Это упрощает обмен разведывательными данными и в соответствующих случаях помогает органам власти и частному сектору в принятии решений.

В. Механизмы информационного обмена

83. В настоящее время разрабатывается ряд возможных моделей для стимулирования такого добровольного информационного обмена. Среди них двусторонний информационный обмен между финансовыми организациями и/или **совместные инструменты ЗСК и/или централизованные хранилища данных**, которые содержат ключевые элементы информации о клиентах и операциях, распространяемые среди участвующих кредитно-финансовых учреждений с использованием подходящих протоколов и средств контроля доступа. Такие инструменты могут содержать различные типы информации, используемой в целях ПОД/ФТ, включая идентификационную информацию о клиентах и/или бенефициарных собственниках и дополнительную информацию, используемую кредитно-финансовыми учреждениями для оценки рисков и составления профилей рисков клиентов. Эти инструменты могут использоваться во время установления отношений с новыми клиентами, для оценки информации о клиентах, а также на постоянной основе для проведения дальнейших мер надлежащей проверки клиентов. Такие инструменты могут содержать обновленную информацию об учреждениях-респондентах, что упрощает оценку их рисков и проведение надлежащей проверки клиентов учреждениями-корреспондентами. Во всех подобных случаях в конечном итоге за проведение надлежащей проверки клиентов отвечает кредитно-финансовое учреждение, использующее такие инструменты.

84. Указанные инструменты и базы данных могут находиться во владении органов власти, или частного сектора, или партнерств органов власти и частного сектора. Например, в некоторых странах для упрощения информационного обмена между подотчетными учреждениями, административными и правоохранительными органами были созданы базы данных для обмена сведениями о совершенных международных электронных денежных переводах, о фактах (не)направления СПО и/или о содержании СПО, а также сопутствующей информацией. Однако такие инструменты и/или хранилища, независимо от того, кто ими владеет, могут вызывать вопросы насчет того, кто в конечном итоге отвечает за контроль и кого привлекать к ответственности за ошибки – еще одна форма морального риска.

85. В некоторых случаях юрисдикции заключали **специальные договоры об информационном обмене**, упрощающие обмен информацией между кредитно-финансовыми учреждениями в целях ПОД/ФТ. Это может стать законным способом упрощения информационного обмена в целях ПОД/ФТ между кредитно-финансовыми учреждениями в международном масштабе.

Руководство ФАТФ

86. Кроме того, в ряде юрисдикций образуются **партнерства между государственным и частным секторами** в целях информационного обмена, и это дало положительные результаты. В рамках таких партнерств информация передается между правоохранительными органами, ПФР, подвергаемыми проверке представителями частного сектора и, в некоторых случаях, международными партнерами, что позволяет увидеть более общую картину операций и поведения клиентов. Такой обмен часто происходит в защищенной среде с целью упрощения дальнейшего поиска данных, оперативного анализа и просмотра частным сектором, чтобы восполнить пробелы в разведывательных данных.

87. **Отраслевые форумы или платформы.** Кредитно-финансовые учреждения могут создавать структуры, такие как межбанковские форумы или банковские/отраслевые ассоциации, для обмена информацией между участниками о новейших преступных тенденциях, методах и типологиях. В таких инициативах могут принимать участие представители правоохранительных и надзорных органов, оказывая дополнительную поддержку.

88. Обмену информацией о клиентах и подозрительных операциях могут способствовать положения о «безопасных гаванях» для кредитно-финансовых учреждений, при условии, что они не используют «безопасную гавань» в злонамеренных целях и ввели адекватные процедуры для защиты и обеспечения конфиденциальности такой информации. Такие «безопасные гавани» являются средством правовой защиты, делающим возможным информационный обмен в целях ПОД/ФТ между кредитно-финансовыми учреждениями.

89. В Приложении 2 данного руководства приводится информация о подходах, применяемых рядом стран в целях содействия такому информационному обмену. Они подробно описаны, в частности, в пунктах 10-22, 29-30 и 32-34 Приложения. Эти примеры приводятся исключительно в информационных целях, и их включение в данное руководство не означает их одобрение ФАТФ. Далее, Приложение носит иллюстративный характер и не содержит исчерпывающий перечень всех примеров, которые могут приводить к различным результатам. Однако в нем подчеркивается, как различные типы информации (стратегическая, операционная или относящаяся к клиентам) может передаваться в целях ПОД/ФТ в рамках различных моделей или механизмов в разных ситуациях.

90. Информационный обмен между кредитно-финансовыми учреждениями имеет значительные преимущества, но в то же время существуют потенциальные риски, которые необходимо устранять или смягчать. А также он сопряжен с некоторыми сложностями, отмеченными выше. Странам

рекомендуется оценить, как такой добровольный обмен информацией, выходящий за рамки требований Стандартов ФАТФ, может усовершенствовать их системы ПОД/ФТ, и разработать законодательные системы, предусматривающие такой информационный обмен.

РУКОВОДЯЩИЕ УКАЗАНИЯ И ОБРАТНАЯ СВЯЗЬ

91. Отсутствие руководящих указаний и обратной связи с органами власти частного сектора по поводу информации, передаваемой частным сектором, может помешать частному сектору эффективно контролировать операции и передавать в ПФР качественно составленные сообщения. В соответствующих случаях страны могут рассмотреть возможность введения улучшенной «траектории обратной связи», посредством которой частному сектору предоставляются наиболее последовательные и подробные пояснительные отзывы на сообщения о подозрительных операциях. Дальнейшее развитие каналов связи, по которым частный сектор получает отзывы по темам или целевым направлениям, поможет прояснить ожидания органов регулирования (*пункты 23-28 Приложения 2*). А также страны могут рассмотреть возможность разработки специальных программ взаимодействия с секторами, которые оказываются уязвимыми к угрозам ОД/ФТ (*пункт 31 Приложения 2*).

92. Кроме того, отсутствие руководящих указаний и обратной связи с органами власти частного сектора может затруднять или сдерживать информационный обмен между различными организациями частного сектора или между частным и государственным секторами и наоборот, так как ожидания органов регулирования не ясны или вследствие нехватки информации о рисках. Поэтому государственный сектор должен четко сообщать посредством руководящих указаний и обратной связи о механизмах, которые необходимо внедрять для обмена информацией. Кроме того, странам следует рассмотреть возможность публикации информации о существующих правовых механизмах, путях и разрешениях, позволяющих кредитно-финансовым учреждениям обмениваться информацией как в пределах одной группы, так и между различными финансовыми организациями. Это внесет ясность и позволит обеспечить и повысить единообразное понимание данной темы представителями частного сектора.

ВЫВОДЫ

93. Эффективность системы национального взаимодействия и сотрудничества и международного сотрудничества зависит от того, насколько хорошо различные заинтересованные стороны как государственного, так и частного секторов взаимодействуют друг с другом и обмениваются разведывательной и аналитической информацией.

94. Правовые ограничения, такие как различные правовые нормы защиты данных и конфиденциальности и их применение, положения о сохранении тайны финансовых учреждений и оперативные проблемы могут препятствовать обмену информацией в широком контексте группы, а также между финансовыми учреждениями, не входящими в одну и ту же группу. В условиях быстро развивающихся угроз и рисков, особенно касающихся финансирования терроризма, национальным органам власти и частному сектору крайне важно найти согласованные способы устранения барьеров для информационного обмена. Такие меры могут включать взаимодействие властей между собой (например, органов власти в сфере ПОД/ФТ и органов власти, отвечающих за защиту данных и конфиденциальности), если это необходимо для отыскания общего решения. В ходе такого взаимодействия также можно выявить области, в которых имеется неясность или расхождение мнений государственного и частного секторов. Ясность и указания по таким вопросам могут способствовать эффективному выполнению обязательств.

95. Как ПОД/ФТ, так и защита данных и конфиденциальности относятся к значимым общественным интересам. Национальные правовые режимы должны способствовать соблюдению обоих, чтобы предотвратить отмыwanie денег, финансирование терроризма и финансирование распространения оружия массового уничтожения способом, позволяющим соблюсти права граждан на защиту данных и частной информации, и при этом обеспечить наличие законного режима для кредитно-финансовых учреждений, гарантирующего, что законы о ПОД/ФТ и о защите данных не противоречат друг другу. Важно, чтобы национальные власти, отвечающие за ПОД/ФТ и защиту данных, признавали частичную отмену законов, если это необходимо для предотвращения конфликтов, а также дали частному сектору ясные и последовательные указания, чтобы предотвратить неверное понимание или консервативные подходы к информационному обмену в сфере ПОД/ФТ.

96. Частный сектор – важный партнер в борьбе с ОД/ФТ, который располагает ценной информацией, критически важной для правоохранительных и других компетентных органов. Эффективный и своевременный обмен такой информацией способствует достижению целей

Руководство ФАТФ

правоохранительных органов. Далее, это двусторонние отношения государственного и частного секторов, для которых необходимо наличие адекватных механизмов для передачи стратегической, операционной, тактической и специальной информации правоохранительными органами частному сектору. Выстраивание сотрудничества, атмосферы доверия и непрерывный диалог между органами власти и частным сектором способствует достижению положительных результатов в данной связи.

ПРИЛОЖЕНИЕ 1. РАЗЛИЧИЯ РЕЖИМОВ DPP И ИХ ПРИМЕНЕНИЕ

1 Как говорилось в разделе 1 данного Руководства, различия правовых режимов DPP (защита данных и конфиденциальности) в разных юрисдикциях могут приводить к сложностям реализации, особенно для частного сектора, при передаче информации как в рамках одной группы, так и между различными организациями. Эти сложности могут возникать в связи со следующими факторами.

- i. **Барьеры для обмена информацией в пределах одной группы.** В некоторых юрисдикциях обмен информацией, содержащей персональные данные, в пределах одной группы приравнивается к обмену информацией с третьими сторонами. Это происходит потому, что, согласно законодательству о защите данных, другие подразделения или филиалы организации считаются третьими сторонами, в результате чего на них распространяются ограничения. Это может также относиться к офисам одной группы, находящимся в разных юрисдикциях, в которых на такой информационный обмен распространяются ограничения. Это влияет на обмен информацией в пределах одной группы, осуществляемый в целях снижения рисков в сфере ПОД/ФТ, между подразделениями и их головными офисами и материнскими компаниями. Международные фирмы часто считают значимыми требования о защите данных на уровнях разных регионов и юрисдикций, так как они ограничивают свободную передачу информации в пределах фирмы.
- ii. **Принцип минимизации объема данных в режиме DPP** предписывает организации обрабатывать только те персональные данные, которые ей действительно необходимо обработать для достижения своих процессинговых целей, определенных недостаточно ясно и точно. Часто это приводит к неопределенности по поводу законности информационного обмена. Если обработка персональных данных требуется в соответствии с национальной системой ПОД/ФТ, неопределенность возникает тогда, когда закон недостаточно ясно определяет обязательство об обработке персональных данных, а именно, когда отсутствуют руководящие указания о целях, в которых необходимо собирать, обрабатывать и передавать такие данные. В некоторых случаях национальные власти работают над разработкой системы соответствия, которая будет учитывать информационный обмен в пределах одной группы.

- iii. **Обработка персональных данных** производится всеми кредитно-финансовыми учреждениями при открытии счета в целях надлежащей проверки клиента и впоследствии, при совершении клиентом операций, в целях отчетности и снижения рисков, в том числе в сфере ПОД/ФТ. В некоторых юрисдикциях для обработки персональных данных необходимо особое и явно выраженное согласие клиента, в зависимости от типа обрабатываемой информации. В таких случаях необходимо, чтобы согласие было дано добровольно, и в нем должно быть явно выражено конкретное информированное согласие физического лица на обработку его/ее персональных данных в виде заявления или четкого подтверждения. Согласие, если оно необходимо, также относится и к передаче данных. И возникает неопределенность, может ли кредитно-финансовое учреждение получить общее согласие в момент установления отношений с новыми клиентами или каждый раз для обработки данных учреждение должно получать отдельное согласие. Далее, в некоторых юрисдикциях может существовать абсолютный запрет на передачу персональных данных (или некоторых таких данных), даже если клиент дает на это согласие. Кредитно-финансовым учреждениям может быть сложно опираться на общие согласия или отступать от общественных интересов для передачи данных о клиентах в целях борьбы с финансовой преступностью. Содействовать информационному обмену в указанных целях могут четко сформулированные законодательные положения или указания, определяющие обстоятельства, при которых данные о клиентах можно передавать между юрисдикциями.
- iv. **В некоторых случаях передача персональных данных третьим странам запрещена**, за исключением случаев, когда органы власти данной страны, отвечающие за защиту данных, подтверждают, что информация, направляемая в третью страну, будет удовлетворительно защищена с использованием определенных мер защиты (например, при передаче данных в пределах одной группы такие органы власти могут использовать Обязательные корпоративные правила). Отсутствие таких указаний может пагубно повлиять на информационный обмен. И хотя подобное законодательство предусматривает основания для отступления от общественных интересов, часто такие основания действуют только для конкретных случаев передачи данных, а не для систематической передачи информации, для которой нужна специальная правовая база. Своевременному беспрепятственному потоку информации могут мешать требования предварительно уведомлять национальные органы, отвечающие за защиту данных, и

получать многочисленные разрешения, что может пагубно повлиять на информационный обмен.

- v. **Если в деловых отношениях кредитно-финансовых учреждений участвуют бенефициарные собственники, доступ к информации о бенефициарных собственниках может быть затруднен в случаях, когда кредитно-финансовое учреждение или его филиалы находятся в юрисдикциях, в которых обработка такой информации не разрешена.** Поэтому в таких случаях кредитно-финансовое учреждение может оказаться не в состоянии получить согласие бенефициарного собственника, необходимое для сбора, обработки и передачи его персональной информации. Это может привести к конфликтам требований к DPP и ПОД/ФТ, что на практике означает столкновение кредитно-финансовых учреждений с дополнительными проблемами при передаче информации о бенефициарных собственниках. На уровне группы это может затруднять способность кредитно-финансовых учреждений выявлять любые необычные шаблоны поведения при установлении связей (например, операции, имеющие место между двумя или несколькими компаниями с одним и тем же бенефициарным собственником) и помешать выявлению подозрительных шаблонов деятельности. Поэтому во многих случаях могут возникать дополнительные проблемы, так как личность бенефициарного собственника обычно раскрывается третьей стороне (представителю юридического лица), либо эту информацию получает и хранит само кредитно-финансовое учреждение, без участия бенефициарного собственника. В подобных случаях получение специального разрешения указывается как сложность.
- vi. **Выполнение требования о применении дополнительных мер к членам семей и лицам из ближайшего окружения ПДЛ** способом, не противоречащим принципам защиты данных – нелегкая задача. Сбор идентификационных сведений из различных источников, включая информацию об известных отношениях между клиентами (например, члены семьи, лицо из близкого окружения и т.п.) можно считать сложной задачей по соображениям защиты данных и конфиденциальности. Например, факты того, что ПДЛ является высокопоставленным лицом определенной политической партии или однополым партнером ПДЛ отражают политические взгляды или сексуальную ориентацию. Оба факта считаются уязвимыми персональными данными, и поэтому их обработка для одной или нескольких конкретных целей может быть запрещена, за исключением

Руководство ФАТФ

случаев, когда субъект данных дал четко выраженное согласие или когда такая обработка необходима в существенных общественных интересах. Однако это не мешает кредитно-финансовым учреждениям получать такую информацию напрямую от клиентов или из общедоступных источников. В данном отношении нужно вспомнить, что кредитно-финансовые учреждения должны располагать адекватными системами управления рисками для определения того, является ли клиент или бенефициарный собственник публичным должностным лицом. Это требование должно относиться также к членам семьи ПДЛ и лицам из его близкого окружения.

- vii. **Право на анонимность и удаление данных может ограничивать период действия требования о хранении данных и документов и их доступность для проведения расследований ОД/ФТ.** Согласно Стандартам ФАТФ, документы о клиентах и операциях необходимо хранить как минимум пять лет. Законы о защите данных могут предусматривать максимальный период хранения, который меньше, чем минимальный период хранения, определенный в Стандартах ФАТФ. В некоторых юрисдикциях сохраняется неопределенность по поводу совместимости требований о хранении данных с законами о защите данных и «правом на забвение/анонимность», которые являются следствием права на защиту персональных данных.

ПРИЛОЖЕНИЕ 2 – ПОКАЗАТЕЛЬНЫЕ ПРИМЕРЫ ИЗ ПРАКТИКИ

2. В настоящем разделе приведены примеры из практики стран по конструктивному взаимодействию между органами, занимающимися вопросами ПОД/ФТ, и организациями, занятыми вопросами защиты данных и конфиденциальности (DPP), а также практическими методами обеспечения обмена информацией внутри финансовых учреждений, между государственным сектором и частным сектором, а также между разными финансовыми учреждениями. Примеры из практики стран представлены для информационных целей, предназначены именно в целях иллюстрации. Их включение в настоящее руководство не означает утверждение такой практики группой ФАТФ. Настоящий раздел основан на информации, содержащейся в Разделе 3 Отчета о показателях рисков ФТ, и содержит дополнительную информацию о страновой практике, с соответствующими примерами, представленными странами. Эти методы работы и примеры из практики относятся к следующим широким областям деятельности:

А. Сложные задачи согласования требований в области ПОД/ФТ и нормативно-правовой базы по защите данных.

3. В ряде стран для финансовых учреждений национальными компетентными органами были подготовлены соответствующие руководства, направленные на то, чтоб помочь КФУ принять и соблюдать ожидаемые требования регулирующих органов, содержащиеся в двух типах законодательных актов. В некоторых странах надзорные органы по ПОД/ФТ также проводят совместные встречи и консультации друг с другом, чтобы лучше сформулировать свои регламентирующие требования и соответствующие задачи. Такой диалог происходит до принятия правил органами, регулирующими вопросы защиты данных и конфиденциальности (DPP), а также на постоянной основе с целью предоставления дальнейших рекомендаций и ответов на часто задаваемые вопросы (FAQs). Среди принятых мер – создание рабочих групп надзорными органами, органами защиты данных и регуляторами, КФУ и представителями сектора финансовыми услугами для обеспечения скоординированного подхода и последовательного обеспечения соответствующего руководства по реализации нормативных требований.

Франция

Каждая инструкция, руководство или назначение, осуществляемые надзорным органом Франции в области ПОД/ФТ, до утверждения и публикации, сначала подлежит согласованию и решению специальным комиссией экспертов,

называемой Консультативной комиссией по вопросам противодействия отмыванию денег и финансированию терроризма (CCLCBFT), которая была создана советом надзорного органа. Для участия в заседаниях данной Консультативной комиссией приглашаются представители Департамента французского казначейства, а также Службы финансовой разведки Франции и другие соответствующие органы, включая уполномоченный орган Франции по защите данных и гражданских прав Комиссия по информационной защите и свободам (Commission for Data Protection and Liberties, CNIL). Особенно активно проходили обсуждения, когда французский надзорный орган издал руководящие принципы по обмену информацией внутри финансовой группы (системы), так и за ее пределами.

Кроме того, указанная Комиссия CNIL также издала свои положения с изложением своей интерпретации предлагаемого государственного законопроекта, который повлияет на условия защиты данных или создание новых файлов в области ПОД/ФТ. Наконец, с 2005 года французским органом DPR принят единый разрешительный регламент (общий стандарт) в сотрудничестве с государственными органами и представителями частного сектора. Единый регламент регулярно обновляется. Цель состоит в том, чтобы найти баланс мер ПОД/ФТ и требований по защите данных с целью формирования гармонизированной комплексной системы норм и правил для всех заинтересованных сторон. Кроме того, такой общий регламент также является инструментом упрощения требований: почти 1800 организаций сообщили о своем принятии соблюдения единых требований с использованием общей регламентирующей базы. Кроме того, такое единое регулирование разрешает общее использование информационных данных клиентов совместно с компетентными французскими правовыми организациями, ответственными за борьбу с ОД/ФТ.

4. Во многих случаях к органам по защите данных и конфиденциальности обращаются за консультацией и приглашают их представителей в случаях специфических вопросов в отношении мер ПОД/ФТ, чтобы избежать вероятного возникновения противоречий или двусмысленности, неопределенности между требованиями двух регламентирующих систем. Органам, регулирующим вопросы защиты персональных данных и конфиденциальности, также рекомендуется консультироваться с органами ПОД/ФТ при разработке своих мер. Такая практика способствует созданию и развитию условий сотрудничества между двумя регламентирующими органами и способствует формированию убеждений, что их политические цели и задачи не являются взаимоисключающими.

Канада

Органы, занимающиеся вопросами DPP, и органы ПОД/ФТ обычно работают совместно до разработки соответствующего законодательства. Закон о защите персональной информации и электронных документов (*Personal Information Protection and Electronic Documents Act* (PIPEDA)) является федеральным законом Канады, регулирующим вопросы защиты данных и конфиденциальности для частного сектора. Управление Комиссара по защите частной информации разместило Руководство на своем веб-сайте «Принципы конфиденциальности и законодательство ПОД/ФТ (Privacy and PCMLTFA): как обеспечить соблюдение прав ваших клиентов на неприкосновенность конфиденциальной информации и при этом выполнение требований к отчетности по мерам борьбы с отмыванием денег и финансированием терроризма, применяемых в вашей организации». Существует также перечень вопросов и ответов, разработанных с использованием FINTRAC (Канадский центр анализа финансовых операций и отчетности)¹⁶. В руководящих указаниях признается, что Закон о борьбе с отмыванием денег, полученных преступным путем, и финансированием терроризма (PCMLTFA) требует от организаций, на которые распространяется действие Закона, выполнять определенные действия в целях выполнения требований законодательства, такие как идентификация клиентов и ведение учета данных. Кроме того, по определенным операциям требуется представление отчетов в Центр анализа финансовых операций и отчетности Канады. Далее, в Законе ПОД/ФТ Канады указано, что Управление Комиссара Канады по защите частной информации поддерживает усилия организаций по борьбе с отмыванием денег и финансированием терроризма, что программы или инициативы должны осуществляться таким образом, чтобы учитывать нюансы уважения прав на частную жизнь и законы о защите персональных данных.

5. В некоторых случаях органы, работающие в области защиты данных, являются частью институциональной структуры ПОД/ФТ и непосредственно участвуют в процессе создания правил и требований ПОД/ФТ. Тесное взаимодействие и совместное участие органов помогает улучшить координацию работы разных ведомств и оценку различных перспектив.

Испания

Основной координационной структурой для разработки и согласования регламентов Испании в области ПОД/ФТ является Комиссия по предотвращению отмывания денег и финансовых преступлений. Состав Комиссии включает более

¹⁶ См. сайт Управления Уполномоченного по вопросам конфиденциальности Канады

20 ключевых ведомств и учреждений, включая Испанское агентство по защите данных. Одной из основных функций Комиссии является выработка заключения по предлагаемым проектам нормативно-правовых актов и положений, регулирующих вопросы в области предотвращения отмыwania денег и финансирования терроризма. Такая координация работы всех ведомств на самом высоком уровне позволила принять законодательство, в котором предусмотрен отказ от правил, изложенных в Законе о защите данных.

6. В некоторых юрисдикциях законодательство о защите данных предусматривает определенные отступления, которые могут потребоваться для выполнения обязательств, налагаемых другим законодательством. Это может относиться к ограничениям на право доступа субъекта данных, право на получение согласия, предварительное уведомление, право на забвение и т.д. Эти отступления направлены на сбалансирование вопросов безопасности и конфиденциальности. Национальные власти могут рассмотреть возможность предоставления дополнительных указаний в этих областях, если они сочтут это необходимым. В контексте Европейского союза (ЕС) ведется работа по разработке европейских правил защиты данных.

Европейский Союз

14 апреля 2016 года на уровне Европейского Союза был принят Общеввропейский регламент о персональных данных (General Data Protection Regulation, GDPR) в целях применения его всеми странами ЕС. Указанный Регламент заменяет предыдущие законодательные документы ЕС и национальные нормативные документы о защите персональных данных. Закон вступит в силу 25 мая 2018 года. Это еще один шаг к гармонизации европейских правил в области защиты данных. В большинстве случаев Регламент GDPR учитывает данные о местонахождении, IP-адресах и идентификаторах персональных данных, используемых в сети интернет, так как указанные данные могут использоваться для установления личности, в частности, в сочетании с уникальными идентификаторами. Кроме того, Общеввропейский регламент о персональных данных вводит дополнительные инструменты, используемые для передачи данных (коды поведения и сертификаты) в целях содействия обмену информацией.

Италия

Внутреннее законодательство Италии обеспечивает четкие механизмы обработки персональных данных и обмена такими данными в целях соблюдения законодательства и регулирующих документов в области ПОД/ФТ. Для

определенных случаев, в целях внесения наибольшей ясности, национальные органы по защите данных оформили общую процедуру применения мер ПОД в качестве общесистемных требований, что облегчает обмен данными между всеми участниками системы при использовании финансовых посредников. В таких случаях согласие субъекта данных не требуется.

7. В некоторых юрисдикциях финансовые учреждения могут делиться информацией, содержащей данные клиентов, за счет использования специальных исключений, предусмотренных законодательством о защите данных, а также за счет отмены ряда ограничений при обмене информацией в целях ПОД/ФТ. Финансовые учреждения должны тщательно учитывать все такие отступления от общих правил при принятии собственных процедур и практик в области обмена информацией.

Сингапур

Обмен информацией о клиентах между финансовыми учреждениями регулируется Законом о банковской деятельности и Закона о трастовых компаниях Сингапура, который заменяет общие положения о защите данных, изложенные в Законе о защите персональных данных (PDPA). В целях борьбы с отмыванием денег и финансированием терроризма в указанных Законах о банковской деятельности и о трастовых компаниях Сингапура отменяются положения о соблюдении конфиденциальности финансовой информации (например, для соблюдения требований, предъявляемых главными надзорными ведомствами, органами внутреннего надзора, в целях проведения головными организациями внутренних аудитов или проверок в рамках управления рисками). Кроме того, ряд требований национального Закона о защите персональных данных также были отменены, и финансовые учреждения обязаны обмениваться информацией со своими головными офисами, отделениями и дочерними компаниями в рамках финансовой группы в соответствии с уведомлениями Валютного управления Сингапура (MAS) по вопросам ПОД/ФТ, где это необходимо в целях противодействия отмыванию денег и управления рисками в области финансирования терроризма.

В. Межбанковский обмен информацией

8. Совместное использование СПО дочерним банком или отделением финансового учреждения с головным офисом дополняет процессы управления рисками в масштабах всей межбанковской группы и выполняет функции надзора головным офисом. Более того, дальнейшее совместное использование СПО в

Руководство ФАТФ

рамках группы также способствует более эффективным процедурам внутреннего контроля и управления рисками. Такой обмен данными специально разрешен в определенных юрисдикциях при условии соблюдения надлежащего контроля за соблюдением требований конфиденциальности.

США

В январе 2006 года Управление по борьбе с финансовыми преступлениями при Минюсте США (FinCEN) и федеральные агентства США по банковской деятельности (Управление контролера денежного (валютного) обращения (ОСС), Федеральный резервный банк, Федеральная корпорация страхования депозитов (FDIC) и Управление по надзору за сберегательными учреждениями (OTS)) установили, что отделение или офис иностранного банка, расположенный в США, может делиться данными своей отчетности о подозрительной деятельности (SAR) со своим головным офисом. В этом Руководстве, изданном в январе 2006 года, также было указано, что американский банк или сберегательная ассоциация могут обмениваться отчетами о подозрительной деятельности со своей контролирующей компанией (как внутри страны, так и рубежом). Совместное использование СПО или, в более широком смысле, любой информации, которая выявила бы наличие таких отчетных данных о подозрительной деятельности, с головным офисом или контролирующей компанией (в том числе за рубежом) способствует соблюдению существующих требований Закона о банковской тайне (основной закон о ПОД/ФТ), обеспечивая для головного офиса или контролирующей компании выполнение своих надзорных обязанностей в отношении управления рисками в масштабах всей организации, включая надзор за соблюдением депозитарным учреждением применимого законодательства и регламентирующих документов.

Кроме того, в ноябре 2010 года Общее руководство, выпущенное Управлением FinCEN и федеральными банковскими агентствами, предусматривало, что депозитарное учреждение, предоставляющее отчетность о подозрительной деятельности, может обмениваться данными СПО или, в более широком смысле, любой информацией, которая выявила бы наличие таких отчетных данных о подозрительной деятельности, с аффилированным лицом, если такое аффилированное лицо подпадает под нормативные требования к отчетности СПО. Совместное использование данных СПО с такими аффилированными лицами облегчает выявление подозрительных операций, осуществляемых через аффилированные лица депозитарного учреждения, которые должны соблюдать требования по предоставлению отчетности о подозрительной деятельности.

Франция

Статья L. 561-20 Валютно-финансового кодекса Франции разрешает обмен соответствующей информацией в банковской среде. Кроме того, финансовые учреждения должны заполнять на ежегодной основе опросник в области ПОД/ФТ, включая юридические препятствия, которые они встречали в области обмена информацией со своими отделениями или дочерними компаниями. В таких ситуациях информация об иностранных законах и регулирующих документах, которые запрещают или препятствуют финансовому учреждению осуществлять соответствующие меры ПОД/ФТ в своих отделениях и дочерних компаниях за рубежом, должны быть предоставлены подотчетными организациями для французского надзорного органа. ПФР также должно быть проинформировано подотчетными организациями об этих трудностях.

9. В некоторых финансовых группах соблюдение требований в отношении анализа данных подозрительной деятельности, которыми обменивались участники финансовой группы, осуществляется центром мониторинга и анализа, который централизованно создается в рамках финансовой группы, чтобы консолидировать внимание на подозрительных клиентах и уменьшить количество точек доступа с целью предотвращения утечки информации. Такой центр может предпринять оперативные действия в связи с различными обстоятельствами проведения подозрительных операций и уведомить другие подразделения внутри своей системы, чтобы предотвратить воздействие риска на клиента в более чем одном месте или на разные аспекты его операций или движения средств, влияющих на операционную деятельность в соответствующих юрисдикциях.

С. Обмен информацией между финансовыми учреждениями разных финансовых групп/систем

10. Своевременное и добровольное совместное использование финансовой информации финансовыми учреждениями, преимущественно при взаимодействии между собой с учетом правил «безопасной гавани» и защиты от юридических последствий, способствует более эффективной реализации мер ПОД/ФТ, укреплению надежности финансовой системы и предотвращению ее использования преступниками в незаконных целях. Также это дает возможность предоставлять более точные и полные сведения правоохранным органам. В некоторых юрисдикциях существуют определенные законодательные механизмы и условия по применению правил «безопасной гавани» (средства защиты), которые помогают упростить и усовершенствовать обмен информацией между финансовыми учреждениями внутри общей структуры, частью которой они являются.

США

Раздел 314 (b) Закона США о противодействии терроризму – USA PATRIOT АСТ (об обмене информацией между финансовыми учреждениями) предусматривает, что два или более финансовых учреждений и любая ассоциация финансовых учреждений могут обмениваться информацией друг с другом в отношении физических лиц, компаний, организаций и стран, подозреваемых в возможном ведении террористической деятельности или отмывании денег. Финансовое учреждение или объединение, направляющее, получающее или передающее такую информацию при выполнении действий по выявлению сведений и представлению отчетности, которая может включать данные о террористических актах или отмывании денег, не несет ответственность ни перед одним лицом согласно любому закону или нормативному документу США, любой конституции, законодательства или нормативного документа любого государственного или политического органа или по любому договору или другому юридически обязывающему соглашению (включая любое арбитражное соглашение) за указанное раскрытие данных или за любое непредставление уведомления о таком раскрытии лицу, которое является субъектом такого раскрытия или любого другого лица, указанного в таком раскрытии данных.

11. В ряде стран также разрешается обмен информацией между двумя финансовыми учреждениями, которые не принадлежат к одной финансовой группе, при условии, если соблюдаются определенные критерии.

Франция и Румыния

Во Франции обмен информацией между двумя финансовыми учреждениями, которые не принадлежат к одной и той же финансовой группе, допускается, если соблюдаются некоторые критерии (статья L. 561-21 Денежного-финансового кодекса Франции). Среди таких условий есть, в том числе, обязательство гарантирования финансовыми учреждениями того, что их контрагент по сделке применяет меры в области ПОД/ФТ в соответствии с требованиями нормативных правил Франции, которая занимается внедрением Рекомендаций ФАТФ.

Статья 25 (4) Закона Румынии о ПОД/ФТ разрешает финансовым учреждениям обмениваться информацией с другим финансовым учреждением. В частности, согласно пункту (b) кредитным и финансовым учреждениям разрешается обмениваться информацией, которая подпадает под определение конфиденциальной/секретной информации в случаях, когда такие КФУ: (1) находятся в пределах одной финансовой группы; (2) расположены в ЕС, в зоне

Европейского экономического сообщества или другой стране, которое накладывает аналогичные требования к ПОД/ФТ; (3) применяют меры надлежащей проверки клиента и меры ведения отчетности, аналогичные тем, которые предусмотрены законодательством о ПОД/ФТ; (3) подлежат надзору в области ПОД/ФТ. Кредитные и финансовые учреждения могут также обмениваться информацией, подпадающей под определение конфиденциальной, даже если они не входят в одну и ту же финансовую группу, если: (1) они находятся в ЕС, зоне Европейского экономического сообщества или другой стране, которое накладывает аналогичные требования к ПОД/ФТ; (2) информация относится к одному клиенту и транзакции; (3) они относятся к одной и той же категории бизнеса; (4) они обязаны соблюдать аналогичные требования к конфиденциальности и защиты данных.

12. Между некоторыми юрисдикциями были достигнуты двусторонние договоренности для облегчения обмена информацией между финансовыми учреждениями в целях ПОД/ФТ. В них подчеркивается важность снижения определенных национальных/региональных рисков ОД/ФТ посредством механизма двусторонних или многосторонних соглашений.

США и Мексика

В настоящее время между США и Мексикой осуществляется постоянное координирование усилий и взаимодействие в целях общего повышения финансовой прозрачности и предотвращения случаев ОД/ФТ в сфере действий корреспондентских банков.

В свете текущих надзорных требований банки США должны отслеживать все транзакции, которые осуществляются КФУ в качестве финансовых посредников, и где целесообразно вести учет СПО. Американские банки регулярно направляют Запросы на информацию (RFI) для своих респондентов (партнерских банков, т.п.) в целях запроса дополнительной информации в случае обнаружения необычной транзакции. Такие запросы предназначены прежде всего для оперативного оповещения, чем в целях отчетности СПО. По причине действующих положений мексиканского законодательства по требованиям конфиденциальности и Закона о защите персональных данных мексиканские банки не смогли предоставить нужные данные, что может привести к увеличению числа СПО и закрытию ряда счетов. Такое непредставление данных со стороны мексиканских банков на запросы банков США может привести к формированию целого ряда СПО в банках в США и, возможно, к прекращению корреспондентских отношений счета. Чтобы решить эту проблему, в декабре 2014 года были внесены поправки в общие положения мексиканского ПОД/ФТ, применимые к банкам, с тем, чтобы впервые

предоставить возможность мексиканским банкам обмениваться информацией с иностранными банками для целей ПОД и ПФТ.

В частности, правительство Мексики внесло поправки в свои Общие положения ПОД/ФТ, применимые к банкам, и установило юридический механизм, с помощью которого мексиканские банки могут делиться информацией как данными своих постоянных клиентов, так и разовых клиентов, а также об их сделках с иностранными банками исключительно в целях ПОД/ФТ. В соответствии с Законом о кредитных учреждениях Мексики банки должны рассматривать своих постоянных и разовых клиентов как конфиденциальные данные. Поэтому банкам запрещается разглашать историю транзакций или личные данные своих постоянных и разовых клиентов, кроме владельцев счетов, бенефициарных собственников, доверительных собственников, кредиторов или законных представителей. В качестве исключения банки предоставляют указанную информацию в случаях, если она запрашивается: (i) судьей по судебному запросу о представлении данных; (ii) генеральной прокуратурой; (iii) военной прокуратурой; (iv) органами Министерства финансов для целей ПОД/ФТ или налогообложения; или (v) федеральным надзорным органом. Кроме того, банки могут обмениваться соответствующей информацией с другими банками в целях ПОД/ФТ в связи с информацией о своих постоянных и разовых клиентах, а также о сделках с ними.

Прежде чем начать обмен такой информацией Министерство финансов Мексики должно одобрить соответствующие иностранные банки. Аналогичным образом, прежде чем мексиканские и иностранные банки начнут обмениваться информацией, они должны согласовать в письменной форме требования конфиденциальности такой информации, а также указать данные и должности отдельных сотрудников, уполномоченных проводить данный обмен информацией. Такое соглашение должно быть направлено в Национальную комиссию по банковской деятельности и ценным бумагам.

Компетентные органы и банки США и Мексики совместно разработали специальный опросник, который в настоящее время используется в качестве формы для реализации механизма обмена информацией. С учетом этого, до или во время обмена информацией мексиканские банки предоставляют властям копию переданной информации и соответствующих данных.

Благодаря этому механизму мексиканские банки теперь могут обмениваться информацией с другими банками, кроме США, при условии соблюдения тех же информационных протоколов.

13. В ряде других стран, национальные органы обязали свои финансовые учреждения направлять информацию об определенных финансовых операциях в централизованные базы данных, администрирование которыми осуществляется самими финансовыми учреждениями или финансовыми управлениями, и учитывать эту информацию в составе оценки риска, которую такие учреждения должны выполнять в отношении баз своих клиентов.

Мексика

В 2017 году, исходя из тех же доводов, которые легли в условия регулирования работы кредитных бюро, было принято постановление о ПОД/ФТ, которое предусматривает обязательное предоставление банками в централизованную базу данных, управляемой центральным банком или аналогичным банковским учреждением, определенную информацию о каждом международном банковском переводе или переводе внутри страны в иностранной валюте, которую банки отправляют или получают от имени своих клиентов. Кроме того, согласно этому правилу, банки обязаны получать из базы данных определенную сводную информацию обо всех банковских переводах, обрабатываемых их клиентами в банковской системе в целом, и учитывать эту информацию для проведения мер надлежащей проверки своих клиентов, которые делают запрос на такой банковский перевод и общую оценку рисков. Клиенты должны подтвердить согласие своему соответствующему банку по направлению и получению им такой информации для/из базы данных. Действующий регламент по ПОД/ФТ определяет информацию, которую банки должны представить в базу данных, а также статистическую информацию, которую база данных в свою очередь предоставляет банкам.

Эту база данных разработана Центральным банком, и банки смогут обмениваться информацией о транзакциях своих клиентов уже в конце 2017 года. На втором этапе банки должны будут предоставлять определенную информацию и сведения «знай своего клиента» (KYC) и соответствующие документы таких клиентов, а также проверять эту информацию по базе данных.

14. В существующей практике есть интересные для изучения примеры того, как организации частного сектора могут обмениваться между собой информацией об определенной угрозе и сведениями о высокорисковых клиентах. В некоторых юрисдикциях для облегчения обмена информацией между подотчетными организациями, а также административными и правоохранительными органами были созданы общие базы данных для обмена СПО и связанной с ними

Руководство ФАТФ

информацией. Это способствует более эффективному обмену данными, а также, в соответствующих случаях, оперативно-разведывательной информацией для содействия принятию решений уполномоченными органами и частным сектором.

Испания

Статья 33 Закона о предотвращении ОД/ФТ предоставляет полномочия для подотчетных лиц обмениваться информацией, касающейся транзакций, по которой они направляют отчеты в ПФР с единственной целью предотвращения или предупреждения операций, связанных с ОД/ФТ, когда характеристики или схема конкретного случая предполагают возможность того, что после получения отказа/отклонения транзакции эта же транзакция или частично аналогичная ей транзакция может быть предпринята для исполнения другими подотчетными лицами.

С учетом этих рисков можно создать централизованную базу данных с целью обмена такой информацией. Подотчетные лица и судебные, правоохранительные и административные органы, уполномоченные по принятию мер с целью предотвращения или пресечения случаев ОД/ФТ, могут обращаться за получением нужной информации, содержащейся в созданных файлах. Что касается подотчетных лиц, доступ к таким данным ограничивается их соответствующими внутренними процедурами и отделами, назначенными подотчетными организациями, ответственными за соблюдение требований законодательства.

Д. Обмен информацией между финансовыми учреждениями и уполномоченными органами

15. Тесное взаимодействие между частным и государственным секторами является одним из важнейших элементов системы ПОД/ФТ. Стандарты ФАТФ требуют от стран создания четких проработанных правовых и операционных схем для информирования частного сектора о рисках ОД/ФТ и обеспечения того, чтобы частный сектор учитывал риски ОД/ФТ в процессе своей деятельности. В контексте рисков ФТ, в частности, может потребоваться объединение информации, полученной от подотчетных организаций, со служебной и специальной обработанной информацией компетентных органов.

Россия

В соответствии с положениями Федерального закона о мерах ПОД/ФТ система сотрудничества между ПФР-Росфинмониторингом, надзорным органом, функции которого выполняет Банк России, и подотчетными организациями

предусматривается в случаях, когда было отказано в совершении сделки, открытии счета или расторжении договора. Обо всех таких случаях подотчетные организации должны сообщать в ПФР, где информация анализируется, а затем передается в Банк России, чтобы далее направить соответствующую информацию кредитным организациям и некредитным финансовым учреждениям через защищенные каналы связи. Информация, полученная подотчетными организациями, должна учитываться ими при проведении оценки рисков по своим клиентам, что способствует определению соответствующего уровня риска и разработке соответствующих соразмерных мер по снижению риска.

а) Партнерства с участием государства и частного сектора

16. В частном секторе хранится множество данных, которые могут быть использованы правоохранительными органами в целях проведения расследований. В некоторых странах созданы государственно-частные партнерства для содействия обмену информацией между государственным и частным секторами и между финансовыми учреждениями, которые являются участниками таких партнерств. Цель подобных формальных или неофициальных платформ – создание благоприятных условий для обратной связи и обеспечения методологической поддержки в процессе взаимодействия между государственным и частным секторами, а также для обмена оперативной информацией, информацией о рисках и решения задач по предотвращению, выявлению и устранению возможных угроз.

Швейцария

В Швейцарии созданы различные механизмы и платформы для взаимного обмена информацией с частным сектором. В 2010 году в контексте пересмотра стандартов ФАТФ уполномоченные органы Швейцарии создали рабочую группу с участием организаций частного сектора (ISFIN) для обеспечения взаимного обмена информацией в отношении разработки нормативной базы в области ПОД/ФТ. Не так давно в более широком контексте межведомственной координационной группой по борьбе с ОД и ФТ, созданной в 2013 году, которая также отвечает за национальные оценки рисков (NRA), была создана дополнительная контактная группа для взаимодействия с частным сектором. В эту группу входят специальные эксперты по ПОД/ФТ с опытом работы в разных секторах, которые подпадают под действие законодательства по ПОД/ФТ, таких как банковский и страховой сектора, и организации, оказывающие услуги по переводу денег или ценностей (MVTs). Данная группа была создана как постоянная платформа для обмена мнениями по вопросам возникающих рисков, их определения, оценки и снижении существующих и возникающих рисков ОД/ФТ.

Группой уже сформированы направления предстоящей работы между государственным и частным секторами, такие как типологии ФТ и корреспондентские отношения банков. Работа Группы способствует укреплению связей с частным сектором и повышению осведомленности по вопросам ПОД/ФТ.

Гонконг, Китай

Целевая группа по борьбе с мошенничеством и отмыванием денег (The Fraud and Money Laundering Intelligence Taskforce) представляет собой механизм обмена информацией между государственным и частным секторами, участниками которого являются полиция Гонконга, Гонконгское денежно-кредитное управление и банковские учреждения, объединяющие усилия с целью улучшения выявления, предотвращения и ликвидации схем мошенничества, отмывания денег и других видов финансовых преступлений в экономическом секторе Гонконга. Созданная в мае 2017 года в рамках 12-месячного экспериментального проекта, целевая группа использует в своей работе существующие уровни неформального сотрудничества и обмена данными; соответствующие подготовительные совещания состоялись до 2016 года по формированию формальной структуры совместной работы банков и компетентных органов в целях улучшения общего понимания угроз, эффективности адресных действий и оперативных мер правоохранительных органов, а также улучшения управления рисками в банковской сфере. Данная целевая группа работает как на стратегическом, так и на операционном уровнях с использованием специальных информационных оповещений, распространяемых в более широком масштабе для участников финансового сектора через безопасную платформу.

Австралия

3 марта 2017 года Австралийский отчетно-аналитический центр транзакций (AUSTRAC) запустил совместный проект **Fintel Alliance**, который объединяет правительство, коммерческий сектор, научно-исследовательские организации и международных партнеров, взаимодействующих в общей и безопасной среде обмена информацией, тем самым обеспечивая комплексный подход к совместным задачам выявления, определения и предотвращения серьезных правонарушений со стороны организованной преступности, взяточничества и коррупции, террористической деятельности, опираясь на аналитические данные финансовой разведки. Число участников Fintel Alliance продолжает расти по мере поступления новых заявок, которые в настоящее время проходят оценку экспертами организации. По состоянию на конец апреля 2017 года группа Fintel Alliance

включает 19 партнерских организаций, в том числе AUSTRAC, AFP, NSW Police, ATO, Австралийские банки – ANZ, Commonwealth, Macquarie Bank, Национальный банк Австралии, Westpac, а также системы Western Union и PayPal. К альянсу Fintel Alliance присоединилось Британское национальное агентство по борьбе с преступностью, и сейчас центр AUSTRAC ведет переговоры с другими потенциальными международными партнерами.

Объединением Fintel Alliance был создан операционный центр – Operations Hub, где аналитики из государственных органов и коммерческих отраслей работают бок о бок в совместных рабочих проектах, обмениваясь информацией в режиме реального времени. В целях создания единой рабочей среды организованы следующие три крупных проекта:

- оценка Панамских документов;
- выявление и категоризация нелегальных онлайн-посредников или посредников по передаче денег (online money mules); а также
- расширение использования баз данных австралийской сети Cyber Online Reporting Network.

17. Партнерские организации признают важность вовлечения частного сектора не только в качестве источника информации, но и в качестве получателя конфиденциальной информации и аналитических данных, находящихся в ведении государственного сектора, для улучшения работы по выявлению потенциальных случаев финансирования терроризма. Такой обмен данными преимущественно происходит в безопасной информационной среде после получения надлежащих разрешений, чтобы облегчить дальнейший анализ данных, оперативный анализ и сверку (сканирование) данных предприятиями частного сектора для заполнения потенциальных пробелов в информационных базах. Такая деятельность должна осуществляться на постоянной основе, а не только в связи с отдельными транзакциями и конкретными случаями, поскольку частный сектор должен также иметь правильное и полное понимание постоянно меняющейся картины рисков в дополнение к действиям правоохранительных органов.

Канада

Улучшение мер бдительности и отчетности (СПО) подотчетных организаций: сразу после террористических атак в Оттаве и Квебеке Канадский центр анализа финансовых операций и отчетности (FINTRAC) опубликовал рекомендации для подотчетных организаций, чтобы обратить внимание на важную роль отчетности о подозрительной деятельности, которая может охватывать разные типы угроз ФТ. Объем направляемых отчетов СПО увеличился на 22% в течение месяца

после атак в Оттаве (более 8 700 в октябре 2014 года). В дополнение к оповещениям, направляемым по другим случаям, связанным с атаками ИГИЛ, FINTRAC также разработал и направил для всех подотчетных организаций соответствующий перечень показателей (индикаторов) ФТ.

Развитие системы действующего партнерства с подотчетными организациями и система оперативных оповещений и сообщений (Operational Alerts and Briefs): последние несколько лет FINTRAC тесно сотрудничал с крупными финансовыми учреждениями в области ПОД/ФТ. Центр FINTRAC разработал новую линейку продуктов, включающую систему оперативных оповещений (Operational Alerts). Ее цель – обеспечить современные способы выявления подозрительных финансовых операций и факторов высокого риска, связанных с конкретными методами ОД/ФТ, которые имеют большое значение, представляя собой как новые методы, вновь задействованные методы, так и традиционные методы, формирующие особое решение для сегодняшнего дня. Эта система предназначена для оперативной поддержки подотчетных организаций в их работе по выявлению, оценке и снижению связанных с их деятельностью рисков, а также по направлению отчетов о подозрительных случаях для FINTRAC. Центр FINTRAC также разработал условия формирования «Оперативных сообщений», чтобы обеспечить подотчетные организации соответствующими разъяснениями и рекомендациями по вопросам, которые относятся к возможностям подотчетных организаций надлежащим образом обеспечивать правильное и полное соблюдение канадского законодательства. В частности, указанные информационные продукты ориентированы на риски и уязвимости, связанные с практикой использования предприятий в целях ОД/ФТ, а также обязательств по отчетности СПО. В настоящее время FINTRAC также разрабатывает пакет «оперативных оповещений», связанных с ФТ, чтобы предоставлять канадским подотчетным организациям важную оперативную информацию о ФТ, включая актуальный перечень индикаторов риска / признаков рискованной деятельности (red flags), которые подотчетные организации могут использовать в своих внутренних процедурах мониторинга транзакций и внутренних расследований, что в конечном итоге увеличивает объем и качество финансовой аналитической и служебной информации, связанной с ФТ, поступающей от подотчетных организаций.

18. Частный сектор нередко нуждается в поддержке и получении конкретной оперативной информации от государственных организаций, чтобы интерпретировать те данные, которые у них уже есть. Такая поддержка может включать, например, совместное использование перечня характеристик подозрительного поведения соответствующих лиц (например, людей, находящихся

под наблюдением, надзором или по которым ведется расследование). Такая методика, основанная на соответствующих описаниях и списках, может помочь в определении отдельных подозрительных транзакций, в выявлении сети или связей субъектов, подпадающих под указанные характеристики. Однако обмен данными по таким спискам субъектов является деликатной проблемой, поскольку сохранение конфиденциальности текущих расследований и операций является приоритетной задачей для правоохранительных органов. Среди возможных способов – отнесение таких клиентов к категории высокого риска, что может привести к приостановке или прекращению бизнес-операций без применения надлежащей юридической процедуры или процесса расследования, что создает правовые проблемы. Даже если невозможно установить конкретные факты дела, общее указание на сопряженную с угрозой деятельность может помочь в привлечении ресурсов финансовой разведки. Совместное использование индикаторов риска предоставляет для подотчетных лиц возможности более успешного выявления подозрительной деятельности и предоставления эффективных отчетов о подозрительной деятельности в ПФР.

19. Частный сектор ведет учет определенных нефинансовых данных о клиенте в целях надлежащей проверки клиентов, в частности, таких данных, как IP-адреса, номера мобильных телефонов, адресов электронной почты, адресов проживания и данных геолокации в режиме реального времени для пользователей онлайн-банкинга. В сочетании с информацией от компетентных органов такие данные могут быть полезными для правоохранительных органов в целях обнаружения и расследования.

б) Обмен информацией по подозрительным счетам и транзакциям

20. Определенные условия «зоны безопасности» или конкретные порталы и межсетевые интерфейсы (шлюзы) могут обеспечить возможность обмена информацией о подозрительных транзакциях без необходимости передачи полного содержания отчетов о подозрительной деятельности. С учетом строго соблюдения требований по конфиденциальности информации, такие специальные шлюзы (порталы – *gateways*) могут способствовать улучшению обмена информацией не только между финансовыми учреждениями из разных финансовых групп, но также и в межведомственном контексте. Эти специализированные порталы нацелены на эффективный и своевременный обмен соответствующей информацией и помогают правоохранительным органам в достижении целей противодействия отмыванию денег и финансированию терроризма.

Платформа ЕС-OF2Cen

Инициатива ЕС-OF2Cen – это итальянский проект нового поколения по борьбе с интернет-мошенничеством, который сейчас разворачивается на уровне ЕС. Его цели – обеспечить систематический обмен информацией по подозрительным операциям и фактам интернет-мошенничества между банками и правоохранительными органами с целью предотвращения поступления платежей мошенникам и денежным мулам (money mules, «денежные мулы» – пособники, помогающие криминальным элементам получать доступ к краденым товарам или деньгам). Проект финансируется Европейской комиссией и поддерживается несколькими ключевыми заинтересованными учреждениями банковского сектора и органами правопорядка.

21. Сотрудничество и обмен информацией, опытом и прогнозами в отношении показателей риска, например, связанных с ФТ, международным терроризмом и небольшими террористическими ячейками, а также повышение информированности уполномоченных органов, помогает формированию возможностей частного сектора. Значительные результаты были достигнуты благодаря успешному партнерству ФАТФ и Группы Эгмонт (например, недавний отчет о показателях риска ФТ, подготовленный ФАТФ, бюллетень EGMONT, посвященный вопросам борьбы с международным терроризмом, и т.д.).

США

Правила FinCEN (Сеть по расследованию финансовых преступлений при Министерстве финансов США), функционирующей в соответствии с разделом 314 (a) Закона США о борьбе с терроризмом (Patriot Act) позволяют системе FinCEN охватить более 43 000 точек контакта в более чем 22 000 финансовых учреждениях с целью выявления счетов и сделок с лицами, которые могут быть связаны с терроризмом или отмыванием денег. В сети FinCEN формируются запросы для аналитических и следственных целей от имени федеральных, государственных, местных и некоторых иностранных органов (например, Европейского Союза) правоохранительной системы. Раздел 314 (a) Закона содержит только директивную информацию (для финансовых расследований) и не заменяет судебные запросы или судебные разбирательства, обычно предпринимаемые после выявления данных для формирования соответствующей информации с целью проведения дальнейших следственных действий или сбора доказательств.

Благодаря ускоренной системе коммуникации, процессы, реализуемые в рамках

FinCEN (раздел 314 (а)) позволяют следователю предоставлять конфиденциальную информацию о результатах расследования непосредственно представителям подотчетных организаций. FinCEN предоставляет безопасную систему электронной почты для передачи такой конфиденциальной информации. Основываясь на исходной информации, которую предоставляют финансовые учреждения, следственные органы быстро устраняют пробелы в соответствующих местах и процессах. Кроме того, в Сети FinCEN организуются и проводятся совместные обсуждения и обмен информацией с соответствующими финансовыми учреждениями для подачи запросов на информацию в соответствии с разделом 314 (а). Такое сотрудничество в рамках партнерства финансового сообщества и правоохранительных органов позволяет им выявлять, централизовать и быстро оценивать разрозненные части информации.

Кроме того, Объединенный совет национальной безопасности США (DSAC) представляет инициативу в области обеспечения безопасности и обмена информацией между ФБР, Департаментом внутренней безопасности и частным сектором, включая крупнейшие банки США. Созданный в 2005 году, Совет DSAC обеспечивает эффективный двухсторонний процесс обмена проверенной информацией между ФБР и соответствующими участниками.

Инициатива «Европейский банковский союз» (European Bankers Alliance)

В 2015 году была запущена инициатива Европейского банковского союза, в которую вошли ведущие международные финансовые учреждения, действующие в ЕС и в системе Европола. Она направлена на то, чтобы оказывать помощь финансовым институтам совместно с системой правоохранительных органов по выявлению рисков, связанных с торговлей людьми, проверять свои системы на предмет выявления подозрительных транзакций и оперативно оповещать полицейские органы.

22. Информация о терроризме и ФТ по своему характеру является строго конфиденциальной, и для нее необходимы меры защиты. Отсутствие доверия между компетентными органами и частным сектором может препятствовать обмену конфиденциальными данными. Перед государственным сектором стоит сложная задача в балансировании между обеспечением конфиденциальности секретной оперативной информации и повышением осведомленности о рисках ФТ среди заинтересованных сторон. Такая задача подчеркивает важность построения тесных отношений, основанных на взаимном доверии и поддержании конфиденциальности. Прочные формальные и неформальные связи с частным сектором могут помочь в преодолении определенных барьеров/задержек при организации доступа к информации. Например, в некоторых юрисдикциях нередко

Руководство ФАТФ

поддерживаются личные контакты компетентных органов со специалистами по отмыванию денег финансовых учреждений, через которых можно получить информацию.

Великобритания

Совместная целевая группа по вопросам отмывания денег – это общая инициатива по взаимодействию между финансовыми учреждениями, отраслевыми регуляторами, правительственными и правоохрнительными органами, действующими в Великобритании. Эта группа была создана в феврале 2015 года и в настоящее время является неотъемлемой частью ответных действий Великобритании на отмывание денег и финансирование терроризма. Цель этой инициативы – создание условий финансовому и государственному секторам для обмена и анализа информации в целях выявления, предотвращения и пресечения отмывания денег и других серьезных экономических преступлений в отношении Великобритании. Работа группы включает обмен стратегической информацией о существующих методах отмывания денег и финансирования терроризма, рисках и типологиях, которые разрабатываются и распространяются на более широкий финансовый сектор посредством адресных оповещений. Ее функции включали также обмен оперативной информацией, которая направлена на то, чтобы заполнить пробелы в работе спецслужб, когда в предполагаемых операциях по отмыванию денег задействовано несколько финансовых учреждений. Эта функция обмена оперативной информацией осуществляется через совместную операционную группу, которая еженедельно организует заседания уполномоченных сотрудников финансовых учреждений с представителями правоохрнительных органов, чтобы рассматривать и разрешать запросы, представляющие взаимный интерес. Эта работа опирается на четкие правовые рамки (положения раздела 7 Закона о расследованиях и судах) и официальное Соглашение об обмене информацией. Запросы, выполняемые в рамках этой совместной операционной группы, привели к арестам, раскрытию преступных фондов, изменениям во внутренних системах контроля банков, а также проведению новых проверок, осуществляемых банками.

с) Руководящие документы и обратная связь

23. Большое значение имеет предоставление частному сектору руководящих указаний, рекомендаций, обратной связи, в том числе для разъяснения вопросов в части ожиданий регулирующих органов в отношении выполнения требований ПОД/ФТ, а также для обеспечения обратной связи по итогам оценки отчетности. Для частного сектора это обеспечивает решение вопросов о выделении значительных ресурсов для выполнения необходимых требований и взаимодействия с правоохрнительными органами. Информация, касающаяся

возникающих рисков, моделей поведения и угроз, имеет жизненно важное значение для частного сектора, чтобы организации частного сектора могли внедрять или вносить изменения в свои системы мониторинга транзакций с учетом меняющейся ситуации и, кроме того, обеспечивать осведомленность своих сотрудников, занимающихся работой с клиентами на постоянной основе.

24. Компетентные органы могут организовывать обсуждения, распространение информации и аналитических данных, которые имеют значение для частного сектора при выявлении подозрительной деятельности. В рамках годового отчета, информационного пресс-релиза или электронного бюллетеня регулярно предоставляются данные по расследованиям, типологии по отмыванию денег и финансированию терроризма с исключением данных, не подлежащей оглашению. Более подробные версии специальных расследований или аналитика по расследованным случаям могут быть переданы через соответствующие каналы, такие как совместные обсуждения и партнерские каналы, отмеченные выше. Другим полезным механизмом, используемым для распространения информации по проведенным расследованиям и практическим примерам, а также по обновленным типологиям, являются национальные оценки рисков. Эти оценки полезны во взаимодействии с частным сектором на ранней стадии и в целях повышения его осведомленности о конкретных рисках.

25. В функции компетентных органов также входит информирование частного сектора о конкретных странах, которые могут представлять повышенный риск финансирования терроризма или определенной деятельности, представляющей зону повышенного риска. В некоторых случаях власти могут проводить подробный анализ данных по географии зон риска, касающихся границ, логистических схем или транзитных районов. В других случаях финансовые сведения, полученные правоохранительными органами (например, банкноты, квитанции и т. д.) могут быть предоставлены для финансовых учреждений, которые затем могут использовать такие данные с целью проверки на наличие соответствующих учетных записей в своей собственной системе в целях выявления любых подозрительных транзакций.

Франция

Французское ПФР предоставляет обратную связь всем организациям, которые направляют СПО. Такая функция обеспечения обратной связи осуществляется как в виде общего информирования, так и специально для отдельных организаций. Общие оценки и рекомендации предоставляются на конференциях, в годовых отчетах, при участии в работе Группы по противодействию легализации

Руководство ФАТФ

незаконных доходов при Ассоциации банков или страховщиков, на встречах с финансовыми учреждениями по вопросам соблюдения требований. Конкретные отзывы и рекомендации даются через неофициальные контакты со специалистами компаний, которым сообщается о принятии отчетности и предлагается анализ и оценка по представленной в отчете информации. Кроме того, с 3 июня 2016 года в целях организации отправки данных финансовыми учреждениями для усиления борьбы с финансированием терроризма ПФР имеет право предлагать для внесения в списки определенные физические или юридические лица, которые могут представлять повышенные высокие риски ОД/ФТ, что подразумевает применение финансовыми учреждениями расширенных мер МНПК и специальных надзорных по определенным сделкам и отдельным лицам.

Россия

Общее взаимодействие с представителями частного сектора, в том числе в целях повышения качества обмена информацией с компетентными органами и обратной связи, регулярно реализуется через Консультативный совет Межведомственной комиссии по ПОД/ФТ, где представлены крупнейшие ассоциации финансовых учреждений, и через специальный рабочий орган – «Совет комплаенс» при указанной Межведомственной комиссии, представляющий определенные организации, осуществляющие операции с денежными средствами и другими активами.

26. Руководящие указания, обратная связь и информационно-просветительская деятельность предоставляют подотчетными организациям важную или «адресную» информацию с явно выраженной целью оказания помощи частному сектору в предоставлении отчетности о подозрительной деятельности. Такой цикл («контур обратной связи») в конечном итоге приводит к еще большему охвату и информированию подотчетных организаций компетентными органами, что способствует повышению эффективности стандартов отчетности. Такое взаимодействие также предоставляет содействие частному сектору при создании необходимых типологий по определенному ряду параметров. Такая помощь может быть предоставлена с учетом конфиденциального характера информации и способа ее подачи в соответствии с запросами частного сектора.

Китай

Народный банк Китая предоставил обобщенную оценку основных параметров подозрительных операций, связанных с ФТ, разработал модель мониторинга операций, подозрительных с точки зрения ФТ, и предоставил эту модель

мониторинга своим основным КФУ и финансовым учреждениям в ключевых регионах. Использование такой модели обеспечивает значительное увеличение количества СПО, имеющих отношение к ФТ, согласно сведениям, предоставляемым финансовыми учреждениями, что способствует успешному проведению расследований и судебных преследований по случаям преступлений в области ФТ. Одним коммерческим банком на данном этапе проведена эффективная проверка операций физического лица, связанного с ИГИЛ. В настоящее время Народный банк Китая продолжает работать над оптимизацией и корректировкой указанной модели мониторинга с учетом ее практического использования.

Австралия

Регулярные встречи с соответствующими организациями частного сектора – например, Австралийский отчетно-аналитический центр транзакций (AUSTRAC) взаимодействует с частным сектором путем проведения ежеквартальных открытых встреч с приглашением ведущих обозревателей и реализацией мер по обмену информацией о моделях поведения.

Румыния

Годовой отчет румынского ПФР представляет совокупный итог стратегического анализа и, в первую очередь, направлен на предоставление соответствующей обратной связи для подотчетных организаций. В отчете представлены перспективные направления работы ПФР, с учетом его функции по сбору информации от всех участников как финансового сектора, так и некоммерческого сектора. В материале приводится описание основных категорий подозрительного финансового поведения на основе информации из представленных СПО. Благодаря своему партнерству с подотчетными организациями ПФР обеспечивает их поддержку в части информированности о задачах по предоставлению отчетности. Что им необходимо сообщать? Что должно входить в объем отчетности других организаций соответствующих секторов? Обратная связь повышает доверие и помогает подотчетным организациям развивать и регулировать свои системы выявления подозрительной деятельности. Кроме того, такие отчеты формируются с учетом координации общих усилий с правоохранительными органами.

27. Обеспечение обратной связи по качеству отчетности играет особо важную роль для обеспечения того, чтобы финансовые учреждения развивали самостоятельное управление активами и могли обновлять свои системы и процедуры. Такое сотрудничество также способствует четкому формированию надзорных функций и более эффективным мерам реагирования со стороны

Руководство ФАТФ

финансовых учреждений при реализации поставленных целей. Использование руководящих документов, особенно когда они адресованы более широкой аудитории, также способствуют формированию эффективной отраслевой практики в финансовом секторе.

Франция

Многие ПФР и отраслевые регуляторы на постоянной основе обеспечивают предоставление оценок и предложений, обеспечивая таким образом обратную связь с целью улучшения качества и объема отчетности, направляемой им финансовыми учреждениями. Например, во Франции обратная связь и информированность обеспечиваются в ходе двусторонних встреч с подотчетными организациями на ежегодной основе, а также благодаря обеспечению более широкой обратной связи при проведении общих отраслевых обсуждений.

Турция

В Турции Управление по расследованию финансовых преступлений (MASAK) регулярно встречается с комплаенс-специалистами по соблюдению банками требований в отношении вопросов ПОД/ФТ, включая риски финансирования терроризма. На этих встречах специалисты по вопросам соблюдения требований банков информируются о последних событиях, и стороны обмениваются идеями друг с другом.

Австралия

В Австралии компетентные органы предоставляют рекомендации и обратную связь по СПО на периодической основе определенному количеству заинтересованных лиц. Каждый квартал ПФР и правоохранительные органы встречаются с четырьмя крупнейшими банками для обсуждения вопросов соблюдения и предоставления обратной связи по СПО. Такие встречи привели к 300-процентному увеличению объема отчетности СПО по рискам в области ФТ после целенаправленного информирования соответствующих подотчетных лиц о показателях риска ФТ.

Гонконг, Китай

Объединенная служба финансовой разведки (JFIU) и Управление денежного обращения (НКМА) Гонконга провели совместную работу над повышением качества и количества СПО на территории своей страны. В декабре 2013 года

НКМА и JFIU выпустили руководящий документ, в котором были представлены отзывы по тематическим проверкам (в качестве конкретных указаний по качеству и соответствию отчетов), а в 2014 году было организовано специальное отраслевое обучение. Сразу после этой проведенной работы объем отчетности о подозрительной деятельности увеличился на 14% – с 27328 отчетов в 2013 году до 31095 в 2014 году. Параллельно Объединенная служба финансовой разведки предоставляет обратную связь по отраслевым секторам в рамках ежегодного обучения по ПОД/ФТ для представителей всех секторов и для отдельных организаций по специальным запросам, а Управление денежного обращения продолжает собирать отчеты СПО, выполненные банками, во время своих выездных проверок, уделяя особое внимание качеству отчетов. JFIU и НКМА предоставляют общие оценки и рекомендации для частного сектора в рамках обратной связи, например, через квартальные отчеты о подозрительной деятельности, которые публикуются на веб-сайте JFCU, также освещаются на конференциях и семинарах по ПОД/ФТ. Кроме того, специальные оценки и рекомендации предоставляются при неофициальных контактах или специальных совещаниях с подотчетными организациями, с оценками определенных примеров из отчетности.

28. Обратная связь от частного сектора по предлагаемым вариантам профиля риска и индикаторов риска ФТ может быть полезна для уточнения конечного информационного продукта; эту работу полезно выполнить до того, как итоговый документ будет выпущен компетентными органами в качестве официального руководства. Некоторые страны разработали для этой цели отдельную платформу для обсуждения рисков ФТ, а также для обеспечения обратной связи по СПО и обмена новыми аналитическими показателями и методами.

29. Информация, касающаяся случаев, происходящих в текущий момент, должна быть наиболее подробной и конкретной, чтобы частный сектор мог принять немедленные меры. Данные, которыми располагает частный сектор, могут помочь компетентным органам выявлять определенные угрозы и предоставлять информацию в режиме реального времени, например, в течение или после террористического акта. Однако конкретная информация, касающаяся определенных лиц и событий, часто подлежит ограничениям. Существуют практические проблемы в отношении текущих расследований актов терроризма или финансирования терроризма. По этой причине в ряде случаях и органы, и организации частного сектора не могут действовать надлежащим образом из-за юридических ограничений, требований конфиденциальности или юридических обязательств. Следует рассмотреть установление исключений или протоколов,

Руководство ФАТФ

чтобы обеспечить компетентным органам возможность обмениваться информацией с частным сектором, если это необходимо в срочном порядке, когда происходит реальный инцидент или развитие событий, либо когда имеются фактические случаи со смертельным исходом или потенциальная угроза человеческой жизни.

30. Некоторые страны разработали отдельный онлайн-портал и другие инструменты для подачи запросов на получение информацию от частного сектора и для безопасного и эффективного обмена информацией. Указанные меры обеспечивают приоритетность таких запросов и их своевременное рассмотрение, особенно в вопросах, связанных с терроризмом или финансированием терроризма, когда основной задачей является предотвращение возможных террористических атак.

Китай и Турция

Для направления запросов и получения отчетов организациями частного сектора, а также для предоставления информации частному сектору, в некоторых странах используются интернет-порталы (например, в Китае – система электронных информационных запросов (Digital Information Inquiring System)) для взаимодействия органов безопасности и банковского сектора. В Турции MASAK запрашивает финансовые данные в электронном виде через особый вид связи – red network, созданный в каждом банке, данные загружаются в электронном виде через такую «красную сеть». Безопасность данных обеспечивается с помощью надлежащих протоколов безопасности и аутентификации.

d) Работа с учетом отраслевой специфики, информационная и методологическая поддержка

31. Некоторые страны разработали отдельные программы взаимодействия с теми секторами, которые являются наиболее уязвимыми с точки зрения подверженности существенным рискам, включая угрозы ФТ. Такие сектора могут быть в пределах регулируемой отрасли, могут не подпадать под регулирование, но иметь важное значение с учетом возникающих тенденций и аналитики

Местные органы власти и другие заинтересованные стороны в уязвимых террористических зонах, включая сектор НКО, также могут участвовать в сотрудничестве и определении необходимых превентивных мер и других мер с целью устранения этих угроз.

Франция и Швейцария

Разъяснительная работа и информационная поддержка организаций из уязвимых

секторов являются важной стратегической задачей многих юрисдикций в борьбе с терроризмом и ФТ. Например, Министерство финансов (МФ) Франции выстроило свой формат общения с лицами, занимающимися торговлей предметами, имеющими культурно-историческую ценность и антиквариатом, чтобы привлечь их внимание к конкретным рискам ФТ, связанным с их специфической деятельностью, особенно в отношении текущей финансовой деятельности ИГИЛ. МФ Франции опубликовал Руководство для НКО, которое предлагает финансовым учреждениям принять конкретные меры для повышения информированности своих клиентов об этих специфических рисках (например, торговля нефтью с Ираком). Аналогичным образом, после публикации отчета НОР в Швейцарии, швейцарские власти инициировали диалог с представителями сектора, представляющими торговлю предметами искусства, с целью обсуждения мер ПОД/ФТ, реализуемых в данном секторе. Были проведены отдельные встречи с представителями сектора с целью повышения их осведомленности. К работе были привлечены также представители крупного международного аукционного дома.

Канада

Разъяснительная работа и информационно-методическая поддержка организаций благотворительного сектора проводятся в целях консультирования благотворительных организаций и оказания им помощи по их правовым обязательствам и способам защиты от злоупотреблений и незаконного использования таких организаций в целях терроризма. Это включает общее руководство по темам, связанным с рациональным внутренним управлением, процедурами подотчетности и прозрачной отчетностью, а также с конкретными инструментами, такими как контрольный список (checklist) для выявления незаконной деятельности, отдельная веб-страница, действующая в международном контексте. Такая информационная поддержка может принимать различные формы, включая интернет-страницы/RSS-канал, списки адресатов для рассылок по адресам электронной почты, вебинары и личные встречи.

е) Механизмы обмена информацией

32. Двусторонние отношения между частным и государственным секторами относятся к необходимым мерам борьбы с ОД/ФТ. Механизмы обмена информацией могут включать официальные заседания и неофициальные рабочие встречи как на уровне «один на один», так и с несколькими организациями. Многие страны проводят по крайней мере одну ежегодную встречу или семинар с представителями сектора, чтобы обсудить возникающие угрозы, риски и

Руководство ФАТФ

тенденции. Нередко к такой совместной работе привлекаются оперативные подразделения, например, правоохранительные органы или службы безопасности, которые приглашаются для предоставления практических примеров или конкретной информации о риске. В других случаях обсуждения рисков ОД/ФТ проводятся в рамках конференций, обучающих семинаров и тренингов для подотчетных организаций. Кроме того, такая информационно-разъяснительная работа может проводиться по инициативе частного сектора, чтобы обеспечить более широкое обсуждение потенциальных угроз преступной деятельности.

33. Возможно формирование отдельного механизма или процедуры для частного сектора в пределах определенной юрисдикции для сообщений о возможных транзакциях ФТ или, по крайней мере, таких операциях, которые имеют признаки, указывающие на то, что есть реальная угроза террористического акта в отношении правоохранительных органов/служб безопасности в ближайшее время. Это предполагает, что компетентный орган имеет отдельный канал связи для получения такого типа информации и может предпринять соответствующие действия. Среди примеров можно указать выделенные телефонные «горячие линии» или юридическое обязательство финансовых учреждений сообщать о подобных случаях сразу же, а не в течение сроков, планируемых для направления отчетности СПО.

34. В некоторых случаях государственным и частным секторами создаются специальные совместные рабочие группы ФТ или целевые группы. Такие типы целевых групп служат площадками оперативной совместных действий, что способствует улучшению работы всех участвующих сторон в области аналитических данных и расследований.

Египет

Объединение египетских банков (Federation of Egyptian Banks – FEB), созданное как некоммерческая независимая организация, объединяет все египетские банки и иностранные банки, работающие в Египте. Цели организации – предоставить возможность всем членам этого отраслевого объединения обсудить общие вопросы и обменяться мнениями в дополнение к оценкам предлагаемых законопроектов и поправок к действующему законодательству, касающихся банковского сектора.

В 2003 году по инициативе FEB была создана профессиональная Ассоциация комплаенс-специалистов. В этой ассоциации участвуют все те сотрудники банков, работающих в Египте, которые отвечают за соблюдение банком требований законодательства. Проводятся регулярные встречи по вопросам в области ПОД/ФТ. Для участия в этих встречах всегда приглашаются представители Центрального

банка и ПФР для обеспечения обратной связи и технической помощи по вопросам, которые поднимают на таких встречах комплаенс-специалисты банков.



ОБМЕН ИНФОРМАЦИЕЙ В ЧАСТНОМ СЕКТОРЕ

В руководстве определены ключевые вопросы, препятствующие обмену информацией для управления рисками ОД/ФТ между членами финансовых групп и между финансовыми учреждениями, не входящими в одну и ту же группу. В документе затрагиваются вопросы применения стандартов ФАТФ по обмену информацией, и приводятся примеры того, как органы власти могут содействовать обмену информацией, а также случаи конструктивного взаимодействия между государственным и частным секторами.

