FATF

ОБНОВЛЕНИЕ: РИСКИ ОТМЫВАНИЯ ДЕНЕГ И ФИНАНСИРОВАНИЯ ТЕРРОРИЗМА, СВЯЗАННЫЕ С ПАНДЕМИЕЙ COVID-19

Декабрь 2020

Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) является независимым межправительственным органом, который разрабатывает и поощряет политику защиты глобальной финансовой системы от отмывания денег, финансирования терроризма и распространения оружия массового уничтожения. Рекомендации ФАТФ признаны глобальным стандартом в области борьбы с отмыванием денег (AML) и финансированием терроризма (CFT).

Для получения дополнительной информации о ФАТФ посетите сайт www.fatf-gafi.org.

Настоящий документ и/или любые данные, включенные в него, не наносят ущерба статусу или суверенитету любой территории, делимитации международных границ и рубежей и названию любой территории, города или рай она.

Citing reference:

FATF (2020), *Update*: *COVID-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses*, FATF, Paris, France,
www.fatf-gafi.org/publications/methodandtrends/documents/update-covid-19-ML-TF.html

РИСКИ ОТМЫВАНИЯ ДЕНЕГ И ФИНАНСИРОВАНИЯ ТЕРРОРИЗМА, СВЯЗАННЫЕ С ПАНДЕМИЕЙ COVID-19

1. Введение

1. Всемирная организация здравоохранения (ВОЗ) объявила вспышку COVID-19 пандемией в марте 2020 года. С тех пор пандемия оказывает беспрецедентное воздействие на жизнь людей во всем мире. Страны отреагировали на это принятием различных мер в области общественного здравоохранения и осуществлением программ стимулирования, направленных на защиту отдельных лиц и компаний. Эти меры эволюционировали в течение последних шести месяцев в ответ на меняющуюся ситуацию в разных странах.

2. Изменения в поведении в результате пандемии - будь то поведение отдельных лиц, компаний или правительств - в свою очередь предоставили преступникам новые возможности для совершения преступлений и отмывания доходов. ФАТФ отслеживала эти изменения в сфере преступной деятельности, их воздействие на режимы противодействия отмыванию денег/финансированию терроризма (ПОД/ФТ), а также меры, принимаемые правительствами в ответ на различные виды возникающих проблем. В частности, в мае был опубликован документ о рисках COVID-19 и политических мерах реагирования , который был дополнен веб-конференциями с участием представителей как государственного, так и частного секторов[1].

3. С мая ФАТФ продолжает сбор и оценку соответствующей информации о воздействии пандемии. Эта оценка подтверждает, что документ о рисках и политических мерах реагирования, опубликованный ФАТФ в мае, остается актуальным. Цель настоящего документа - предоставить подотчетным субъектам, представителям частного сектора и всем заинтересованным сторонам дополнительную информацию о рисках отмывания денег и финансирования терроризма, связанных с пандемией COVID-19.

4. В настоящем документе рассматриваются как изменение характера предикатных преступлений, так и изменение деятельности по отмыванию денег и финансированию терроризма. Отдельные примеры описывают изменения в преступной деятельности, зафиксированной с начала пандемии. Более подробный перечень примеров, представленных юрисдикциями со всего мира, находится в Приложении.

2. Риски ОД/ФТ, связанные с пандемией COVID-19

2.1. Предикатные преступления

5. Анализ ФАТФ показывает, что преступники продолжают использовать новые возможности, которые появились с приходом пандемии, о чем свидетельствует рост числа случаев подделки медицинских товаров, мошенничества с инвестициями и правительственными мерами экономического стимулирования, а также случаев, адаптированных к ситуации киберпреступлений. Известны также случаи эксплуатации детей онлайн в связи с увеличением времени, проводимого в сети, рост преступлений против собственности, связанных с нежилым недвижимым имуществом, а также случаи коррупции, связанные с контрактами на поставку медикаментов.

---

[1] Информацию о первых двух онлайн-конференциях: "COVID-19 и меняющаяся ситуация рисков отмывания денег и финансирования терроризма" и "Влияние COVID-19 на выявление случаев отмывания денег и финансирования терроризма" можно найти соответственно здесь и здесь.

6. Несмотря на то, что трудно определить, связан ли рост преступной деятельности в целом с воздействием пандемии, и характер рисков в разных юрисдикциях неодинаков, ряд юрисдикций сообщает о резком увеличении числа конкретных видов преступлений. Как представляется, во многих странах такое увеличение связано с определенными видами мошенничества, такими как подделка медицинских товаров и незаконное использование мер экономического стимулирования или коррупция, связанная с государственными контрактами. Ниже приводится пример увеличения числа конкретных видов преступлений в Бразилии в результате пандемии, а также указываются меры, принятые властями для расследования и пресечения преступной деятельности [Пример 1].

Пример 1. Бразилия: COVID-19, Организованная преступность и рост предикатных преступлений

В Бразилии в период с апреля по ноябрь 2020 года федеральная полиция провела 56 полицейских операций в 17 различных штатах страны, связанных с актами коррупции или незаконного использования государственных ресурсов и отмывания денег. Эти операции завершились 133 арестами, выдачей 985 ордеров на обыск и конфискацию, а также ордеров на арест по целому ряду дел о мошенничестве с государственными контрактами на общую сумму около 1,9 млрд. бразильских реалов (примерно 360 млн. долл. США). Размеры и масштабы операций варьировались. Например, в мае в штатах Сан-Паулу и Рио-де-Жанейро в рамках операции Placebo было раскрыто мошенничество с государственными контрактами на сумму 835 млн. бразильских реалов (примерно 160 млн. долл. США), а 29 сентября в штате Пара в рамках операции S.O.S. - на сумму 500 млн. бразильских реалов (примерно 95 млн. долл. США).

Указанные дела были связаны с перечисленными ниже правонарушениями:

• завышение цен на продажу медицинского оборудования в ущерб государству и обществу,

• закупка нелицензионного медицинского оборудования,

• нарушения при отмене конкурсных заявок на заключение контрактов на приобретение респираторов,

• общее мошенничество при проведении публичных тендеров и хищение средств, предназначенных для борьбы с COVID-19,

• незаконное использование государственных ресурсов, выделенных на борьбу с пандемией,

• мошенничество при заключении контрактов на приобретение антиептиков и масок, лекарств и диагностических тестов на наличие COVID-19, а также

• нарушения при прямом заказе услуг по уборке, дезинфекции и антисептической обработке в рамках борьбы с COVID-19.

Расследования проводились по факту отмывания денег, а также незаконного использования государственных ресурсов, коррупции, мошенничества, хищений и других предикатных преступлений. Практика отмывания денег включала в себя использование банковских счетов третьих лиц и компаний, сокрытие ценностей в наличных денежных средствах, инвестиции на рынках крупного рогатого скота, а также другие виды незаконной деятельности.

Источник: Cooperação Jurídica Internacional em Matéria Penal (Международно-правовое сотрудничество по уголовным делам), Бразилия (2020).

2.1.1. Подделка медицинских товаров

7. Интерпол, Европол и другие организации считают фальсификацию медицинских товаров, таких как подделка медикаментов и средств индивидуальной защиты, серьезной угрозой.[2] Целый ряд практических примеров, представленных ФАТФ представителями Глобальной сети, а также частота сообщений об этой типологии в качестве одного из ключевых рисков позволяют предположить, что подделка медицинских товаров по-прежнему является особенно распространенным правонарушением, причем о нем сообщают из всех регионов мира. Последствия этого преступления особенно значительны. Некачественные или неконтролируемые медицинские изделия могут причинить физический вред лицам, их использующим.

Пример 2. Интерпол: Разоблачение международного мошенничества, связанного с пандемией COVID-19

В марте немецкие органы здравоохранения заключили контракт с двумя компаниями в Цюрихе и Гамбурге на закупку защитных масок на сумму 15 млн. евро. В связи с тем, что глобальная нехватка медикаментов затрудняла поиск обычных каналов закупок, покупатели искали новых поставщиков и нашли адрес электронной почты и веб-сайт, который, как выяснилось позже, был связан с одной из компаний в Испании. Они не знали, что сайт был фальшивым, а учетные записи электронной почты, указанные на нем, были взломаны.

Первоначально компания утверждала, что у нее есть 10 миллионов масок, но поставка сорвалась. После этого она направила покупателей к дилеру в Ирландии, который связал их с поставщиком в Нидерландах. С голландским поставщиком было заключено соглашение о первоначальной поставке 1,5 миллионов масок, предусматривающее предоплату в размере 1,5 млн. евро. Непосредственно перед датой поставки покупатели были проинформированы о необходимости перечислить дополнительно 880 000 евро.

Когда покупатели поняли, что их обманули, они связались со своим банком в Германии, который, в свою очередь, обратился к подразделению Интерпола по борьбе с финансовыми преступлениями. К расследованию Интерпола присоединились банки, подразделения финансовой разведки и судебные органы, а также партнерские организации Европол и Евроюст. Оперативное вмешательство позволило им заморозить 1,5 млн. евро и выявить причастную к этому ирландскую компанию. Голландские власти отследили 880 000 евро, которые были переведены из немецкого банка. Почти 500 000 евро уже были отправлены в Великобританию, и вся сумма была предназначена для перевода на счет в Нигерии.

Благодаря оповещению, осуществленному следователями, британский банк смог отозвать всю сумму. Теперь эти средства возвращены в Нидерланды и заморожены властями. В результате операции в Нидерландах были арестованы и осуждены два подозреваемых. Согласно актуальным результатам расследований, эти двое преступников действовали по поручению главного подозреваемого, который был арестован в августе в Нигерии.

[2] Для получения более подробной информации смотрите соответственно https://www.interpol.int/en/News-and-Events/News/2020/Global-operation-sees-arise-in-fake-medical-products-related-to-COVID-19 и https://www.europol.europa.eu/newsroom/news/viralmarketing-counterfeits-in-time-of-pandemic.

Рисунок 1. Международное мошенничество, связанное с пандемией COVID-19

Подписи к рис.:

DEALER	ПРОДАВЕЦ
1. 1.5 mln transfer	1. Перевод 1.5 млн. евро
2. 880k transfer	2. Перевод 880 000 евро
3. 3.500k to UK	3. Перевод 500 000 евро в Великобританию
4. 500k destined for Nigeria	4. 500 000 евро, предназначенных для перевода в Нигерию
BUYER	ПОКУПАТЕЛЬ

Источник: Интерпол (2020)

8. Примеры, представленные юрисдикциями, свидетельствуют о том, что схемы, связанные с продажей поддельных медицинских товаров или их недоставкой, могут быть как внутренними, так и международными по своему характеру – как приведенный выше пример мультинациональной компании [Пример 2] или приведенный ниже пример с ориентацией на внутренние рынки [Пример 3]. Эти виды мошенничества могут быть связаны со средствами индивидуальной защиты, фармацевтической продукцией и другими видами медицинских товаров, спрос на которые значительно возрос в последнее время.

Пример 3. Гонконг, Китай: мошенничество со средствами индивидуальной защиты

В январе 2020 года обвиняемый разместил на различных электронных торговых площадках объявление о продаже большого количества хирургических масок и спиртосодержащих дезинфицирующих средств. В период с января по март 2020 года более 200 потерпевших внутри страны заплатили за эти товары, внеся

наличные деньги или сделав электронные переводы денежных средств. В общей сложности 1,4 млн. гонконгских долларов (180 630 долл. США) было депонировано на три банковских счета в Гонконге и четыре электронных кошелька, принадлежащих супруге обвиняемого и их подельникам.

В начале марта 2020 года жертвы сообщили, что они не получили свои товары и не смогли связаться ни с одним из контактных лиц. Расследование показало, что деньги были сняты вскоре после того, как жертвы внесли их на специально выделенные банковские счета и электронные кошельки.

В апреле 2020 года правоохранительные органы арестовали четырех человек. На момент публикации настоящего доклада этим лицам не были предъявлены обвинения, расследование продолжается.

Источник: Казначейское Бюро Гонконга, Гонконг, Китай (2020 г.)

2.1.2. Киберпреступления

9. Значительное число юрисдикций из различных регионов мира сообщают о продолжающемся росте случаев мошенничества, связанного с киберпространством, включая, фишинговые схемы с использованием электронной почты и SMS-сообщений [Пример 4], взлом деловой переписки по электронной почте [Пример 5] и атаки с использованием троянских программ-вымогателей.

10. По мере того, как за последние шесть месяцев менялись действия правительств и интересы отдельных лиц, схемы фишинговой рассылки SMS-сообщений и электронных писем, связанные с COVID-19, также изменились. Теперь в них используются электронные письма с поддельными ссылками на веб-сайты с информацией о правительственной поддержке, на сайты банков, распределяющих помощь, а также на сайты с картами распространения инфекции и компаний, продающих маски. Однапроан из юрисдикций сообщила о случае, когда преступники посылали электронные письма с угрозами не только разглашения личных данных жертв, но также и заражения их и членов их семей коронавирусом, если они не заплатят преступникам.

Пример 4. Испания: Фишинговые атаки с использованием электронной почты

Департамент по борьбе с киберпреступностью Национальной полиции Испании получил сообщение о фишинговой атаке с использованием большого количества электронных писем, отправители которых выдавали себя за известную компанию, занимающуюся розничной торговлей через Интернет. Эти фишинговые атаки были направлены на получение идентификационной информации о жертвах и номерах их кредитных карт. Данные, полученные от жертвы, затем могли быть проданы другим преступным организациям или использоваться в дальнейшей мошеннической деятельности. Этот инцидент произошел в конце марта, во время первого периода карантина в начале пандемии, когда были введены жесткие ограничения на передвижение и произошел рост объема онлайновых покупок (и, следовательно, - числа фишинговых атак).

Содержание электронных сообщений указывало на то, что личный счет клиента в вышеупомянутой компании был заблокирован по соображениям безопасности из-за возможного нелегитимного доступа. Электронное сообщение также содержало ссылку на веб-страницу, создатели которой выдавали себя за компанию, занимающуюся розничной торговлей через Интернет, с целью получения информации мошенническим путем.

Незаконная деятельность была выявлена путем анализа информации и данных о транзакциях,

проанализированных специализированными полицейскими подразделениями по борьбе с киберпреступностью. В связи с возросшей активностью в режиме онлайн в период карантина эти подразделения осуществляли усиленный мониторинг или так называемое "киберпатрулирование". Преступление было связано с местными испаноязычными пользователями, судя по языку сообщений электронной почты. Расследование по этому делу продолжается.

Источник: Подразделение финансовой разведки, Испания (2020 г.)

Пример 5. Сингапур и Франция: Международное мошенничество, связанное со взломом деловой переписки по электронной почте

В марте 2020 года сингапурский банк поднял тревогу после того, как получил от французской компании сообщение об отзыве средств. Банк уведомил сингапурские власти о своих подозрениях, и, учитывая международную составляющую операции, они незамедлительно уведомили своих французских коллег о подозрительных денежных потоках и возможности мошенничества. Благодаря быстрому вмешательству и сотрудничеству с банками Департамент по коммерческим вопросам полиции Сингапура в тот же день конфисковал более 6,4 млн. сингапурских долларов (4 млн. евро).

Последующее расследование показало, что французская фармацевтическая компания стала жертвой мошенничества, связанного с фальшивыми поручениями о перечислении денег на общую сумму 6,64 млн. евро. Компания оплатила заказ на поставку хирургических масок и водно-спиртового геля для рук, сделанный своим обычным поставщикам, данные которых были украдены в результате взлома электронной почты. Французская компания была обманута после перевода 6,64 млн. евро на банковский счет в Сингапуре, принадлежащий мошенникам, т.к. не получила продукцию и не смогла связаться с поставщиком.

Позднее, в марте 2020 года, в Сингапуре был арестован 39-летний мужчина по подозрению в отмывании доходов от махинаций с медицинскими товарами, предназначенными для борьбы с COVID-19, на сумму 10,2 млн. сингапурских долларов (6,64 млн. евро). Обвинения этому лицу до сих пор не предъявлены. Было установлено, что он действовал совместно с организованной преступной группой, базирующейся за рубежом. Власти Сингапура продолжают сотрудничать с французскими властями по этому делу.

Источник: Полиция Сингапура, Министерство экономики и финансов, Франция (2020 г.).

2.1.3. Мошенничество в инвестиционной сфере

11. Юрисдикции большинства регионов продолжают сообщать о рисках мошенничества в инвестиционной сфере, связанного с мошеннической рекламой компаний, которые якобы разрабатывают так называемые "чудодейственные лекарства" от COVID-19. Мошенники привлекают жертв, делая ложные заявления о том, что их инвестиции в результате пандемии вырастут в геометрической прогрессии, при этом денежные средства затем изымаются и отмываются преступниками, действующими по этой схеме.

Пример 6. Калифорния, Соединенные Штаты Америки: Мошенничество в инвестиционной сфере

В июне 2020 года гражданин Калифорнии был обвинен в мошенничестве в связи с тем, что он призывал людей по всей стране инвестировать в компании, которые, как он утверждал, будут производить таблетки, предотвращающие заражение коронавирусом, и инъекционные лекарства для тех, кто уже страдает от COVID-19.

Посредством текстовых сообщений, видеозаписей и заявлений, отправленных потенциальным инвесторам и размещенных в Интернете, обвиняемый утверждал, что разработал лекарство от COVID-19 и профилактическое средство, предотвращающее заражение коронавирусом. В обвинительном заключении говорится, что он обманным путем вымогал инвестиции в две компании путем ложных обещаний, включая чудесные результаты использования профилактического средства и лекарства, а также безрисковую и стопроцентную гарантию "огромной прибыли" от инвестиций.

Более того, ответчик ложно заявил, что неназванная сторона в Дубае предложила приобрести две компании за 10 млрд. долл. США, утверждая, что это предложение обеспечит вложения инвесторов в две компании, и что он получил финансирование от семи инвесторов, каждый из которых уже инвестировал от 750 000 до 1 000 000 долл. США.

Обвиняемый был арестован ФБР в марте 2020 года после того, как он передал таблетки - якобы профилактическое средство, предотвращающее коронавирусную инфекцию, - агенту под прикрытием, выдававшему себя за инвестора. Ему было предъявлено 11 обвинений в мошенничестве с использованием электронных сообщений в связи с предложениями, которые он, как утверждается, сделал потенциальным инвесторам в Неваде, Нью-Йорке, Техасе и Колорадо. Два из этих обвинений были вынесены благодаря работе агента под прикрытием.

Примечание: В Соединенных Штатах обвинительный акт содержит только обвинение в совершении уголовного преступления. При этом каждый обвиняемый считается невиновным до тех пор, пока его вина не будет полностью и неоспоримо доказана в суде.
Источник: Министерство юстиции, Соединенные Штаты Америки (2020 г.)

2.1.4. Мошенническая благотворительность

12. Случаи мошенничества посредством сбора средств для фиктивных благотворительных организаций имели место на протяжении всей пандемии. При использовании этих схем мошенники связываются с отдельными лицами, вводят их в заблуждение и пытаются получить от них деньги для несуществующей благотворительной организации или используют социальные медиа-платформы для привлечения средств. В некоторых случаях мошенники обманывают жертв, действуя как представители известных благотворительных организаций, либо создают фиктивные благотворительные организации.

Пример 7. Китай: практический пример мошеннической благотворительности

W, занимавшийся сбором средств для борьбы с COVID-19, опубликовал на онлайн-платформе информацию с QR-кодом, призывая к публичным пожертвованиям. Во время пандемии более 100 человек со всего Китая вносили, отсканировав QR-код, различные суммы, в основном, кратные 10 юаням (1,50 долл. США) или 100 юаням (15 долл. США). Общая сумма пожертвований превысила 100 000 юаней (14 960 долл. США). Вскоре после перечисления денег они были переведены на личный банковский счет W. Соответствующая информация о пожертвованиях не была зарегистрирована, имелись только очевидные признаки мошеннических действий. Дело было передано в полицию для расследования.

Источник: Бюро по борьбе с отмыванием денег, Китайская Народная Республика (2020 г.)

2.1.5. Незаконное использование мер экономического стимулирования

13. Число случаев незаконного использования мер экономического стимулирования продолжает расти. За последние шесть месяцев страны увеличили число программ экономического стимулирования и расширили их масштабы. В связи с этим у преступников появились новые возможности, что привело к учащению случаев, когда отдельные лица, компании или организованные преступные группы пытаются обманным путем получить деньги у правительства.

Пример 8. Вашингтон, Соединенные Штаты Америки: Незаконное использование мер экономического стимулирования и отмывание денег

В июле 2020 года руководитель предприятия информационных технологий в штате Вашингтон был обвинен по одному пункту обвинения в мошенничестве с использованием электронных средств сообщения и по одному пункту обвинения в отмывании денег в связи с предполагаемой подачей как минимум восьми заявок на получение кредита по линии Программы поддержки бизнеса в США в связи с пандемией COVID-19 (Paycheck Protection Program, PPP) от имени шести различных компаний в кредитно-финансовые учреждения, застрахованные на федеральном уровне. Заявки были поданы на получение кредитов на сумму более 5,5 млн. долл. США. В обоснование мошеннических кредитных заявок обвиняемый, как утверждается, сделал многочисленные ложные и вводящие в заблуждение заявления о соответствующих деловых операциях компаний и расходах на заработную плату. В обвинительном акте также утверждается, что он представил фальсифицированные документы, в том числе поддельные федеральные налоговые документы и измененные учредительные документы.

В частности, утверждается, что он сообщил о том, что в одной из его компаний работают десятки сотрудников и что он выплатил миллионы долларов в виде заработной платы и налогов на заработную плату. Компания, купленная в интернете в мае 2020 года, на момент покупки фактически не имела сотрудников и не вела деловой активности. Как утверждается, обвиняемый также перечислил не менее 231 000 долл. США, полученных мошенническим путем, на свой брокерский счет в личных интересах. Это дело расследовалось Офисом Генерального инспектора Федерального агентства по финансированию жилищного строительства, Отделом уголовных расследований Федеральной налоговой службы США, Генеральным инспектором Казначейства США по налоговому администрированию и Офисом Генерального инспектора Федеральной корпорации по страхованию вкладов.

Примечание: В Соединенных Штатах обвинительный акт содержит только обвинение в совершении уголовного преступления. При этом каждый обвиняемый считается невиновным до тех пор, пока его вина не будет полностью и неоспоримо доказана в суде.
Источник: Министерство юстиции, Соединенные Штаты Америки (2020 г.)

Пример 9. Швейцария: Мошеннические заявки на получение кредита в связи с пандемией COVID-19

В середине июня 2020 года одно из кредитно-финансовых учреждений предоставила компании, работающей в строительном секторе, кредит в размере около 90 000 швейцарских франков (98 500 евро) в связи с пандемией COVID-19. Через несколько дней кредитно-финансовое учреждение было проинформировано о том, что это же предприятие обратилось за дополнительным кредитом в другое кредитно-финансовое учреждение. В то же время большая часть первоначального займа была снята наличными или потрачена на ежедневные потребительские расходы. В связи с этим кредитно-финансовое учреждение направило в швейцарское ПФР отчет о подозрительной деятельности. Дело было передано компетентным швейцарским правоохранительным органам, ведущим в настоящее время уголовное разбирательство.

Источник: Федеральный департамент финансов. Швейцария (2020 г.)

Пример 10. Италия: Организованная преступность и незаконное использование мер экономического стимулирования

В ходе расследований, завершившихся в июле 2020 года, было установлено, что члены преступной группы, связанной с организованной преступной группировкой мафиозного типа (Ндрангетой), занимались предпринимательской деятельностью, предположительно в сфере торговли металлами в Италии. Однако на самом деле этот бизнес был направлен на совершение ряда предикатных преступлений, связанных с пандемией COVID-19.

В их число входила подготовка ложных или вводящих в заблуждение налоговых деклараций, которые использовались для мошеннического получения возмещения НДС. Затем средства отмывались через банки и провайдеров услуг перевода денег или ценностей. Часть денег была отправлена в компанию, находящуюся в зарубежной стране в Европе, другая часть - в другую зарубежную страну, а преступники сняли деньги наличными с корреспондентского счета в Италии.

Мошенничество с НДС создало ложный оборот для компаний, участвующих в этой схеме, за счет чего возникли условия для получения государственных безвозмездных субсидий в связи с пандемией COVID-19. Преступная схема также использовалась для того, чтобы попытаться запросить дополнительную экономическую поддержку.

Дальнейшие расследования показали, что основной подозреваемый использовал ложный оборот, возникший в результате мошенничества с НДС, для ложного обоснования убытков, вызванных пандемией, с тем, чтобы получить безвозмездные субсидии, предоставляющиеся в качестве контрмер COVID-19 для трех компаний, входящих в эту преступную схему. Расследование также выявило попытку преступника воспользоваться государственными займами в контексте мер, направленных на поддержку экономической системы в условиях чрезвычайной ситуации, связанной с пандемией COVID-19. Правоохранительные органы арестовали активы и финансовые ресурсы на сумму около 7,5 млн. евро и произвели 10 арестов.

Источник: Guardia di Finanza (Финансовая гвардия Италии), июль (2020 г.)

14. Помимо незаконного использования государственных средств, связанного с мошенническим предоставлением займов предприятиям, заявок на субсидии и заявок на страхование по безработице, ряд юрисдикций также выразили обеспокоенность по поводу возможного неправомерного использования международной помощи, полученной в целях борьбы с пандемией. Кроме того, несколько юрисдикций сообщили также о случаях коррупции, связанных с нецелевым использованием государственных средств, предназначенных для закупки медицинского оборудования или контрактов, финансируемых государством.

Пример 11. Тунис: Незаконное присвоение помощи

В октябре 2020 года подразделение финансовой разведки Туниса (CTAF) получило от одного из кредитно-финансовых учреждений сообщение о подозрительных операциях, в котором указывалось, что гражданин Туниса (X) обналичил банковский чек на 2 млн. тунисских динаров (примерно 724 000 долл. США) и

положил деньги на счет своей фирмы, компании С. Х утверждал, что якобы этот чек был выписан ему в консульстве иностранного государства с целью обеспечения 2 000 иностранных граждан, находившихся в Тунисе в период карантина, жильем, медикаментами, припасами и средствами для проведения теста на наличие COVID-19.

В тот же день, когда Х обналичил чек, он перевел всю сумму на различные счета физических лиц, клиник и фирмы своего брата - компании А. Вскоре после этого CTAF получило еще одно сообщение о подозрительных операциях от другого кредитно-финансового учреждения, причиной которого стал тот факт, что на счет компании А в тот же день поступило пять идентичных электронных переводов от компании С на общую сумму 400 000 тунисских динаров (145 000 долл. США).

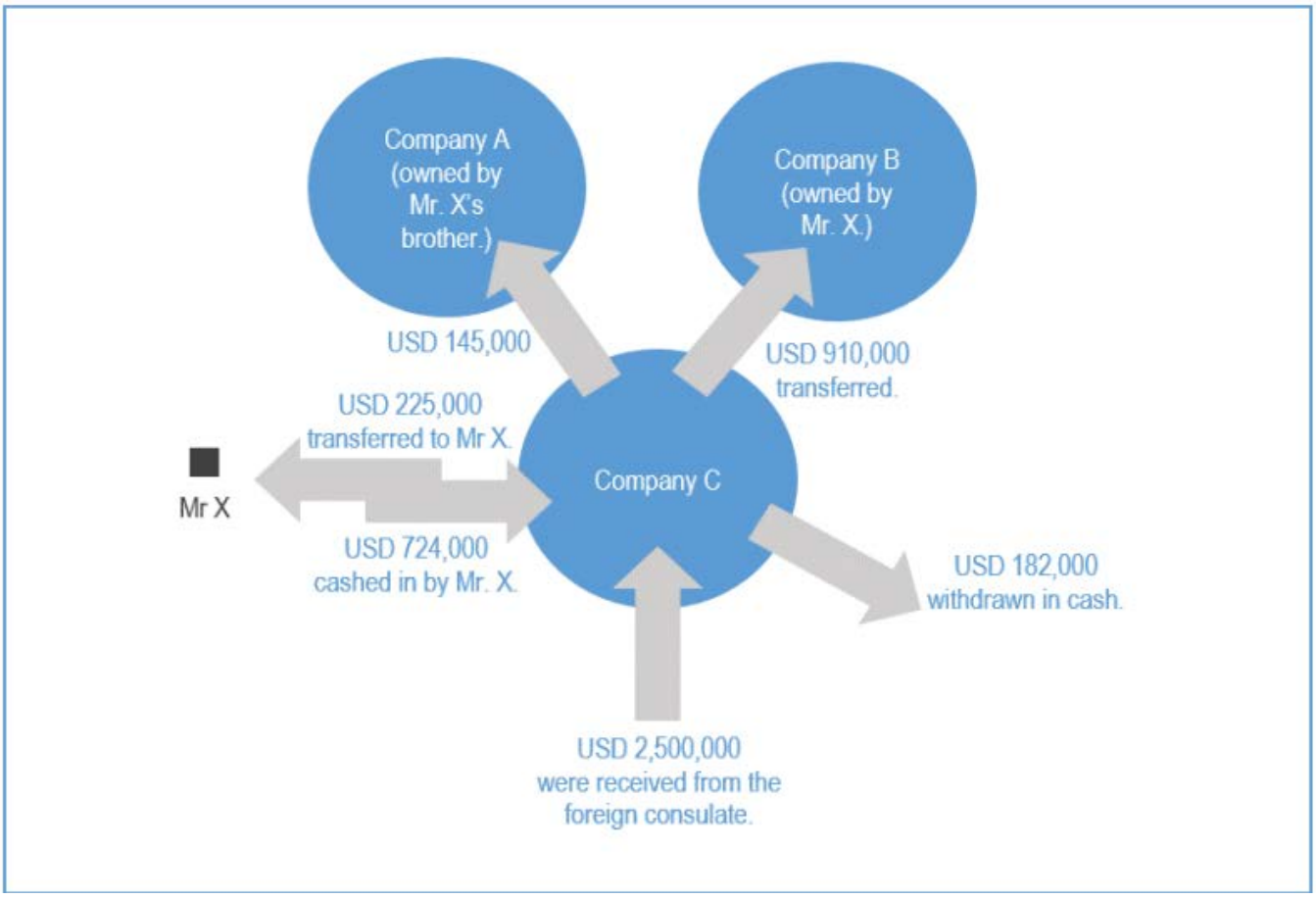
Дальнейший анализ показал, что в течение короткого промежутка времени (менее 6 месяцев с момента открытия счета) компания С получила шесть электронных переводов только от упомянутого консульства на общую сумму почти 7 млн. тунисских динаров (2,5 млн. долл. США). Вскоре после этого 500 000 тунисских динаров (182 000 долл. США) были сняты наличными, 2,5 млн. тунисских динаров (910 000 долл. США) были переведены на счет Компании В (принадлежавшей Х), а 700 000 тунисских динаров (255 000 долл. США) были переведены на личный счет Х.

Х потратил 15% от суммы, полученной от иностранного консульства, на гостиницы, клиники и аптеки. В договоре, заключенном между консульством и компанией С, не были определены требуемые от компании услуги, цены, а также связанные с ними налоги. Кроме того, компания С не имеет других банковских счетов и не ведет хозяйственной деятельности. Также было установлено, что переводы, направляемые в компанию А, были основаны на фальсифицированных счетах на оплату, содержащих аномально высокие цены по сравнению с теми, которые обычно взимаются.

В результате, сотрудники CTAF пришли к выводу, что Х использовал подставную компанию (компания С), семейные компании и фальсифицированные счета на оплату, чтобы направить государственную помощь, предоставленную иностранным государством своим гражданам, оказавшимся в затруднительном положении в Тунисе из-за пандемии COVID-19. В качестве превентивной меры CTAF приказало заморозить счета компаний А, В и С и банковский счет Х. Кроме того, CTAF по своей инициативе направило информацию в иностранное подразделение финансовой разведки и препроводило отчет прокурору. Расследование продолжается.

Источник: Подразделение финансовой разведки, Тунис (2020 г.)

Рисунок 2. Тунис: Незаконное присвоение помощи



Подписи к рис.:

Mr. X	X
Company A (owned by Mr. X's brother)	Компания А, владельцем которой является брат X
USD 1450,000	1 450 000 долл. США
USD 225,000 transferred to Mr. X	225 000 долл. США поступили на счет X
USD 724,000 cashed in by Mr. X	724 000 долл. США были обналичены X
Company C	Компания С
USD 2,500,000 were received from the foreign consulate	2 500 000 долл. США были получены от иностранного консульства
Company B (owned by Mr. X)	Компания В, владельцем которой является X
USD 910,000 transferred	910 000 долл. США
USD 182,000 withdrawn in cash	182 000 долл. США, снятые со счета наличными

Источник: Подразделение финансовой разведки, Тунис (2020 г.)

2.2. Риски отмывания денег и финансирования терроризма

15. Вероятно, что в ближайшие месяцы, по мере продолжения воздействия пандемии COVID-19, риски отмывания денег станут более очевидными. При этом в юрисдикциях по-прежнему наблюдаются некоторые из уязвимостей, выявленных ФАТФ ранее в этом году на фоне пандемии.

16. Уязвимости связаны с изменением финансового поведения, в частности ростом числа удаленных операций, что влияет на способность финансовых учреждений выявлять отклонения от нормы. В условиях

роста безработицы и увеличения числа граждан, осуществляющих операции удаленно, существует также риск того, что уязвимые граждане могут эксплуатироваться в качестве курьеров наличных.

17. Другие уязвимости связаны с возросшей финансовой нестабильностью, вызванной глобальным экономическим спадом вследствие принятия мер по ограничению распространения COVID-19. К ним относятся увеличение объема наличных средств в обращении и использование виртуальных активов.

18. Во многих юрисдикциях не было выявлено изменений в рисках финансирования терроризма в результате пандемии, хотя некоторые из них обозначили потенциальные уязвимости. Они связаны с незаконным использованием некоммерческих организаций и повышенным уровнем угрозы совершения характерных предикатных преступлений.

2.2.1. Изменение финансового поведения

19. Изменения в поведении клиентов продолжают затруднять для финансовых учреждений выявление отклонений от нормы. Например, финансовые модели клиентов меняются вследствие того, что они работают из дома и проводят больше операций в Интернете. В некоторых странах, где дистанционные операции и услуги используются реже, подотчетные субъекты, возможно, еще не привыкли содействовать осуществлению операций или предлагать услуги дистанционно. Это затрудняет для них проведение эффективной комплексной проверки клиентов или постоянного мониторинга. В некоторых случаях переход на дистанционную работу повлиял на эффективность систем и механизмов контроля подотчетных субъектов, при этом сотрудники, отвечающие за соблюдение требований, не могли выполнять свои функции с той же эффективностью, с какой они выполняли их до пандемии.

20. Эффективное использование технологий, независимо от того, используются ли они для адаптации нового сотрудника при поступлении на работу или для обеспечения эффективного обмена информацией между компетентными органами и подотчетными субъектами, приобретает еще большее значение, поскольку изменения в поведении клиентов и меры по социальному дистанцированию означают, что очное взаимодействие не всегда возможно.

21. Меняющийся ландшафт рисков также означает, что индикаторы рисков следует регулярно обновлять и корректировать, а для обмена информацией по мере изменения рисков с течением времени необходима эффективная постоянная связь между государственным и частным секторами.

Пример 12. Незаконное использование неактивных счетов в Эфиопии

Сотрудник банка незаконно снял со счета неактивного клиента 3 миллиона эфиопских быров (68 300 евро) и одолжил их своему другу без залога. Когда внутренние аудиторы банка обнаружили незаконное снятие денег с неактивного счета, они сообщили об этом случае в Центр финансовой разведки Эфиопии как о подозрительной операции. Затем Центр провел анализ и отправил его результаты в правоохранительные органы для дальнейшего уголовного расследования. Как сотрудник банка, так и лицо, получившее деньги, находятся под следствием. Они обвиняются в коррупции и других связанных с ней финансовых преступлениях и временно освобождены из-под стражи под залог. Следствие по делу продолжается.

Это преступление было совершено в период чрезвычайного положения, объявленного в Эфиопии в целях сдерживания пандемии COVID-19. Вследствие этого лишь 50% сотрудников работали в банке, а остальные - на дому. Это позволило сотруднику получить доступ к системе и совершить преступление. Кроме того,

многие предприятия постоянно были бездействующими во время чрезвычайного положения. Оба сценария создавали уязвимости. Кроме того, системы контроля в финансовых учреждениях были ослаблены в связи с уменьшением количества сотрудников, физически присутствующих в банках, для осуществления мер по установлению личности и комплексной проверке клиентов и т.п.

Источник: Центр финансовой разведки Эфиопии (2020 г.)

2.2.2. Повышение финансовой нестабильности и спад экономики

22. Многие юрисдикции сталкиваются с экономическим спадом, также являющимся причиной возникновения уязвимостей с точки зрения возможностей для отмывания денег. Один из рисков заключается в том, что средства из незаконных источников могут быть использованы для эксплуатации предприятий, находящихся в бедственном положении или подверженных быстрой смене спроса посредством предоставления капитала или поглощения. Сектора недвижимости, строительства, промышленной уборки и транспортных услуг, а также малые и средние предприятия в целом, по-видимому, являются особенно уязвимыми.

23. Между тем, опасения по поводу состояния экономики привели к увеличению объемов наличных денежных переводов и наличного денежного обращения. В сочетании с закрытием границ и ограничениями на передвижение физических лиц это привело к росту использования преступными группировками фиатной валюты для хранения наличных денег и отмывания доходов от своих преступлений.

24. К другим уязвимым областям относятся лица, обращающиеся за нерегулируемыми финансовыми услугами, и мошенничество с целью привлечения лиц, которые, возможно, потеряли работу или лишились дохода и потенциально могут быть использованы в качестве курьеров наличных. Повышенная финансовая нестабильность также создает предпосылки для совершения инсайдерских торговых операций в результате больших скачков цен в условиях пандемии.

25. В связи с возросшей финансовой нестабильностью могут появиться дополнительные уязвимости, связанные с незаконным использованием виртуальных активов (ВА) в схемах, использующих ситуацию с пандемией (например, оплата в таких схемах мошенничества может производиться при помощи ВА). Это в значительной степени объясняется тем, что, как и в случае с наличными деньгами (см. выше), накопление ВА увеличивается в тех случаях, когда имеется озабоченность нестабильностью экономики.

26. Компетентные органы отмечают еще ряд проблем, связанных с ВА, в том числе мошенничество с использованием лиц, потерявших работу или отправленных в неоплачиваемый отпуск, в качестве курьеров наличных. В одной из типологий описывается, что преступники, выдавая себя за законных работодателей, обращаются к своим жертвам с просьбой принять "пожертвование" на собственный банковский счет и положить денежные средства в крипто-киоск. Если эти средства незаконны, жертва невольно соглашается принять участие в отмывании денег, выступая в роли курьера наличных.

Пример 13. Гонконг, Китай: Мошенничество, связанное с виртуальными активами и пандемией COVID-19

В период с конца февраля по начало марта 2020 года владелица компании, занимающейся торговлей товарами медицинского назначения в Гонконге (Китай), увидела в Интернете рекламу, размещенную несколькими предполагаемыми продавцами хирургических масок и медицинского оборудования, в том

числе на крупной социальной медиа-платформе. При попытке приобрести это оборудование, она была обманута, перечислив 450 000 гонконгских долларов (58 000 долл. США) на различные банковские счета в Гонконге, Китай, и восточноевропейской стране, а также конвертировав 3,96 млн. гонконгских долларов (510 000 долл. США) в эквивалентную сумму в Bitcoin. Для этого потерпевшая сняла наличные деньги со своего личного банковского счета и положила их в специально определенный банкомат Bitcoin, где средства были переведены в специально отведенные для этого кошельки Bitcoin. В общей сложности были задействованы три банка, расположенных в двух юрисдикциях (Гонконг, Китай, и восточноевропейская юрисдикция). Пять переводов на сумму от 47 250 до 235 830 долл. США были переведены на счета, принадлежащие преступнику. Все мошенники перестали отвечать на запросы жертв после получения платежа. Расследование продолжается.

Источник: Казначейское Бюро Гонконга, Гонконг, Китай (2020 г.)

3. Заключение

27. Последствия пандемии продолжают существовать в разных проявлениях. Следовательно, изменения как в области отмывания денег, так и в области финансирования терроризма на фоне пандемии, по всей вероятности, также будут происходить. Растущая безработица, финансовые трудности, банкротство компаний, увеличение оборота наличных средств в экономиках, потенциальное накопление наличности организованными преступными группами и ускоренная реализация программ стимулирования являются факторами уязвимости, которыми преступники могут воспользоваться в ближайшие месяцы во все большей степени. Кроме того, по мере ускорения создания новых вакцин против COVID-19, преступники также будут иметь возможность разрабатывать преступные аферы с целью эксплуатации новых достижений в области медицины для незаконного получения прибыли.

28. Несмотря на выявление ряда глобальных тенденций, некоторые риски могут быть характерными для конкретных стран или регионов. ФАТФ будет продолжать осуществлять мониторинг воздействия пандемии на глобальные риски ОД/ФТ, а также на режимы ПОД/ФТ, работая в тесном сотрудничестве с организациями-наблюдателями и сетью региональных организаций, созданных по типу ФАТФ, чтобы принимать во внимание региональную специфику. ФАТФ будет и в дальнейшем предоставлять информацию в случае значительного видоизменения последствий пандемии.

29. Для юрисдикций, кредитно-финансовых учреждений и установленных нефинансовых предприятий и профессий по-прежнему чрезвычайно важно выявлять, оценивать и понимать конкретные риски ОД/ФТ, с которыми они сталкиваются, и принимать соответствующие меры по их снижению в соответствии с Рекомендациями ФАТФ.

30. Ваши отзывы о настоящем отчете или о мерах реагирования ФАТФ на пандемию COVID -19 вы можете направить нам по электронной почте: secretariat@fatf-gafi.org.

Приложение A. Список практических примеров, связанных с пандемией COVID-19

Примеры рисков ОД/ФТ, связанных с пандемией COVID-19, включая вошедшие в отчет

Расследование многих из этих дел еще не закончено. Если не указано иное, по некоторым делам лишь предъявлены обвинения в совершении преступления, а обвиняемые имеют право считаться невиновными до тех пор, пока их виновность не будет установлена законным порядком путем гласного судебного разбирательства.[3]

Данный список дел, связанных с пандемией COVID-19, в которых фигурируют риски ОД/ФТ, не следует считать исчерпывающим. Это краткий перечень имеющихся на данный момент практических примеров по указанной теме, сведения о которых были раскрыты для публикации.

Тип преступления	Юрисдикция(и)	Описание
Организованная преступная деятельность	Бразилия	В Бразилии в период с апреля по ноябрь 2020 года федеральная полиция провела 56 полицейских операций в 17 различных штатах страны, связанных с актами коррупции или незаконного использования государственных ресурсов и отмывания денег. Эти операции завершились 133 арестами, выдачей 985 ордеров на обыск и конфискацию, а также ордеров на арест по целому ряду дел о мошенничестве с государственными контрактами на общую сумму около 1,9 млрд. бразильских реалов (примерно 360 млн. долл. США). Размеры и масштабы операций варьировались. Например, в мае в штатах Сан-Паулу и Рио-де-Жанейро в рамках операции "Placebo" было раскрыто мошенничество с государственными контрактами на сумму 835 млн. бразильских реалов (примерно 160 млн. долл. США), а 29 сентября в штате Пара в рамках операции "S.O.S." - на сумму 500 млн. бразильских реалов (примерно 95 млн. долл. США). Указанные дела были связаны с перечисленными ниже правонарушениями: • завышение цен на продажу товаров медицинского назначения в ущерб государству и обществу, • закупка нелицензионного медицинского оборудования, • нарушения при отмене конкурсных заявок на заключение контрактов на приобретение респираторов, • общее мошенничество при проведении публичных тендеров и хищение средств, предназначенных для борьбы с COVID-19, • незаконное использование государственных ресурсов, выделенных на борьбу с пандемией, • мошенничество при заключении контрактов на приобретение антиептиков и масок, лекарств и диагностических тестов на наличие COVID-19, а также • нарушения при прямом заказе услуг по уборке, дезинфекции и антисептической обработке для борьбы с COVID-19. Расследования проводились по факту отмывания денег, а также незаконного использования государственных ресурсов, коррупции, мошенничества, хищений и других предикатных преступлений. Практика отмывания денег включала в себя

[3]В соответствии с Всеобщей декларацией прав человека (1948 г.). См. здесь.

		использование банковских счетов третьих лиц и компаний, сокрытие ценностей в наличных денежных средствах, инвестиции на рынках крупного рогатого скота, а также другие виды незаконной деятельности. Пример 1 Источник: Cooperacao Juridica Internacional em Materia Penal (Международно-правовое сотрудничество по уголовным делам), Бразилия (2020 г.).
Подделка медицинских товаров – мошенничество со средствами индивидуальной защиты	Германия, Испания, Нидерланды, Ирландия, Великобритания, Нигерия	В марте немецкие органы здравоохранения заключили контракт с двумя компаниями в Цюрихе и Гамбурге на закупку масок для лица на сумму 15 млн. евро. В связи с тем, что глобальная нехватка медикаментов затрудняла поиск обычных каналов закупок, покупатели искали новых поставщиков и нашли адрес электронной почты и веб-сайт, который, как оказалось, был связан с одной из компаний в Испании. Они не знали, что сайт был фальшивым, а учетные записи электронной почты, указанные на нем, были взломаны.

		Первоначально компания утверждала, что у нее есть 10 миллионов масок, но поставка сорвалась. После этого она направила покупателей к дилеру в Ирландии, который связал их с поставщиком в Нидерландах. С голландским поставщиком было заключено соглашение о первоначальной поставке 1,5 миллионов масок, предусматривающее предоплату в размере 1,5 млн. евро. Непосредственно перед датой поставки покупатели были проинформированы о необходимости перечислить дополнительно 880 000 евро. Когда покупатели поняли, что их обманули, они связались со своим банком в Германии, который, в свою очередь, обратился к подразделению Интерпола по борьбе с финансовыми преступлениями. К расследованию Интерпола присоединились банки, подразделения финансовой разведки и судебные органы, а также партнерские организации Европол и Евроюст. Оперативное вмешательство позволило им заморозить 1,5 млн. евро и выявить причастную к этому ирландскую компанию. Голландские власти отследили 880 000 евро, которые были переведены из немецкого банка. Почти 500 000 евро уже были отправлены в Великобританию, и вся сумма была предназначена для перевода на счет в Нигерии. Благодаря оповещению, сделанному следователями, британский банк смог отозвать всю сумму. Теперь эти средства возвращены в Нидерланды и заморожены властями. В результате операции в Нидерландах были арестованы и осуждены два подозреваемых. Согласно нынешним результатам расследований, эти двое преступников действовали по поручению главного подозреваемого, который был арестован в августе в Нигерии. Пример 2 Источник: Интерпол (2020 г.)
Подделка медицинских товаров – мошенничество	Гонконг, Китай, Республика Корея	На ранней стадии пандемии, когда у многих появилось ощущение страха в связи с нехваткой медицинских средств защиты в условиях распространения COVID-19, пострадавший пытался закупить хирургические маски, воспользовавшись

со средствами индивидуальной защиты		рекламой в Instagram. Он начал общаться с мошенником, который попросил осуществить авансовый платеж для подтверждения заказа. Пострадавший отправил 54 250 евро на корейский банковский счет в соответствии с инструкциями мошенника. После этого продавец перестал общаться с пострадавшим. Об этом деле было сообщено правоохранительным органам, которые предупредили Национальное центральное бюро Интерпола (НЦБ) в Гонконге. В феврале Гонконгское бюро Интерпола направило в Сеул запрос об оказании помощи в проведении этого расследования. Были также установлены контакты с ПФР в каждой соответствующей стране, которые, в свою очередь, поддерживали связь с соответствующим кредитно-финансовым учреждением. Благодаря оперативному взаимодействию всех участников расследования двое подозреваемых были арестованы через четыре дня после получения заявления потерпевшего, а вся сумма была возвращена на его счет. Источник: Интерпол (2020 г.)
Подделка медицинских товаров – мошенничество со средствами индивидуальной защиты	Италия, Индонезия	В мае 2020 года итальянская компания вела переговоры с китайской компанией о закупке большого количества медицинского оборудования, в том числе ИВЛ и оборудования для мониторинга пациентов, больных коронавирусом. Злоумышленники получили доступ к электронной переписке между двумя компаниями и убедили итальянских покупателей сделать три банковских перевода на общую сумму 3,67 млн. евро на контролируемый ими счет в Индонезии. Считая, что это был законный поставщик, итальянская компания осуществила денежные переводы. Мошенничество было обнаружено, когда поставщик в Китае сообщил итальянской компании, что не получал платежи за приобретенное медицинское оборудование. Дальнейшие проверки показали, что имел место взлом электронной переписки, в результате которого было произведено перенаправление средств на банковский счет в Индонезии. В связи с этим, пострадавшая компания обратилась в итальянскую полицию. Через НЦБ Интерпола в Риме была запрошена помощь Подразделения по борьбе с финансовыми преступлениями Интерпола. Интерпол содействовал установлению связей с индонезийскими властями через свою глобальную сеть. Правоохранительные органы связались с ПФР и кредитно-финансовыми учреждениями в каждой юрисдикции. Взаимодействие между соответствующими субъектами, занимающимися борьбой с отмыванием денег, быстро привела к перехвату и замораживанию в начале июня 3,1 млн. евро похищенных мошенниками платежей. В целях дальнейшей поддержки расследования в августе Интерпол провел виртуальное координационное совещание с ключевыми заинтересованными сторонами в Италии и Индонезии, включая НЦБ Интерпола в Риме, Итальянскую почтовую полицию, Национальное центральное бюро в Джакарте, а также Подразделение финансовой разведки и Департамент уголовных расследований Индонезии.

		Все они поделились важными следственными деталями и работали вместе, чтобы обезопасить замороженные активы и установить местонахождение подозреваемых в мошенничестве. После совещания индонезийские власти выявили трех подозреваемых, которые являлись частью более широкой преступной сети, причастной к мошенничеству. Они были арестованы в начале сентября, когда полиция арестовала также наличные средства и имущество, которое, как утверждалось, было приобретено на украденные деньги. Расследование деятельности преступного синдиката продолжается с тем, чтобы установить, не было ли еще потерпевших из других стран. Источник: Интерпол (2020)
Подделка медицинских товаров – мошенничество со средствами индивидуальной защиты	Гонконг, Китай	В январе 2020 года обвиняемый разместил на различных электронных торговых площадках объявление о продаже большого количества хирургических масок и спиртосодержащих дезинфицирующих средств. В период с января по март 2020 года более 200 потерпевших внутри страны заплатили за эти товары, внеся наличные деньги или сделав электронные переводы денежных средств. В общей сложности 1,4 млн. гонконгских долларов (180 630 долл. США) было депонировано на три банковских счета в Гонконге и четыре электронных кошелька, принадлежащих супруге обвиняемого и их партнерам. В начале марта 2020 года жертвы сообщили, что они не получили свои товары и не смогли связаться ни с одним из контактных лиц. Расследование показало, что деньги были сняты вскоре после того, как жертвы внесли их на специально созданные банковские счета и электронные кошельки. В апреле 2020 года правоохранительные органы арестовали четырех человек. На момент публикации настоящего отчета этим лицам не были предъявлены обвинения, расследование продолжается. Пример 3 Источник: Казначейское Бюро Гонконга, Гонконг, Китай (2020 г.)
Подделка медицинских товаров – мошенничество со средствами индивидуальной защиты	Германия	В конце февраля 2020 года немецкая компания заказала большое количество защитных масок у поставщика из страны, не являющейся членом ЕС. Ему был перечислен авансовый платеж в размере крупной шестизначной суммы в евро (примерно 50% от покупной цены). Однако поставка не была произведена. На все попытки установления контакта немецкая компания ответа не получила. Правоохранительный орган направил срочный запрос в ПФР Германии. После этого ПФР Германии незамедлительно запросило информацию у ПФР страны, не являющейся членом ЕС, а также сделало дополнительный запрос о замораживании денежных средств или блокировании банковского счета получателя. ПФР страны, не являющейся членом ЕС, заморозило денежные средства в тот же день. Немецкое ПФР было проинформировано о замороженных средствах, после чего был установлен прямой контакт с правоохранительным органом в Германии и находившимся там сотрудником по связям и взаимодействию с ПФР. После этого прокуратура добилась ареста имущества,

		направив запросы об оказании административной и правовой помощи по обычным судебным каналам, предусмотренным для этой цели. Кроме того, информация об аресте имущества была также передана в ПФР страны, не являющейся членом ЕС. Источник: Федеральное министерство финансов, Германия (2020 г.)
Подделка медицинских товаров – мошенничество со средствами индивидуальной защиты	Люксембург	В марте 2020 года в ПФР Люксембурга поступил срочный запрос о предоставлении информации в отношении компании, расположенной в Люксембурге и предлагающей значительное количество хирургических масок для продажи правительству страны-члена ЕС. В условиях общемировой пандемии COVID-19, приведшей к нехватке медицинского и защитного оборудования, возникли сомнения в серьезности этого предложения и намерений компании, сделавшей его. Сомнения еще более усилились в связи с тем, что банковский счет, упомянутый в счете на оплату, выписанном люксембургской компанией, находился в другой юрисдикции (Страна А). Предварительный анализ ПФР Люксембурга показал, что компания, зарегистрированная в 2013 году, является холдинговой компанией, не приносящей дохода и владеющей долей в другой компании, находящейся в стране В. Кроме того, у компании отсутствовал номер плательщика НДС и разрешение на торговлю. Поскольку компания владела долей в трастовой компании, являющейся подотчетным субъектом, ПФР запросило банковские выписки для дальнейшего анализа. Оказалось, что компания имела в стране А только банковские счета, но с момента регистрации в 2013 году никаких торговых операций она не производила. ПФР Люксембурга сотрудничает с ПФР страны А. Кроме того, ПФР Люксембурга было проинформировано о том, что компания находится в процессе продажи бизнеса и что стал известен потенциальный покупатель. Так как у компании были

		неоплаченные счета, трастовая компания приняла решение о расторжении контракта, а директор компании ушел в отставку. Источник: Подразделение финансовой разведки, Люксембург (2020 г.)
Подделка медицинских товаров – мошенничество со средствами индивидуальной защиты	Малайзия	ПФР Малайзии получила от одной из европейских стран (страна А) запрос на предоставлении информации о предполагаемом мошенничестве с защитными масками, связанном с пандемией COVID-19. Примерно 5 млн. евро было передано государственным агентством в стране А организации в стране А, а именно компании ABC, для покупки защитных масок в стране В. Как выяснилось, только часть масок была доставлена, но все они были признаны непригодными для использования. Данные финансовой разведки, собранные впоследствии в стране А, показали, что компания ABC, возможно, впоследствии перевела значительную сумму денег, предназначенную для приобретения масок, другой организации, а именно компании XYZ в Малайзии.

		Дальнейшая проверка операций по счету компании также выявила входящий денежный перевод, полученный компанией XYZ от организации, расположенной в стране C, с примечаниями по операциям, которые потенциально могут указывать на то, что эти операции связаны с защитными масками. В тот же день была получена еще одна крупная сумма денежных средств в размере примерно 150 000 долл. США от компании DEF, другой организации, расположенной в стране A, которая, как предполагается, занимается продажей медицинских товаров, включая перчатки, очки и средства защиты органов слуха. Было отмечено, что денежные средства, полученные компанией XYZ, были распределены между различными организациями в стране C и стране D. Источник: Подразделение финансовой разведки, Малайзия (2020 г.)
Подделка медицинских товаров – мошенничество со средствами индивидуальной защиты	Малайзия	ПФР Малайзии получило от одной из европейских стран (страна E) запрос на предоставление информации о предполагаемом мошенничестве с использованием защитного оборудования для тестирования на наличие COVID-19. Национальное агентство здравоохранения, расположенное в стране E, получило коммерческое предложение от компании OPQ, расположенной в стране E, о приобретении защитного оборудования для тестирования на наличие COVID-19 на сумму в несколько миллионов евро. Национальное агентство здравоохранения, расположенное в стране E, подписало контракт на поставку оборудования по завышенной цене, т.к. было обмануто компанией OPQ, предоставившей ложную информацию о продукции. Данные финансовой разведки, собранные впоследствии в стране E, показали, что компания OPQ, возможно, впоследствии перевела 6,05 млн. евро, предназначенных для закупки защитного оборудования для тестирования на наличие COVID-19, через сети компаний, в которые входили компании, расположенные в стране E и двух соседних странах, другой организации, а именно компании RST, расположенной в Малайзии. Анализ операций по счету компании позволили выявить платежный паттерн, заключающийся в быстром и частом осуществлении входящих и исходящих операций с участием нескольких контрагентов, а именно входящего перевода SWIFT и исходящего банковского перевода в другую страну. Дальнейшее изучение счета показало, что компания RST получила входящий перевод от компании UVW, расположенной в одной из соседних стран. Позднее полученные средства были перечислены организациям, расположенным за пределами Малайзии, посредством электронных переводов. Источник: Подразделение финансовой разведки, Малайзия (2020 г.)
Подделка медицинских товаров – мошенничество со средствами индивидуальной	Финляндия	Финская государственная структура приобрела 3,1 миллиона масок примерно на 5 миллионов евро у частной финской компании. Эта компания, в свою очередь, приобрела товар у продавца в Китае. Однако сразу после покупки выяснилось, что у частной финской компании сомнительная деловая история, а качество большей части поставляемых

защиты		медицинских товаров было низким. ПФР обнаружило сомнительную деловую историю во время плановых проверок. Отсутствовала налоговая отчетность, имелась просроченная налоговая задолженность за прошлые финансовые годы, кроме того, компания была исключена из некоторых официальных баз данных. Дело по-прежнему расследуется как мошенничество при отягчающих обстоятельствах. В ходе расследования были конфискованы активы на сумму 2,6 млн. евро. Источник: Подразделение финансовой разведки, Финляндия (2020 г.)
Киберпреступление	Сингапур, Франция	В марте 2020 года сингапурский банк поднял тревогу после того, как получил от французской компании сообщение об отзыве средств. Банк уведомил сингапурские власти о своих подозрениях, и, учитывая международную составляющую операции, они незамедлительно уведомили своих французских коллег о подозрительных денежных потоках и возможности мошенничества. Благодаря быстрому вмешательству и сотрудничеству с банками Департамент по коммерческим вопросам полиции Сингапура в тот же день конфисковал более 6,4 млн. сингапурских долларов (4 млн. евро).

		Последующее расследование показало, что французская фармацевтическая компания стала жертвой мошенничества, связанного с фальшивыми поручениями о перечислении денег на общую сумму 6,64 млн. евро. Компания оплатила заказ на поставку хирургических масок и водно-спиртового геля для рук, сделанный своим обычным поставщикам, данные которых были украдены в результате взлома электронной почты. Французская компания была обманута после перевода 6,64 млн. евро на банковский счет в Сингапуре, принадлежащий мошенникам, т.к. не получила продукцию и не смогла связаться с поставщиком. Позднее, в марте 2020 года, в Сингапуре был арестован 39-летний мужчина по подозрению в отмывании доходов от махинаций с медицинскими товарами, предназначенными для борьбы с COVID-19, на сумму 10,2 млн. сингапурских долларов (6,64 млн. евро). Обвинения этому лицу до сих пор не предъявлены. Было установлено, что он действовал совместно с организованной преступной группой, базирующейся за рубежом. Власти Сингапура продолжают сотрудничать с французскими властями по этому делу. Пример 5 Источник: Полиция Сингапура, Министерство экономики и финансов, (Франция).
Киберпреступление	Испания	Департамент по борьбе с киберпреступностью Национальной полиции Испании получил сообщение о фишинговой атаке с использованием большого количества электронных писем, отправители которых выдавали себя за известную компанию, занимающуюся розничной торговлей через Интернет. Эти фишинговые атаки были направлены на получение идентификационной информации о жертвах и номерах их кредитных карт. Данные, полученные от жертвы затем могли

		быть проданы другим преступным организациям или использоваться в дальнейшей мошеннической деятельности. Этот инцидент произошел в конце марта, во время первого периода карантина в начале пандемии, когда были введены жесткие ограничения на передвижение и произошел рост объема онлайновых закупок (и, следовательно, - числа фишинговых атак). Содержание электронных сообщений указывало на то, что личный счет клиента в вышеупомянутой компании был заблокирован по соображениям безопасности из-за возможного нелегитимного доступа. Электронное сообщение также содержало ссылку на веб-страницу, создатели которой выдавали себя за компанию, занимающуюся розничной торговлей через Интернет, с целью получения информации мошенническим путем. Незаконная деятельность была выявлена путем анализа информации и данных, разработанного специализированными полицейскими подразделениями по борьбе с киберпреступностью. В связи с возросшей активностью в режиме онлайн в период карантина эти подразделения осуществляли усиленный мониторинг или так называемое "киберпатрулирование". Преступление было связано с местными испаноязычными пользователями, судя по языку сообщений электронной почты. Расследование по этому делу продолжается. Пример 4 Источник: Подразделение финансовой разведки, Испания (2020 г.)
Мошенничество в сфере мобильной телефонной связи	Израиль	Региональное киберподразделение Национальной полиции Израиля недавно провело тайное расследование в связи с подозрениями в мошенничестве в размере сотен тысяч израильских шекелей, которое было совершено группой из 16 человек, систематически занимавшихся организованной преступной деятельностью под руководством супружеской пары в возрасте около 40 лет. Группа обманным путем похитила у десятков жертв около 700 000 израильских шекелей (примерно 210 000 долл. США), захватив учетные записи их мобильных телефонов путем мошенничества со сменой SIM-карты (SIM-Swap scam), взломав их персональные банковские счета при помощи разовых SMS-паролей и выведя тысячи израильских шекелей со счетов жертв. Расследование началось в марте 2020 года, когда одно из региональных киберподразделений Национальной полиции Израиля проанализировало несколько жалоб, поданных гражданами, большинство из которых являлись состоятельными пожилыми людьми. Расследование выявило распространенный по всей стране метод мошенничества, при котором сотни банковских переводов осуществлялись без согласия или ведома владельцев счетов. Негласные следственные действия показали, что мошенничество было преднамеренно осуществлено во время карантина в связи с пандемией COVID-19, поскольку жертвы (особенно пожилые) не имели возможности покинуть свои дома или посетить банк и, следовательно, не могли

		обнаружить или отследить мошеннические переводы, сделанные с их банковских счетов. В октябре 2020 года израильская национальная полиция арестовала 16 подозреваемых, провела обыски в их домах и изъяла компьютеры и цифровые запоминающие устройства. В результате сотрудничества между израильской национальной полицией и израильским ПФР (IMPA) были обнаружены исходящие международные электронные переводы. В иностранное ПФР был направлен информационный запрос с целью отслеживания и конфискации денежных средств. Обвинительное заключение в отношении двух основных подозреваемых было предъявлено 9 ноября 2020 года.

		Источник: Управление Израиля по борьбе с отмыванием денег и финансированием терроризма, IMPA (2020 г.)
Мошенническая благотворительность	Китай	W, занимавшийся сбором средств для борьбы с COVID-19, опубликовал на онлайн-платформе информацию с QR-кодом, призывая к публичным пожертвованиям. Во время пандемии более 100 человек со всего Китая вносили, отсканировав QR-код, различные суммы, в основном, кратные 10 юаням (1,50 долл. США) или 100 юаням (15 долл. США). Общая сумма пожертвований превысила 100 000 юаней (14 960 долл. США). Вскоре после перечисления денег они были переведены на личный банковский счет W. Соответствующая информация о пожертвованиях не была зарегистрирована, имелись только очевидные признаки мошеннических действий. Дело было передано в полицию для расследования. Пример 7 Источник: Бюро по борьбе с отмыванием денег, Китайская Народная Республика (2020 г.)
Мошенничество в инвестиционной сфере	Соединенные Штаты Америки	В июне 2020 года гражданин Калифорнии был обвинен в мошенничестве, в связи с тем, что он призывал людей по всей стране инвестировать в компании, которые, как он утверждал, будут производить таблетки, предотвращающие коронавирусные инфекции, и инъекционные лекарства для тех, кто уже страдает от COVID-19. Обвиняемый ложно утверждал, что разработал лекарство от вируса COVID-19 и профилактическое средство, предотвращающее заражение вирусом COVID-19, посредством текстовых сообщений, видеозаписей и заявлений, отправленных потенциальным инвесторам и размещенных в Интернете. В обвинительном заключении говорится, что он обманным путем вымогал инвестиции в две компании путем ложных обещаний, включая чудесные результаты использования профилактического средства и лекарства, а также безрисковую и стопроцентную гарантию "огромной прибыли" от инвестиций. Более того, ответчик ложно заявил, что неназванная сторона в Дубае предложила приобрести две компании за 10 миллиардов долл. США, утверждая, что это предложение обеспечит вложения инвесторов в две компании, и что он получил

		финансирование от семи инвесторов, каждый из которых уже инвестировал от 750 000 до 1 000 000 долл. США. Обвиняемый был арестован ФБР в марте 2020 года после того, как он передал таблетки - якобы профилактическое средство, предотвращающее коронавирусную инфекцию, - агенту под прикрытием, выдававшему себя за инвестора. Ему было предъявлено 11 обвинений в мошенничестве с использованием электронных средств сообщения в связи с предложениями, которые он, как утверждается, сделал потенциальным инвесторам в Неваде, Нью-Йорке, Техасе и Колорадо. Два из этих обвинений были вынесены благодаря работе агента под прикрытием. Примечание: В Соединенных Штатах обвинительный акт содержит только обвинение в совершении преступления. При этом каждый обвиняемый считается невиновным до тех пор, пока его вина не будет полностью и неоспоримо доказана в суде. Пример 6 Источник: Министерство юстиции, Соединенные Штаты Америки (2020 г.)
Незаконное использование мер экономической поддержки	Соединенные Штаты Америки	В июле 2020 года руководитель предприятия информационных технологий в штате Вашингтон был обвинен по одному пункту обвинения в мошенничестве с использованием электронных средств сообщения и по одному пункту обвинения в отмывании денег в связи с предполагаемой подачей как минимум восьми заявок на получение кредита по линии Программы поддержки бизнеса в США в связи с пандемией COVID-19 (Paycheck Protection Program, PPP) от имени шести различных компаний в кредитно-финансовые учреждения, застрахованные на федеральном уровне. Заявки были поданы на получение кредитов на сумму более 5,5 млн. долл. США. В обоснование мошеннических кредитных заявок обвиняемый, как утверждается, сделал многочисленные ложные и вводящие в заблуждение заявления о соответствующих деловых операциях компаний и расходах на заработную плату. В обвинительном акте также утверждается, что он представил фальсифицированные документы, в том числе поддельные федеральные налоговые документы и измененные учредительные документы. В частности, утверждается, что он сообщил о том, что в одной из его компаний работают десятки сотрудников и что он выплатил миллионы долларов в виде заработной платы и налогов на заработную плату. Компания, купленная в интернете в мае 2020 года, на момент покупки фактически не имела сотрудников и не вела деловой активности. Как утверждается, обвиняемый также перечислил не менее 231 000 долл. США, полученных мошенническим путем, на свой брокерский счет в личных интересах. Это дело расследовалось Офисом Генерального инспектора Федерального агентства по финансированию жилищного строительства, Налоговой службой США – Следственным управлением, Генеральным инспектором Казначейства США по налоговому администрированию и Офисом Генерального

		инспектора Федеральной корпорации по страхованию вкладов. Примечание: В Соединенных Штатах обвинительный акт содержит только обвинение в совершении уголовного преступления. При этом каждый обвиняемый считается невиновным до тех пор, пока его вина не будет полностью и неоспоримо доказана в суде. Пример 8 Источник: Министерство юстиции, Соединенные Штаты Америки (2020 г.)

Незаконное использование мер экономической поддержки	Соединенные Штаты Америки	В рамках расследования, проведенного Целевой группой по борьбе с организованной преступностью и незаконным оборотом наркотиков (OCDETF) в отношении влиятельных лиц, занимающихся незаконным оборотом героина и метамфетамина в Южной Каролине, агенты узнали, что некоторые из них также занимаются мошенничеством с использованием электронных средств сообщения и отмыванием денег. В сентябре 2020 года семи лицам было предъявлено обвинение в отмывании средств, полученных мошенническим путем, на сумму свыше 750 000 долл. США, включая более 390 000 долл. США, полученных в рамках Программы поддержки бизнеса в США в связи с пандемией COVID-19 (Paycheck Protection Program, PPP). Согласно судебным документам, один из обвиняемых подал мошенническую заявку на получение кредита PPP, наряду с поддельными подтверждающими документами, которые содержали многочисленные ложные и вводящие в заблуждение заявления о количестве сотрудников компании и расходах на заработную плату. Как утверждается, он получил кредит на сумму более 395 000 долл. США, который различными способами распространял среди других участников заговора. Вскоре после этого он трижды снимал денежные средства с банковского счета на общую сумму почти 350 000 долл. США. Из записей телефонных переговоров стало известно, что еще один человек сообщил третьему о том, что в рамках этой схемы были поданы мошеннические заявки в банк и что им необходимо подать как можно больше заявок в банк до 30 июня 2020 года. Примечание: по этим делам лишь предъявлены обвинения в совершении преступления, и обвиняемые считаются невиновными до тех пор, пока их вина не будет в полной мере и неоспоримо доказана в суде. Источник: Министерство юстиции, Соединенные Штаты Америки (2020 г.).
Незаконное использование мер экономической поддержки	Соединенные Штаты Америки	В августе 2020 года Тарик Джаафар признал себя виновным в обмане Программы поддержки бизнеса в США в связи с пандемией COVID-19 (Paycheck Protection Program, PPP). Согласно судебным документам, Джаафар сговорился со своей женой о создании четырех подставных компаний, которые не вели законного бизнеса и существовали исключительно как средство осуществления схемы обмана. В период с 13 апреля 2020 года по 6 мая 2020 года пара подала заявку на 18 отдельных займов в рамках PPP на имя четырех подставных

		компаний на сумму около 6,6 млн. долл. США, ложно утверждая, среди прочего, что в этих компаниях были сотрудники, и что они нуждались в получении ссуды для выплаты им зарплаты. Эта пара обманным путем заставила банки выделить примерно 1,4 млн. долл. США в виде ссуды, которые они намеревались использовать для своей личной выгоды. 20 июня 2020 года пара была арестована в нью-йоркском аэропорту при попытке бежать в Польшу. Большая часть средств была возвращена банками и правоохранительными органами. Тарик Джаафар признал себя виновным в заговоре с целью обмана Соединенных Штатов, и ему грозит максимальное наказание в виде пяти лет тюремного заключения. Расследование проводилось подразделением ФБР Вашингтонского отделения по борьбе с мошенничеством в отношении кредитно-финансовых учреждений и Администрацией Генерального инспектора по вопросам управления малым бизнесом. Источник: Министерство юстиции, Соединенные Штаты Америки (2020 год).)
Незаконное использование мер экономической поддержки	Швейцария	В середине июня 2020 года одно из кредитно-финансовых учреждений предоставила компании, работающей в строительном секторе, кредит в размере около 90 000 швейцарских франков (98 500 евро) в связи с пандемией COVID-19. Через несколько дней кредитно-финансовое учреждение было проинформировано о том, что это же предприятие обратилось за дополнительным кредитом в другое кредитно-финансовое учреждение. В то же время большая часть первоначального займа была снята наличными или потрачена на ежедневные потребительские расходы. В связи с этим кредитно-финансовое учреждение направило в швейцарское ПФР отчет о подозрительной деятельности. Дело было передано компетентным швейцарским правоохранительным органам, ведущими в настоящее время уголовное разбирательство. Пример 9 Источник: Федеральный департамент финансов. Швейцария (2020 г.)
Незаконное использование мер экономической поддержки	Италия	В ходе расследований, завершившихся в июле 2020 года, было установлено, что члены преступной группы, связанной с организованной преступной группировкой мафиозного типа (Ндрангетой), занимались предпринимательской деятельностью, предположительно в сфере торговли металлами в Италии. Однако на самом деле этот бизнес был направлен на совершение ряда предикатных преступлений, связанных с пандемией COVID-19. В их число входила подготовка ложных или вводящих в заблуждение налоговых деклараций, которые использовались для мошеннического получения возмещения НДС. Затем средства отмывались через банки и провайдеров услуг перевода денег или ценностей. Часть денег была отправлена в компанию, находящуюся в зарубежной стране в Европе, другая часть - в другую зарубежную страну, а преступники сняли деньги наличными с корреспондентского счета в Италии. Мошенничество с НДС создало ложный оборот для компаний,

		участвующих в этой схеме, за счет чего возникли условия для получения государственных безвозмездных субсидий в связи с пандемией COVID-19. Преступная схема также использовалась для того, чтобы попытаться запросить дополнительную экономическую поддержку.

		Дальнейшие расследования показали, что основной подозреваемый использовал ложный оборот, возникший в результате мошенничества с НДС, для ложного обоснования убытков, вызванных пандемией, с тем, чтобы получить безвозмездные субсидии, предоставляющиеся в качестве контрмер COVID-19 для трех компаний, входящих в эту преступную схему. Расследование также выявило попытку преступника воспользоваться государственными займами в контексте мер, направленных на поддержку экономической системы в условиях чрезвычайной ситуации, связанной с пандемией COVID-19. Правоохранительные органы арестовали активы и финансовые ресурсы на сумму около 7,5 млн. евро и произвели 10 арестов. Пример 10 Источник: Guardia di Finanza (Финансовая гвардия Италии), июль (2020 г.)
Незаконное использование мер экономической поддержки	Испания	В апреле 2020 года Национальная полиция Испании ликвидировала преступную организацию, которая пыталась получить государственные субсидии для компаний и работников, пострадавших от экономического кризиса в связи с пандемией COVID-19, путем изготовления и использования поддельных документов. В предыдущие годы членами преступной организации было зарегистрировано около 50 компаний, не имевших работников и не осуществлявших какой-либо деятельности. Организация изготавливала и использовала поддельные документы с целью получения налоговых льгот, а также субсидий от системы социального обеспечения и в рамках других мер государственного стимулирования на имя фиктивных сотрудников этих компаний. Некоторые члены преступной группы до принятия мер экономического стимулирования в связи с пандемией COVID-19 занимались фабрикацией и продажей фальшивых контрактов на работу для иностранных граждан с целью получения для них субсидий. В ходе операции члены организации были арестованы, изъято большое количество документов, а также около 15 000 евро наличными, и администрация отказала им в предоставлении каких-либо субсидий в рамках экономического стимулирования. Источник: Подразделение финансовой разведки, Испания (2020 г.)
Незаконное использование мер экономической поддержки	Дания	В октябре 2020 года Высокий суд Дании вынес первое решение по делу о незаконном использовании мер экономического стимулирования в условиях пандемии COVID-19. По этому делу 29-летний мужчина был приговорен к 2 годам и 3 месяцам тюремного заключения, а также к удовлетворению иска на сумму приблизительно 1,3 млн.

		датских крон (170 000 евро) в связи с попыткой получить необоснованную компенсацию за фиктивные рабочие места в его компании. Общая сумма компенсации, на которую было подано заявление, составила 427 500 датских крон (57 500 евро). Агентство Дании по делам предпринимательства провело тщательное расследование заявления. В результате денежные средства так и не были предоставлены, а о компании было сообщено в датскую полицию. Источник: Агентство Дании по делам предпринимательства (2020)
Мошенничество в сфере страхования по безработице	Соединенные Штаты Америки	В октябре 2020 года во Флориде были арестованы четыре человека в ходе широкомасштабного совместного федерального расследования и расследования на уровне штата в связи с большим количеством мошеннических заявлений о страховании по безработице, поданных в Департамент труда и профессиональной подготовки Род-Айленда (RIDLT) и в другие учреждения для получения пособий, частично финансируемых в соответствии с Законом об оказании помощи, содействия и обеспечения экономической безопасности в условиях пандемии коронавируса (CARES). На момент ареста в результате обысков, санкционированных судом, было изъято более 1,2 млн. долл. США наличными, несколько сотен дебетовых карт на имя граждан, чьи личные данные были предположительно украдены, большая коллекция высококлассных ювелирных изделий и шесть единиц огнестрельного оружия. Согласно судебным документам, четыре арестованных лица и пятый обвиняемый предположительно были вовлечены в сложные схемы использования украденной личной идентификационной информации, принадлежащей жителям Род-Айленда и другим лицам. Они использовали эту информацию для подачи заявления на получение пособий по безработице в онлайновом режиме и для того, чтобы эти пособия вносились непосредственно на один из многочисленных банковских счетов, открытых специально для получения мошенническим путем выплат по линии страхования на случай безработицы, а также для получения мошенническим путем возмещений по федеральным налогам и налогам штатов. Утверждается, что, по крайней мере, трое из них подали мошеннические заявления в государственные системы трудоустройства для получения пособий по безработице, используя украденные личные идентификационные данные. Все эти пять лиц, как утверждается, сняли обманным путем полученные средства вскоре после того, как они были внесены на депозит и размещены на банковских счетах на имя других лиц. Это бессрочное расследование проводится Прокуратурой Соединенных Штатов, Департаментом Генерального прокурора Род-Айленда, Федеральным бюро расследований, полицией штата Род-Айленд, Отделом уголовных расследований Федеральной налоговой службы США, а также Департаментом труда - Канцелярией Генерального инспектора. Источник: Министерство юстиции, Соединенные Штаты (2020 г.)
Незаконное	Россия	Аудит показал, что частное предприятие по контракту с

присвоение государственных средств		государственным органом закупило медицинское оборудование по значительно завышенным ценам на общую сумму более 3,1 млрд. рублей (35 млн. евро).

		На основе материалов ПФР России возбуждено уголовное дело (по факту мошенничества в организованной группе) в отношении должностных лиц концерна за хищение бюджетных средств в размере 27 млн. рублей (300 тыс. евро). Эти средства, составляющие часть от общей суммы договора, были обналичены. Информация о выявленных подозрительных финансовых операциях и схемах финансовых связей участников группы была направлена в правоохранительные органы, сотрудничество с иностранным ПФР продолжается. Источник: Росфинмониторинг (2020 г.)
Незаконное присвоение помощи	Тунис	В октябре 2020 года подразделение финансовой разведки Туниса (CTAF) получило от одного из кредитно-финансовых учреждений сообщение о подозрительных операциях, в котором указывалось, что гражданин Туниса (X) обналичил банковский чек на 2 млн. тунисских динаров (примерно 724 000 долл. США) и положил деньги на счет своей фирмы, компании С. X утверждал, что якобы этот чек был выписан ему в консульстве иностранного государства с целью обеспечения 2 000 иностранных граждан, находившихся в Тунисе в период карантина, жильем, медикаментами, припасами и средствами для проведения теста на наличие COVID-19. В тот же день, когда X обналичил чек, он перевел всю сумму на различные счета физических лиц, клиник и фирмы своего брата - компании А. Вскоре после этого CTAF получило еще одно сообщение о подозрительных операциях от другого кредитно-финансового учреждения, причиной которого стал тот факт, что на счет компании А в тот же день поступило пять идентичных электронных переводов от компании С на общую сумму 400 000 тунисских динаров (145 000 долл. США). Дальнейший анализ показал, что в течение короткого промежутка времени (менее 6 месяцев с момента открытия счета) компания С получила шесть электронных переводов только от упомянутого консульства на общую сумму почти 7 млн. тунисских динаров (2,5 млн. долл. США). Вскоре после этого 500 000 тунисских динаров (182 000 долл. США) были сняты наличными, 2,5 млн. тунисских динаров (910 000 долл. США) были переведены на счет Компании В (принадлежавшей X), а 700 000 тунисских динаров (255 000 долл. США) были переведены на личный счет X. X потратил 15% от суммы, полученной от иностранного консульства, на гостиницы, клиники и аптеки. В договоре, заключенном между консульством и компанией С, не были определены требуемые от компании услуги, цены, а также связанные с ними налоги. Кроме того, компания С не имеет других банковских счетов и не ведет хозяйственной деятельности. Также было установлено, что переводы, направляемые в компанию А, были основаны на фальсифицированных счетах на оплату, содержащих аномально высокие цены по сравнению с теми, которые

		обычно взимаются. В результате, сотрудники CTAF пришли к выводу, что X использовал подставную компанию (компания C), семейные компании и фальсифицированные счета на оплату, чтобы направить государственную помощь, предоставленную иностранным государством своим гражданам, оказавшимся в затруднительном положении в Тунисе из-за пандемии COVID-19. В качестве превентивной меры CTAF приказало заморозить счета компаний A, B и C и банковский счет X. Кроме того, CTAF по своей инициативе направило информацию в иностранное подразделение финансовой разведки и препроводило отчет прокурору. Расследование продолжается. Пример 11 Источник: Подразделение финансовой разведки, Тунис (2020 г.)
Коррупция - мошенничество с государственными контрактами на поставки	Италия	В апреле 2020 года крупная итальянская компания, ведущая бизнес в сфере швейной промышленности, получила государственный контракт на поставку медицинских халатов и других средств индивидуальной защиты на сумму около 1,5 млн. евро. Этой компанией владел и управлял (по доверенности) близкий родственник президента компании-заказчика, являющегося публичным должностным лицом (ПДЛ). Компания получила контракт на закупку по прямому поручению, без проведения тендерной процедуры. Месяц спустя финансовое учреждение проинформировало итальянское ПФР об исходящем банковском переводе в размере 750 000 евро с зарубежного банковского счета, управляемого ПДЛ по доверенности, на счет компании, получившей контракт. Такие средства, в свою очередь, были получены в результате предыдущих переводов с участием иностранных непрозрачных юридических лиц, в частности, трастов и фондов, якобы связанных с тем же ПДЛ и базирующихся в государствах с льготным режимом налогообложения. Тем временем, денежный перевод был преобразован в пожертвование, очевидно, после получения советов в ходе расследования дела, и компанией-заказчиком, были выданы кредитовые авизо с тем, чтобы отозвать оригинал счета на оплату, который был выписан (как было заявлено сторонами) по ошибке. Первоначально прокуратура открыла информационное досье, не имея ни подозреваемых, ни версий о совершении преступления. Затем тот же самый прокурор возбудил уголовное дело в связи с мошенничеством на торгах и мошенничеством в сфере государственных поставок. В настоящее время судопроизводство продолжается. Источник: Подразделение финансовой разведки, Италия (2020 г.)

Коррупция - мошенничество с государственными контрактами на поставки	Россия	В ходе обязательной проверки были выявлены подозрительные финансовые операции с участием лиц, привлеченных к аудиту. Дело связано с возможным завышением цен на медицинские маски. Подозревается, что компания A принимала и выставляла счета на оплату с НДС,

		включенным в стоимость продукции, которая не облагалась НДС. Три покупателя, участвовавшие в сомнительных сделках, представляли как частные, так и государственные предприятия и заплатили за маски по завышенной цене 115 312 714 рублей (1 270 000 евро). Это считается неоправданным завышением цен на товары, поставляемые также организациям с государственным участием. Позднее был осуществлен перевод части средств на счета двух компаний с индикаторами фиктивности. Подозрения вокруг этих компаний возникли в ходе проведения сотрудниками Росфинмониторинга обязательной комплексной проверки и контроля операций с денежными средствами и иным имуществом. В ходе проведенных мероприятий были выявлены индикаторы мошеннических операций, в связи с чем результаты проверки были направлены в правоохранительные органы и ожидаются дальнейшие действия. Источник: Росфинмониторинг (2020 г.)
Незаконное использование условий удаленной работы	Эфиопия	Сотрудник банка незаконно снял со счета неактивного клиента 3 миллиона эфиопских быров (68 300 евро) и одолжил их своему другу без залога. Когда внутренние аудиторы банка обнаружили незаконное снятие денег с неактивного счета, они сообщили об этом случае в Центр финансовой разведки Эфиопии как о подозрительной операции. Затем Центр провел анализ и отправил его результаты в правоохранительные органы для дальнейшего уголовного расследования. Как сотрудник банка, так и лицо, получившее деньги, находятся под следствием. Они обвиняются в коррупции и других связанных с ней финансовых преступлениях и временно освобождены из-под стражи под залог. Следствие по делу продолжается. Это преступление было совершено в период чрезвычайного положения, объявленного в Эфиопии в целях сдерживания пандемии COVID-19. Вследствие этого лишь 50% сотрудников работали в банке, а остальные - на дому. Это позволило сотруднику получить доступ к системе и совершить преступление. Кроме того, многие предприятия постоянно были бездействующими во время чрезвычайного положения. Оба сценария создавали уязвимости. Кроме того, системы контроля в финансовых учреждениях были ослаблены в связи с уменьшением количества сотрудников, физически присутствующих в банках, для осуществления мер по установлению личности и комплексной проверке клиентов и т.п. Примечание: по этим делам пока лишь предъявлены обвинения в совершении преступления, и обвиняемые считаются невиновными до тех пор, пока их вина не будет доказана вне всякого разумного сомнения в суде. Пример 12 Источник: Центр финансовой разведки Эфиопии (2020 г.)
Виртуальные активы	Гонконг, Китай	В период с конца февраля по начало марта 2020 года владелица компании, занимающейся торговлей товарами медицинского назначения в Гонконге (Китай), увидела в Интернете рекламу, размещенную несколькими предполагаемыми продавцами хирургических масок и

		медицинского оборудования, в том числе на крупной социальной медиа-платформе. При попытке приобрести это оборудование она была обманута, перечислив 450 000 гонконгских долларов (58 000 долл. США) на различные банковские счета в Гонконге, Китае и восточноевропейской стране, а также конвертировав 3,96 млн. гонконгских долларов (510 000 долл. США) в эквивалентную сумму в Bitcoin. Для этого потерпевшая сняла наличные деньги со своего личного банковского счета и положила их в специально определенный банкомат Bitcoin, где средства были переведены в специально отведенные для этого кошельки Bitcoin. В общей сложности были задействованы три банка, расположенных в двух юрисдикциях (Гонконг, Китай и восточноевропейская юрисдикция). Пять переводов на сумму от 47 250 до 235 830 долл. США были переведены на счета, принадлежащие преступнику. Все мошенники перестали отвечать на запросы жертвы после получения платежа. Расследование продолжается. Пример 13 Источник: Казначейское Бюро Гонконга, Гонконг, Китай (2020 г.)