Финансовая грамотность

Экономическое мошенничество: что делать при обмане заказчиками, сотрудниками

Автор: Николай Васильев. Бизнес-аналитик IBA Group. Опубликовано: 2021-06-09. Последняя редакция: 2021-06-10. Полная или частичная публикация материала на других ресурсах допускается только с указанием в качестве автора/источника ник этого сотрудника IBA Group.

За последние два года 67% компаний из разных стран пострадали от экономических преступлений. Бизнес теряет деньги и репутацию из-за экономического мошенничества. По данным PwC, почти половина всех опрошенных компаний по всему миру столкнулись с мошенничеством в среднем шесть раз за последние два года. Каждый пятый респондент наибольший ущерб получил от поставщиков/продавцов.

Мошенниками могут быть как сторонние компании, так и собственные сотрудники. Многие сотрудники работают на удалении, поэтому осваиваются внутренний контроль и повышается риск мошенничества. Сотрудники мошенничество появляется больше возможностей нанести ущерб. Почти четверть компаний столкнулись со сговором между своими сотрудниками и поставщиками.

Я, как эксперт по визуальным расследованиям IBA Group (Минск) помогу разобраться, как предупредить экономическое мошенничество в компаниях.

Типовые схемы мошенничества заказчиков, поставщиков и сотрудников

Обманывать могут все: организаторы тендеров, их участники, а также сотрудники компаний. Эксперты по экономической безопасности описывают три основные схемы мошенничества со стороны участников тендеров.

1. **Предложение-прикрытие.** Недобросовестные участники заранее договариваются с другим участником тендера, чтобы создать видимость конкуренции. А уже после победы передают выполнение работ сторонниму бизнесу.
2. **Карусель предложений.** Исполнители и заказчики заранее договариваются между собой, и компании побеждают на тендерах по уже определенной схеме.
3. **Исчезновение после предоплаты.** Недобросовестные участники тендера сильно занижают цену, что заставляет другие компании выиграть заявку. Нечестные исполнители выигрывают тендер, получают предоплату и перестают выходить на связь. Эта схема работает только в случае, когда в условиях тендера допускается предоплата.

При типовые схемы мошенничества со стороны организаторов тендера, которые выделяют эксперты:

1. **Фиктивные сроки.** Организатор устанавливает сроки, за которые невозможно выполнить той или иной услугой в тендере объем работ. Это значит, что нужные работы уже выполнены или почти завершены, а тендер – просто формальность.
2. **Дробный заказ.** Нужный объем работ или товар организатор описывает очень подробно. Такой тендер рассчитан на какую-то конкретную компанию, которую уже выбрали, но чтобы не возникало вопросов, тендер провести нужно. Часто такая закупка проходит у аффилированных лиц.
3. **Укрупнение заказа.** Крупный заказ не разбивается по лотам и формируется так, чтобы выполнить все работы было невозможно честному участнику тендера.

Схем корпоративного мошенничества много. Это приписки, повторная закупка, неучтенное производство, манипуляции с ценами, подмодные работники и другое. **В сфере закупок мошенничество разделяет на три вида:** корруппция, хищение активов и использование служебного положения.

1. **Коррупция.** Сотрудник могут получать взятки за выбор определенного поставщика, увеличения объемов закупки или предоставления более выгодных условий работы, например, льготные кредит, предоплата и так далее.
2. **Хищение.** Компании обязаны списывать материально-производственные запасы в производство на основании первичных документов, составленных по определенным нормам. Но некоторые предприятия не всегда следуют этому правилу, поэтому материально ответственные сотрудники могут "списать" с запасом или «сэкономить» для себя продукцию. Другой вариант – хищение денежных средств, когда нечестные сотрудники подделывают ведомости или подписывают отчетные спецыаислисты на документами на выдачу денег.
3. **Использование служебного положения.** У сотрудника есть полномочия составлять конкурсные документы. В тендере он прописывает условия, выполнить которые может только «свои» компания, за что сотрудник получает от этой компании откат. Другой вариант – сотрудник компании за вознаграждение предлагает подрядчикам скидки или условия сотрудничества, которые его компании невыгодны.

Это далеко не все схемы обмана. С каждым годом мошенники придумывают новые способы, дорабатывают старые схемы.

Три примера, как работают мошенники

Фиктивный тендер, кража обеспечения заявок или неуместные документы – схемы, о которых сейчас рассказывают компании. Рассмотрим подробно три случая, которыми поделились компании в интернете.

Ненужный сертификат

В СМИ было несколько историй, когда исполнителю среди прочих документов обязательно нужен был сертификат. В одном из случаев это был «Сертификат ГОСТ 315.12», а другие – «ГОСТ РПО 2016-2018 (ИСО.МАО 2016-2018) Рег. № РОСС RU.31512.04ИЕ00». Раньше такой сертификат никто не требовал. Поэтому компании сразу заподозрила, что что-то не так. Поиск сразу же выдал несколько сайтов, где этот сертификат оформляют за один день. По расчету, закупщики запросили информацию, а исполнитель оформил сертификат компании, которые смогут оформить документ быстро.

Список документов с сертификатом РПО

Исчезновение заказчиков

Одна из торговых площадок России предупреждала своих пользователей, что мошенники могут представляться как сотрудниками уполномоченных органов в сфере закупок, заказчики или представители электронных площадок. Они подменяют свои телефонные номера на номера уполномоченных органов в сфере закупок, заказчиков или площадок. Например, мошенники рассылали фейк-сообщения от лица крупной энергетической компании Т Плюс с приглашением на тендер, для участия в котором нужно было заплатить определенную сумму. Естественно, после получения денег на связь никто бы не вышел.

Другой вариант обмана – исчезновение заказчиков после того, как исполнитель выполнил контракт. Предпринимать рассказал РБК что заказчик установил сроки оплаты в 40 рабочих дней. Этот срок еще увеличился за счет нерабочих дней в период карантина. Все это время заказчик отвечал на письма, оставался на связи. Но потом все равно исчез.

Мошенничество персонала

Хищение хуже коррупции, так как компания получает больше ущерба. Сотрудники могут запускать товары «своих» поставщиков по цене, которая в разы превышает цены у других поставщиков. На одной из конференций по внутреннему контролю и аудиту компаний спикер рассказал, что в одном случае фирма закупала товары по цене, которая была выше рыночной на 700%, а в другой – на 1300%. Это были огромные убытки для компаний.

Еще один пример. Закупщик знает, что компании необходимо мыть автомобили. Он открывает автомойку, регистрирует ее на жену и заказывает услуги у «своей» фирмы.

Как не допустить мошенничества

Перед закупками нужно проверять как потенциальных подрядчиков, поставщиков, так и собственных сотрудников. Согласно PwC, самые эффективные факторы, которые помогают обнаружить экономическое мошенничество, – это служба внутреннего аудита, управление рисками мошенничества, мониторинг подозрительной деятельности, служба корпоративной безопасности, анализ данных, Data аналитика) и ротация персонала.

Проверка поставщиков

Прежде всего, компаниям нужно вести список основных поставщиков, с которыми они работает. Возможно, по новой закупке можно сотрудничать с проверенной компанией и избежать заключения договора с неизвестной фирмой.

Если все же нужно заключить договор с новым поставщиком, то необходимо проверить контактную информацию: название, адрес, телефон, УНП. Имея эти данные, компания можно проверить по многим сервисам и базам: реестр недобросовестных плательщиков, картотека арбитражных дел и пр.

Например, в Беларуси поставщиков можно проверить по как минимум по шести базам:

1. Единый государственный регистр юридических лиц и индивидуальных предпринимателей.
2. Реестр задолженности по исполнительным документам.
3. Реестр сведений об организациях и индивидуальных предпринимателях, имеющих задолженность по налогам, сборам (пошлинам), пеням на 1-е число месяца, следующего за отчетным.
4. Список должников по обязательным страховым взносам.
5. Банк данных судебных постановлений, принятых экономическими судами Республики Беларусь.
6. Реестр сведений о делах, рассмотренных экономическими судами в рамках признаного производства.

Проверка сотрудников

Компания стоит обратить внимание на сотрудников, когда специалисты начинают закупать больше сырья, хотя объем производства остается прежним, клиенты – часто жаловаться на качество продукции, на складах обнаруживается некачественный товар. Падает объем продаж или, наоборот, резко увеличивается при снижении цены.

Еще одним грантером служит увеличение представительских расходов или дорогая покупка сотрудника, которая не соответствует его доходам.

Компании сложно понять заранее, кто из сотрудников может пойти на мошенничество. Основные превентивные меры – это рекомендации сотруднику на предыдущим месте работы. При приеме человека на работу нужно запросить рекомендации от бывших коллег, созвониться с ними. Также стоит посмотреть его социальные аккаунты, фотографии, которыми он делится. Уже на этом этапе можно узнать, какая у человека репутация, и отсечь подозрительных кандидатов.

Три способа проверки поставщиков и сотрудников

Есть три способа, как проверять поставщиков и сотрудников: ручной анализ, анализ с помощью готовых ИТ-решений и разработка собственного ПО.

Ручной анализ – это самый распространенный способ проверки, так как не нужно ничего менять в инфраструктуре компании. Но такой анализ информации проходит медленно, не всегда можно вручную проследить связи третьего и более уровней. К тому же, «человеческий фактор» никто не отменял: люди могут просто не заметить важной связи, которая указывает на мошенников.

Пример: с помощью инструмента поиска связей VAS нашли аффилированных учредителей контрагентов у закупки на реконструкцию бомбоубежища. Инструмент показал, что учредитель первого участника торгов является учредителем еще одного юридического лица. Обе организации зарегистрированы на одном и том же адресе.

VLinks
Файл
Операции
Выделение
Выравнивание
Вид
Инструменты
Поиск связей
Все, кого – сбрасывает ресурсы, получает скидки и отдаленный контакт
Один массовый регистратор
Ещё массовый регистратор
Ещё, кого – сбрасывает ресурсы, получает скидки, Одинаковый юридический адрес, Одинаковый телефон, Одинаковый почтовый ящик
Все, кого – сбрасывает ресурсы, получает скидки
Все, кого – сбрасывает ресурсы, получает скидки, Одинаковый телефон, Одинаковый почтовый ящик
Все, кого – сбрасывает ресурсы, получает скидки