Маргарита Акулич

Мошенничество в бизнесе

Маргарита Акулич

Мошенничество в бизнесе

http://www.litres.ru/pages/biblio_book/?art=26713141
ISBN 9785448581120

Аннотация

Мошенничество в бизнесе сегодня является очень распространенным и болезненным для предпринимателей, владельцев бизнеса и компаний явлением.Эту книгу я написала в том числе потому, что сама неоднократно оказывалась жертвой мошенников. Думаю, не последнюю роль в этом сыграло мое незнание вещей, которые стоило знать.Прочтите эту книгу. Она поможет вам сделаться менее уязвимыми в отношении мошенничества.

Содержание

Мошенничество в бизнесе

Маргарита Акулич

ISBN 978-5-4485-8112-0
Создано в интеллектуальной издательской системе Ridero

ПРЕДИСЛОВИЕ

Мошенничество в бизнесе сегодня является очень распространенным и болезненным для предпринимателей, владельцев бизнеса и компаний явлением.

Эту книгу я написала в том числе потому, что сама неоднократно оказывалась жертвой мошенников. Думаю, не последнюю роль в этом сыграло мое незнание вещей, которые стоило знать.

Прочтите эту книгу. Она поможет вам сделаться менее уязвимыми в отношении мошенничества.

I Наличие мошенничества и причины, из-за которых люди становятся мошенниками

1.1 О наличии мошенничества в бизнесе и причине мошенничества, состоящей в давлении со стороны внешних обстоятельств

О наличии мошенничества в бизнесе

О наличии мошенничества в бизнесе обычно вслух не говорят. Однако любому менеджеру известно, что оно есть. Самые распространенные схемы, связанные с мошенничеством, относятся к закупкам материалов, сырья, с услугами, а также с продажами, когда сейл-менеджеры могут заниматься скидками и идти на определенных условиях (получения мзды) на предоставление некоторым из дилеров более выгодных в сравнении с другими условий.

Еще есть различные схемы, содействующие сокрытию доходов, скажем, прибегая к использованию таких компаний как офшорные, «свои», однодневки, или к завышению стои-

мости продукции (в т. ч. таможенной) и т. д.

Если отсутствует открытый рынок, бизнес серьезно зависит от личных взаимоотношений, он является сильно персонализированным и структура сделки оказывается закрытой, проникнуть в нее невозможно. Поэтому деятели, которые работают на рынке в течение, скажем, десяти-пятнадцати лет, имеют много личных контактов и возможностей для совершения того, что называется мошенничеством. Хотя на самом деле тема мошенничества актуальна практически для всех мировых рынков.

Мошенничество совершают люди, и поэтому целесообразно знать, что необходимо для того, чтобы человеком было совершено мошенничество.

Чтобы человек совершил мошенничество, необходим альянс трех составляющих (компонентов-причин): 1) давления обстоятельств; 2) возможности совершения и сокрытия в течение какого-то времени акта мошенничества; 3) способности человека к самооправданию. Без такого альянса совершение мошенничества невозможно.

Причина мошенничества, состоящая в давлении со стороны внешних обстоятельств

На каждого из мошенников довлеют какие-то внешние обстоятельства, чаще всего связанные с фактом финансового неблагополучия. В то же время не только финансовые факторы оказываются довлеющими. Иной раз довлеет необходимость отражения в отчетах улучшенных в сравнении с фактически достигнутыми показателей, или факт нелюбви к выполняемой работе, или даже желание «наказания всей системы».

Мошенники стремятся к обретению выгод – либо для себя лично, либо для своей компании или своего учреждения.

Если говорить о мошенничестве со стороны наемных кадров, в ходе которого они присваивают средства своих нанимателей, то данное мошенничество связано с преследованием цели получения выгоды этими кадрами.

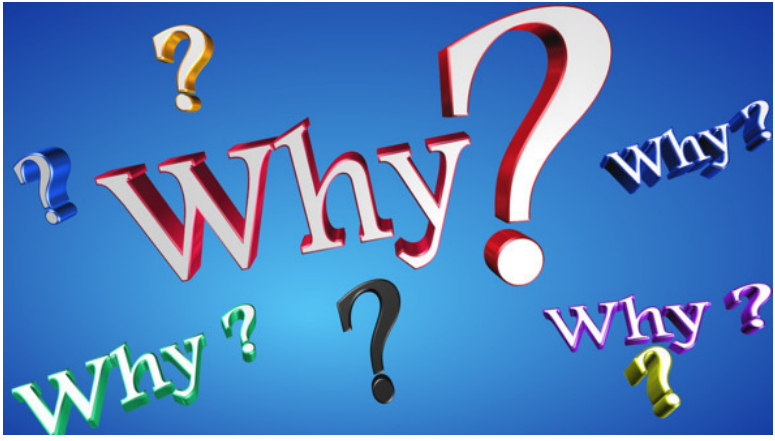
В отношении мошенничества со стороны менеджеров можно сказать, что оно нередко происходит ради интересов компании и ее руководства. Менеджеры могут идти на обман кредиторов или инвесторов.

Давления бывают: 1) финансовыми; 2) связанными с пагубными пристрастиями и разными людскими слабостями и пороками; 3) имеющими отношение к работе; 4) прочими.

Давления финансовые и связанные с человеческими пороками и нехорошими пристрастиями встречаются наиболее часто.

1.2 Наиболее типичные причины появления финансового давления. Давление пагубных пристрастий и связанных с работой обстоятельств

Наиболее типичные причины появления финансового давления



Люди испытывают финансовые давления из-за:
жадности;
наличия больших долгов;

жизни не по средствам;
больших счетов за медобслуживание;
отсутствия денег на счетах;
больших финансовых потрерь;
неожиданных потребностей в деньгах.

Список этот можно продолжить. Каждое из приведенных и других видов финансового давления способно привести и уже неоднократно приводило к мошенничествам.

Бывает, что люди идут на преступления из-за бедности. Но некоторые особы мошенничают даже невзирая на то, что они являются более финансово обеспеченными в сравнении с их коллегами. Например в статье «Психология Обмана и Мошенничества» написано [1]:

> «Когда удалось поймать одного аферист, похитившего у своего работодателя более миллиона трехсот тысяч долларов, оказалось, что он потратил их на рубашки со своей монограммой и золотые заколки для галстука, два дорогих „мерседеса“, на покупку очень дорогого загородного дома и виллы на берегу океана, на меха, кольца и другие дорогие безделушки для жены, на новую машину для своего тестя, на членство в престижном клубе и на чаевые по пятьдесят долларов в барах. Большинство его знакомых никогда бы не сказали, что он испытывал какое-либо финансовое давление».

Если говорить о возникновении финансового давления, приводящего к мошенничеству, то оно может возникнуть

как внезапно, так и после прошествия довольно долгого времени. Причем люди обычно не склонны делиться с коллегами тем, что у них неблагоприятные финансовые обстоятельства.

Чаще всего в компаниях люди искажают финансовую отчетность (ее данные) не просто так, а потому, к примеру, что у них сложилось тяжелое финансовое положение, или появились в кассе недостачи, или имеются задолженности со стороны бизнес-партнеров, или отсутствуют выгодные заказы, или кредиторы выдвинули слишком жесткие условия, или на рынке тяжелое положение и т. д.

Давление пагубных пристрастий и разных пороков а также связанных с работой обстоятельств

Имеет место тесная корреляция давления обстоятельств финансового свойства с приверженностью к азартным играм, с алкоголизмом, наркоманией, сексуальными дорогими удовольствиями. Нередко люди, имеющие пороки и пагубные пристрастия, нарушают закон и занимаются мошенничеством. Бывали даже случаи, когда женщины, являвшиеся

матерями детей-наркоманов, шли на финансовые преступления из-за невыносимости для них наблюдения болезненной ломки своих детей, чтобы найти деньги на наркотики.

Если у кого-то хватает духа для изъятия карманных денег у своих малолетних детей он, скорее всего, не станет долго сомневаться, стоит ли ему красть деньги у своей компании. Многие алкоголики, заядлые любители азартных игр, сексуальных утех и наркоманы являются причинами растрат в компаниях.

Есть особы, которые занимаются мошенничеством из-за желания сведения счетов с начальниками или сотрудниками. Иногда люди уверены, что на работе их недооценивают, что им недостаточно платят за работу, они готовы во имя «восстановления справедливости» мошенничать.

1.3 Разные виды давления обстоятельств. О цене честности

Разные виды давления обстоятельств

В некоторых не очень частых случаях причиной мошенничества становятся другие виды давлений такие, к примеру, как требование жены или мужа обеспечить более роскошный образ жизни или желание «досадить всей системе».

Многим людям в их жизни приходится сталкиваться с разными внешними давлениями. Люди могут испытывать финансовые затруднения, могут рисковать своими сбережениями, рискованно их размещая, могут быть в плену пагубных пристрастий и/или пороков или ощущать, что им недоплачивают и т. д. Нередко людям трудно отличить то, что им необходимо о того, что им хочется.

Люди нередко хотят быть богатыми и успешными финансово. Однако финансовая успешность имеет для разных людей различное значение. Некоторые вполне обеспеченные люди считают себя бедными, а иные бедные думают, что они вполне финансово успешные. Каждому свое…

Финансовую успешность некоторые из людей оценивают выше честности и порядочности.

О цене честности

Как у многих вещей в мире, у честности имеется своя цена. Если у человека большая честность и малые возможности, он должен подвергаться чрезмерно большому давлению, чтобы поступиться своей честностью. Многим людям приходят в голову мысли о том, какие должны сложиться обстоятельства, чтобы они пошли на мошенничество.

Предположим, что у человека дети откровенно не доедают, а он трудится в месте, где много не учитываемой налич-

ности. Скорее всего, человек этот пойдет на мошенничество, станет красть наличность. Но вполне вероятно, что он будет при этом успокаивать себя мыслями о возможности ее возвращения хозяину спустя какое-то время и также о том, что его мошенничество можно оправдать любовью к детям и желанием им помочь, желанием сделать так, чтоб они не голодали.

Честнейшим Абрахамом Линкольном однажды был вышвырнут из кабинета человек, предложивший ему большую взятку. При этом свою ярость он объяснил:

> «У каждого есть своя цена, а он подобрался слишком близко к моей!»

Таким образом, давление внешних факторов может провоцировать человека на совершение мошенничества.

1.4 Причина мошенничества, состоящая в возможности его совершения и причина, состоящая в оправдании мошенника перед собой

Причина мошенничества, состоящая в возможности его совершения

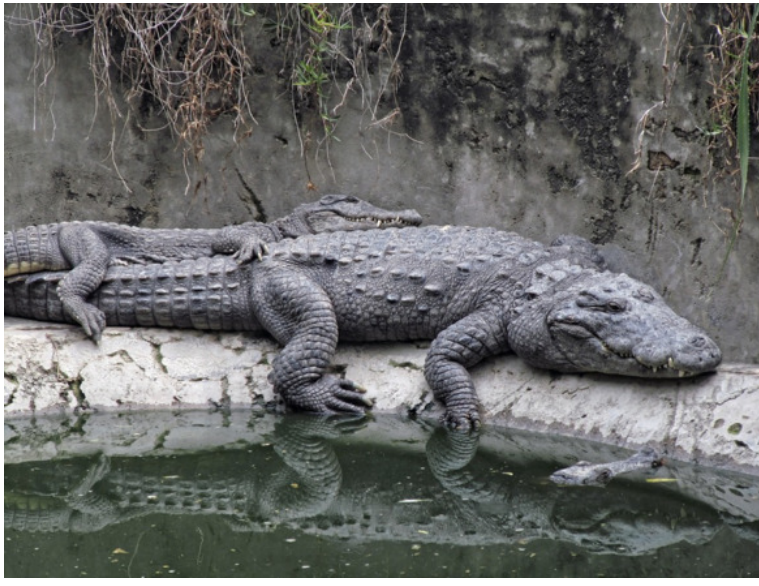
Второй причиной мошенничества является возможность его совершения. Примеров, когда имеется причина, при которой можно совершить мошенничество, немало. Это и невнимательность владельца бизнеса к финансовым аспектам бизнеса, и с тем, что работники компании не компетентны в вопросах начисления зарплаты, и с особым умением мошенника скрывать свои недобросовестные деяния и др.

Рассмотрим пример из книги У. Альбрехта, Дж. Венца и Т. Уильямса «Мошенничество: луч света на темные сторо-

ны бизнеса» [2]:

> «Деннис избрал способ „кайтинга“, связанный с выпиской необеспеченных чеков на один банк для покрытия таких же чеков, выписанных на другой банк. Для этого ему не требовалось иметь доступа к кассовой наличности, применять силу или даже физически приближаться к своим жертвам. Он выписывал фальшивые чеки, сидя в своей комнате, и просто отправлял их по почте в эти два банка. Орудием преступления для него были чеки двух различных финансовых учреждений и авторучка. Не имеет значения, раскаялся ли Деннис в своих действиях или нет – главное здесь, что Деннис считал, что он может скрыть свое мошенничество, что у него есть *возможность* его совершить».

Причина мошенничества, состоящая в оправдании мошенника перед собой

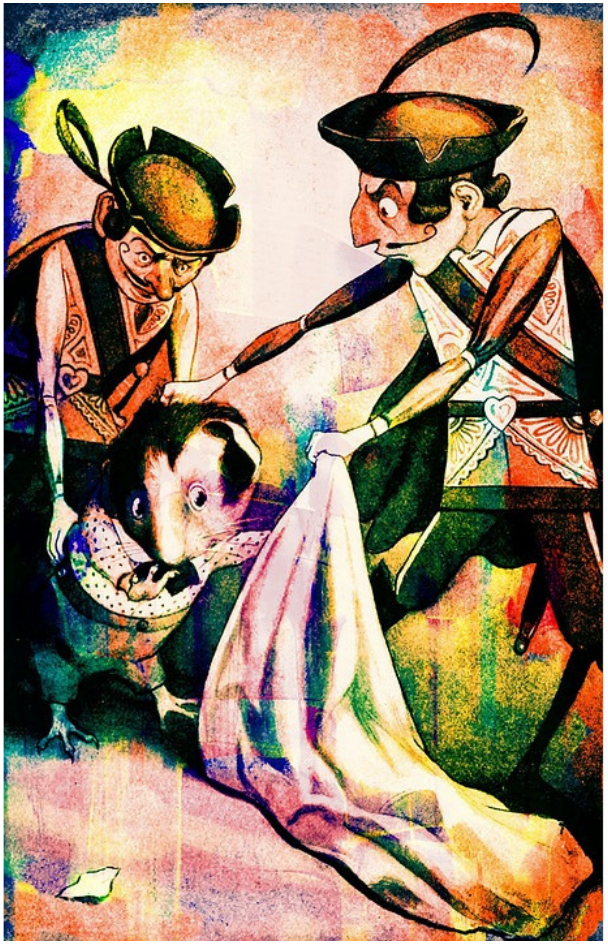


Мошенники таковы, что чем больше возможностей им предоставляется для мошенничества и большее давление обстоятельств со стороны, тем меньше им требуется оправданий себя для совершения злоупотреблений или преступлений. И если человек является по натуре не честным, тем ему меньше требуется возможностей и/или внешних давлений для совершения мошенничества.

К сожалению, во всех практически странах наблюдается понижение уровня честности людей, что провоцирует рост мошенничества. Поэтому владельцам бизнеса нельзя рас-

слабляться, если они не хотят стать жертвами мошенников.

II О распознавании мошенников, их приемах и проверке



2.1 Что целесообразно считать мошенничеством? Доверие как важнейшая составляющая мошенничества

Что целесообразно считать мошенничеством?

В отношении мошеннических схем можно вполне уверенно констатировать, что их на рынке всегда было более чем много. Но во время кризисов эти схемы имеют манеру активно всплывать. Вспомним, кстати, одну из самых грандиозных финансовых пирамид мира «финансового гуру» Медоффа. В результате мошенничества с клиентов было Меддофом собрано пятьдесят миллиардов долларов. После этого он объявил себя банкротом.

Во времена кризисов происходит увеличение численности людей, которыми используются с целью своего личного корыстного обогащения самые разнообразные схемы мошенничества.

Не всегда легко защититься от деяний мошенников, но все-таки можно, если знать кто такие мошенники и какими способами от них можно защититься.

Прежде всего, надо никогда не забывать о существовании мошенников и быть всегда начеку. Кроме того, стоит уяснить, что следует понимать под мошенничеством. Мошен-

ничество – это, по сути, преступление. Мошенники занимаются похищением чужого, не принадлежащего им имущества, обманом, и они злоупотребляют доверием. Конечно, это весьма упрощенное понимание мошенников, но зато довольно простое и доходчивое.

Мошенники-преступники часто вводят своих жертв в заблуждение, которое помогает им, поскольку введенные в заблуждение жертвы действуют «добровольно» – подписывают контракты, перечисляют деньги, передают имущество и рт. д. Поскольку мошенничество в ряде случаев ориентировано на «добровольность: жертв, оно для последних оказывается зачастую весьма болезненным и опасным. Ведь очень часто люди, которых обманули мошенники, стыдятся даже обращаться в правоохранительные органы. Они ощущают стыд за проявление простодушия либо думают, что уже ничего нельзя изменить. И нельзя что-то доказать. Во многом они правы, потому что мошенники зачастую действуют довольно искусно, доказать их обман не так просто. И не только потому, что они искусные, они нередко имеют сообщников, и в этом их сила.

Иногда человек начинает осознавать, что для него приготовлена ловушка, и тогда он прекращает общаться. Мошенник осознает, что у него не вышло втереться в доверие, и он начинает угрожать, говорить, что человек станет иметь со своим бизнесом проблемы, что его родные пострадают, либо что на него будет наведена порча.

Многое не от преступника зависит, а от жертвы. Оказаться жертвой не трудно, мошенники находят в качестве жертв людей, которые способны попасть под их влияние. Много доверчивых людей, даже среди бизнесменов.

Руководители компаний понимают, что нельзя делать отгрузку товара, пока не поступили от клиента деньги. Но им не выгодно, когда товар залеживается и они боятся, что лишатся покупателя. Поэтому осуществляют отгрузку без оплаты. Многие на эту мошенническую удочку попадались. У одного директора хватит твердости сказать: «Деньги от вас не поступали – значит, мы с вами не работаем». А у другого не хватит этой твердости, он поверит на слово мошеннику, и денег от него не дождется. Все зависит от степени доверчивости. Слишком доверчивыми быть нельзя.

Доверие как важнейшая составляющая мошенничества

Ни одно мошенничество, обман или жульничество не может совершиться без доверия. Никто не может оказаться обманутым или жертвой мошенничества, если у него нет к мошеннику доверия.

Иной раз доверие является следствием потери бдительности, но как бы ни было, без доверия такое преступление как

мошенничество просто невозможно. Всегда об этом нужно помнить.

Иногда в бизнесе доверие людей проистекает из-за честности тех, против кого совершается мошенничество.

Настоящие мошенники таковы, что нередко они оказываются последними, кого подозревают в мошенничестве. Мошенники знают свою «работу», они всегда начеку в отличие от тех, кто им доверяет. И они, как правило, не мошенничают до тех пор, пока не добьются доверия. А уж чего чего, а доверия добиваться они действительно умеют.

Вот что написано о мошенниках в статье «Психология Обмана и Мошенничества» [1]:

> «В одном из исследований мошенничества как явления показано, что наибольшую группу жуликов составляют люди от 36 до 45 лет. Хотя статистические данные и не объясняют, почему превалирует именно эта возрастная группа, одной из причин данного факта может быть то, что это возраст большинства менеджеров среднего звена, которые уже добились определенного уровня доверия к себе».

2.2 Некоторые советы по распознаванию мошенников. Об используемых преступниками приемах

Некоторые советы по распознаванию мошенников

Мошенников как врагов нужно знать «в лицо», чтобы эффективно с ними бороться.

Прежде всего, нужно знать о стремлении мошенников к резкому ограничению информации для своих бизнес-партнеров. Они могут заявлять, что информация пока недоступна или она не в том виде, в котором им было бы удобно с нею делиться, или ее пока не существует (к примеру, товар новый или бизнес) и т. д.

Они могут также говорить, что слишком заняты и предоставят необходимые данные как только освободятся. Каждый раз они обещают, но не выполняют обещанного.

Мошенники зачастую вынуждают своих жертв торопиться, принимать скоропалительные решения. Они могут, скажем, заявлять, что имеющаяся у них дешевая и высококачественная продукция очень скоро раскупится, поэтому надо поторопиться ее вам приобрести, причем с оплатой вперед. Или они говорят, что могут для вас что-то сделать (достать например, какой-то дефицитный товар), но вы должны непременно быстро выписать счет и т. д.

Нередко мошенники ставят жертв в известность, что у них, якобы, есть большие связи или очень ценная информация, к которой лишь они имеют доступ. И вы должны еще радоваться, что они с вами вообще имеют дело.

При всем этом мошенники выглядят весьма правдоподобно прилично, они прекрасные актеры и разбираются в пси-

хологических тонкостях.

В то же время все описанные признаки, которые могут принадлежать мошенникам, не обязательно говорят о том, что конкретный человек, обладающий этими признаками, обязательно мошенник. Нужно делать дополнительные проверки и использовать лайспотинг (о котором написано ниже).

Об используемых преступниками приемах

Об используемых преступниками приемах рассказал психиатр-криминалист Михаил Виноградов [3]:

> «Мошенники, как правило, не обладают специальными познаниями в области психологии. Они используют два приема:
>
> 1.Маска доброжелателя. Мошенники сочувствуют, обещают помочь. Человек принимает доброжелательность как норму поведения и не видит, что за этим скрывается что-то иное. Люди отзывчивы. Если к человеку подходят с добрым советом, он готов открыть душу. И это оборачивается для него большой бедой.
>
> 2.Нападение на жертву. Если человек понимает, что его затягивают в ловушку, он уходит от общения. Видя, что втереться в доверие не получилось, мошенник переходит к угрозам. Запугивает человека, что будут проблемы с бизнесом, пострадают близкие или на него

нашлют порчу».

2.3 О некоторых способах проверки людей на причастность к мошенничеству

Изучение адреса предполагаемого мошенника. Составление «черных списков»

Мошенники зачастую указывают на своих визитках не свои адреса (адреса, которые не принадлежат их компаниям). Обычно они указывают такие адреса, которые ассоциируются с такими понятиями как богатство, успех, престиж и т. д.

Рассмотрим пример Игоря Качалова [4]:

«В опыте… была встреча на одной

из международных конференций с неким консультантом, представлявшим себя как мировая знаменитость и мировая звезда. А загвоздка была в том, что я даже не слышал эту фамилию, хотя, в общем-то, слежу внимательно за миром консультантов. После обмена визиток во время конференции я зашел в поисковую систему Google, вошел в подраздел „Карты“ и начал вводить адреса, написанные на визитной карточке. Оказалось, что в небольшом адресном блоке данный консультант мошенник умудрился ввести фактически три разных адреса. В каждом из этих адресов присутствовало ключевое престижное слово „Майями“. В каком-то случае Майями Бич, Северное Майями и так далее. Но в любом из вариантов там не было указания конкретного дома по одной простой причине – это было трудно сделать. Вводя один адрес, мы попадали, например, на пирс, где просто пришвартованы моторные лодки и яхты. А обзор в радиусе ближайшего километра-двух даже не показывал ни одного намека на офис консалтинговой фирмы. Следующий адрес показывал окрестности жилого дома и так далее.

И, наоборот, когда мы проверяли другую фирму, мы увидели ожидаемое офисное здание, увидели все вплоть до табличек на двери и даже номер автомобиля этого человека, который был припаркован к этому офисному зданию».

Если вы заподозрили человека в мошенничестве, поста-

райтесь узнать о нем как можно больше. Сделайте запросы о нем и о его компании в интернет-поисковиках (Яндекс, Гугл), в банках и специализированных компаниях, обратитесь к юристам, запросите у него какие-нибудь документы с печатями, изучите информацию о нем, воспользовавшись инернет-сервисом. Например, на сайте Информационно-аналитического агентства Safe Partner можно найти адреса таких сервисов [5].

По возможности, постарайтесь лично посетить офис предполагаемого преступника. Если его офис совсем не такой, каким он вам представлялся, или если его вообще не существует, не связывайтесь с таким «партнером».

Заведите свои черные списки, вписывая в них информацию о не оправдавших ваше доверие партнерах, чтобы ориентироваться на них и делиться ими с хорошими партнерами, которые доверие оправдали.

Запрашивание у предполагаемого партнера документов и информации и его изучение

Вы можете попросить, чтобы ваш предполагаемый партнер предоставил вам, к примеру: Справку об активах; Копии договоров, которые он с кем-то заключал. Можно попросить его обеспечить предоставление каких-либо первичных документов: платежек, справок о тиражах, потребительских анкет и т. п.

Можно сделать запрос аудиторского отчета, справки от налоговиков, справки об отсутствии судебных исков. В об-

щем, любых документов, из которых вам станет понятно, какой является данная компания и стоит ли с ней иметь дела.

Не стесняйтесь запрашивать у людей информацию. Это для цивилизованного мира нормально. Ведь лучше себя обезопасить, чем потом страдать от того, что вы стали жертвой мошенника.

Изучайте партнеров в интернете, постоянно осуществляйте маркетинговую разведку. Не забывайте, что кто осведомлен, тот вооружен. Не заключайте с кем попало контракты, привлекайте к их составлению юристов. Никому не верьте на слово особенно тем, кто много говорит и обещает золотые горы.

III Виды мошенничества в бизнесе (в корпоративном мошенничестве)

Рассмотрим ряд видов мошенничества в бизнесе (видов корпоративного мошенничества), используя материал с Лондонского сайта Национального бюро по борьбе с мошенничеством (NFIB) [6].

Фото из источника в списке литературы [6]

3.1 Мошенничество через получение контроля над учетной записью и «с приложением»

Мошенничество через получение контроля над учетной записью

Получение вашей учетной записи может произойти, когда мошенник или компьютерный преступник предстанет перед вами как настоящий клиент, получит контроль над вашей учетной записью и затем совершит несанкционированные транзакции. Любая учетная запись может быть получена мошенниками через банк, кредитную карту, электронную почту и т. д.

Учетные записи онлайн-банкинга обычно получаются мошенниками в результате использования фишинга, шпионских или вредоносных программ. Это форма интернет-преступности или компьютерных преступлений.

Мошенничество было совершено, если деньги вами были потеряны.

Мошенничество «с приложением»

Когда учетная запись открывается с использованием приложения поддельных или украденных документов не на свое имя, мошенники используют чужие учетные записи для снятия наличных денег, получения кредита или осуществления других способов обмана.

Предотвращение кражи личных данных может предотвратить мошенничество с использованием приложений. Знайте информацию, необходимую для защиты. Храните ваши данные в частном порядке, а конфиденциальные документы храните в надежном месте. Если вам больше не нужно письмо или документ, отбросьте его; просто разорвите его и положите в корзину, или даже сожгите. Всегда внимательно

но следите за финансами и кредитами.

Вы можете получать простые или электронные письма, подтверждающие получение новых карточек или ссуд, за которыми вы не обращались. Вы платите за подписку или прямой дебет, о которых вы не знаете, например, за пользование мобильным телефоном, которым вы не владеете.

Если вы стали жертвой кражи личных данных, вы можете стать жертвой мошенничества «с приложением»; ваши данные могут быть украдены и использоваться для открытия новой учетной записи на ваше имя.

Поддельные счета обычно открываются в банках или компаниях, которые занимаются оформлением кредитных карт, это быстрый способ доступа мошенников к средствам с использованием данных жертв.

Но мошенники также могут использовать данные для открытия учетных записей на ваше имя, таких как договор на мобильный телефон, счета за использование которого затем станут выставляться на ваше имя.

Мошенничество «с приложениями» отличается от мошенничества с помощью вашей учетной записи. В этом случае преступники используют ваши данные для запуска совершенно новых учетных записей, тогда как при мошенничестве с помощью учетной записи вы сами эти данные передавали. Разница в том, что жертвы могут полностью не знать о мошенничестве «с приложением», поскольку учетная запись была открыта без их ведома.

3.2 Мошенничество, связанное с банкротством, в ставках и азартных играх

Мошенничество, связанное с банкротством

Мошенничество, связанное с банкротством и неплатежеспособностью, может привлекать компании, мошеннически торгующие непосредственно перед объявлением неплатежеспособными компаниями или компаниями-фениксами.

Феникс-компания – это компания, созданная после объявления о несостоятельности какой-то компании, новая компания создается в одночасье с теми же атрибутами, но не несет ответственности за потери предыдущего бизне-

са, потому что они, похоже, являются разными лицами.

Мошенничество, связанное с банкротством и несостоятельностью, также включает незаконную торговлю при приостановлении или дисквалификации какого-то бизнеса. Банкротство описывает финансовый статус человека. Жертвами мошенничества, связанного с банкротством и несостоятельностью, как правило, являются предприятия, которые предоставили кредит банкроту, например, компании, занимающиеся кредитными картами и кредитные компании. Мошенничество было совершено, если деньги были потеряны.

Мошенничество в ставках и азартных играх

Мошенничество в ставках и азартных играх происходит,

когда вам делают предложения о предоставлении своей внутренней информации или предположительно безумных систем, которые гарантируют вам прибыль от азартных игр – на скачках, футболе или различных спортивных мероприятиях.

Остерегайтесь любой схемы, которая гарантирует, что вы выиграете; азартная игра по самой своей природе закладывает деньги на неизвестный исход. Не делайте ставки от имени кого-то другого, особенно того, кого вы не знаете. Спросите себя, почему кто-то продает свои секреты, если у него есть знания. Если это звучит слишком хорошо, чтобы быть правдой, возможно, это неправда.

Как это происходит? Вы получаете глянцевую брошюру, представляющую вас спортивному инсайдеру, у которого имеется послужной список выигрышных ставок. Вас просят заплатить абонентскую плату заранее, чтобы вы могли получить конфиденциальную информацию, которая даст вам преимущество. Вам говорят, что игрок не может разместить свои собственные ставки, потому что они известны букмекерам; они нужны вам и другим, таким же как вы, чтобы делать ставки от их имени.

Вам предлагается внутренняя информация, которая ориентирована на скачки, но может включать в себя ставки на любой вид спорта. Мошенники не имеют внутренней информации или непревзойденных систем, которые гарантируют выигрышные ставки, и вы не сможете увеличить свои

шансы на выигрыш через эти схемы.

В некоторых случаях мошенники будут использовать ложные показания от других, которые, по их утверждению, взяли на себя раздачу советов или приведение примеров гонок, где они каждый раз оказывались правы. Вас попросят заплатить абонентскую плату за отправку вам, якобы, конфиденциальной информации.

Вам может быть предоставлена бесплатная ставка, чтобы вы начали – это либо ставка на фирменного фаворита, либо ставка из тайных советов, которые давали другим жертвам для всех других возможных результатов в той же гонке или событии, так что нужна всего одна выигравшая жертва, чтобы ошибочно полагать, что система работает.

Мошенники будут удерживать авансовый взнос, вашу ставку или подписку и разорвут с вами контакт, если ваши ставки проиграют. Это противоречит правилам гоночных соревнований для людей в отрасли, которые передают конфиденциальную информацию, поэтому маловероятно, что любой, кто имеет внутреннюю информацию, будет рекламировать ее.

3.3 Мошенничество с бизнес-каталогами и с публикацией

Мошенничество с бизнес-каталогами

Мошенничество с бизнес-каталогами происходит, когда вашему бизнесу предлагается бесплатная реклама по почте, электронной почте или факсу, но затем выставляется счет за услугу.

Защитите себя. Обучите своих коллег. Сотрудники, кото-

рые занимаются внешними сообщениями, должны быть готовы бросить вызов вызовам, письмам и счетам-фактурам. Если вы получаете предложение, сделайте свое исследование. Является ли каталог законным? Является ли компания, предлагающая вам листинг, зарегистрированной в каких-либо торговых органах?

Проверьте все, что у вас есть, связанное с каталогами. Не оплачивайте счет, не спрашивая о нем; мошенники хотят, чтобы вы считали, чтобы вы приняли их перечень за часть перечней каталогов вашей компании.

Как это может происходить? Вы получаете звонок с просьбой подтвердить данные своей компании для службы каталогов. Вы получаете форму, предлагающую листинг, которая должна быть возвращена заполненной отправителю, звонящий спрашивает у вас, хотите ли вы быть указанным или нет. Вами подписываются выставляемые окончательные требования вашей компании для списка каталогов, которые вы не помните.

Как это может происходить? Мошенники отправляют компании форму в почте, по электронной почте или факсу, предлагая бесплатный список в бизнес-каталоге либо в каталоге, либо в Интернете. Вам предлагается вернуть форму, даже если вы не хотите размещать заказ, но небольшая печать заявляет, что, возвращая форму, вы совершаете заказ и будете платить за записи в каталоге.

Это своего рода фишинг или мошенничество с искаже-

нием информации: каталог может быть не так известен, как утверждается, или иметь очень малое количество копий в обращении, а в некоторых случаях он даже не существует. Затем вашей компании предоставляется фальшивый счет-фактура, при этом мошенники надеются, что деньги им будут выплачены без допросов. Если ваша компания запросит счет-фактуру, фиктивный издатель может попытаться представить себя в качестве агентства по взысканию долгов и отправить угрожающие письма.

Мошенничество с публикацией

Этот тип мошенничества случается, когда «холодные» абоненты связывают предприятия и продают рекламное пространство в фиктивной публикации по хорошей вроде как причине. У человека, получившего звонок, создается впечатление, что издатель сотрудничает с местными благотворительными организациями, службами неотложной помощи, предупреждения преступности или иными благородными сообществами. Иногда звонящий скажет, что бизнес разместил заказ ранее или даже что кто-то из бизнеса согласился вывезти рекламное пространство. Мошенники могут также отправлять счета-фактуры, независимо от того, согласилась ли жертва принять рекламное пространство. Они могут отслеживать счета-фактуры с угрозами судебного иска. Остерегайтесь тех, кто заявляет, что он представляет собой одно из следующих:

Благотворительное общество. Спасательную службу. 999 Услуги. Реабилитационный проекты. Этот тип мошенничества теперь продвигается к мошенникам, притворяющимся судебными приставами, и применяющим тактику давления, сообщающим жертвам, что они должны внести деньги через суд. Затем жертвы перечисляют деньги на банковский счет подозреваемого, даже когда не уверены, что они когда-либо соглашались размещать рекламу в журнале. Пожалуйста, не отправляйте деньги этим мошенникам. Мошенничество было совершено, если деньги были потеряны.

3.4 Проверочное мошенничество. Мошенничество с доменными именами

Проверочное мошенничество

Когда кто-то дает вам чек, он знает, что вы можете заплатить и наличными. Мошенники все сделали или подделали таким образом, чтобы банк не принял чек. В итоге вы оставите в кармане мошенника все, что вы заплатили за чек.

Принимайте чеки только от людей, которых вы знаете и которым доверяете. Попросите, чтобы вам дали шанс озна-

комиться с разными способами оплаты, которые требуют разного количества денег. Всегда используйте ручку при подписании чека. Четко напишите и поместите записи во все пустые пространства.

Найдите признаки подвоха. Может есть что-то подозрительное в самом чеке или в написании на о нем текста. Проверьте. Допустим, вам дали чек на большее количество денег, чем было согласовано, и вас попросили это изменить.

Как это может происходить? Мошенники могут использовать один из многих способов оплаты фиктивных чеков. Оплата вам денег в их чеке не будет отображаться в вашем аккаунте, чтобы они могли брать с вас товары, наличные или услуги, не платя вам взамен. Они могут использовать фальшивый чек, который был составлен мошенником, чтобы выглядеть реальным, или поддельный чек, который является подлинным, но украденным у кого-то другого с поддельной подписью.

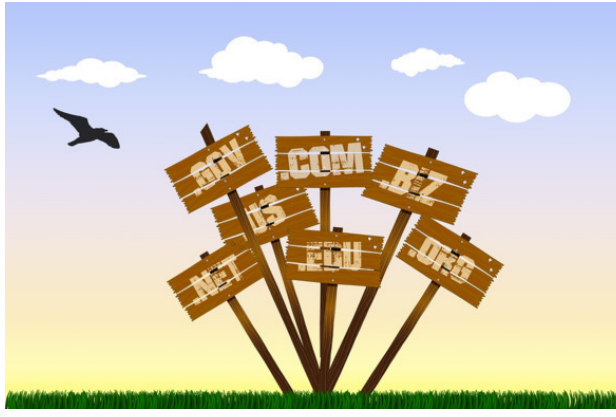
В качестве альтернативы они могут дать вам чек, который был каким-то образом изменен, например, имело место вмешательство в функции безопасности, что заставило его выглядеть хорошо для вас, но будет отклонено банком. В некоторых случаях они могут использовать исчезающие чернила при написании чека, поэтому значение суммы или подпись исчезли к тому моменту, когда ваш банк станет обрабатывать его.

Вы можете потерять еще больше денег за счет переплаты.

Это когда кто-то платит вам или вашему бизнесу, используя фальшивый чек, который выписан на более чем согласованное денежное значение. Они дадут вам повод для написания чека на дополнительную сумму и попросят отправить его им обратно. Если вы отдаете разницу с учетом изменений мошеннику наличными, проверка становится невозможна, а мошенник прерывает все контакты.

Мошенники часто используют эту методику переплаты по чекам для фиктивных рабочих мест или для продажи по классифицированным рекламным объявлениям.

Мошенничество с доменными именами



Здесь речь идет о предложении вам адреса веб-сайта

и ложном обвинении вас. Защитите себя.

Не реагируйте на холодные звонки, когда вам предлагают купить доменные имена. Не покупайте под давлением. Сделайте свое собственное исследование с поставщиком, которого вы знаете и которому доверяете. Знайте, сколько стоит покупка доменного имени. Знайте, кто поставляет ваше доменное имя, и будьте готовы оспорить любые счета от поставщиков, которых вы не знаете.

Вы вызваны из синего с предложения об очень желательном для вас доменном имени. Вам говорят, что кто-то еще собирается купить адрес, и вам нужно решить прямо сейчас, если хотите этот адрес иметь. Вам в итоге выставляют счет за доменное имя, которое вы не используете, или от поставщика, у которого вы никогда ничего не покупали.

Как это происходит? Мошенники находят доменные имена, которые подходят для вас или для вашего бизнеса. Они поставят вас под давление, чтобы вы купили быстро, чтобы у вас не было времени проверить их подлинность или сколько доменное имя действительно стоит, или даже продается ли оно вообще. Они могут принять ваши платежные реквизиты и разорвать все контакты после этого, не предоставив вам обещанный домен.

Некоторые мошенники высылают фиктивные счета-фактуры для доменов, которых у вас нет, или изучают принадлежащие вам домены, и представляют все так, словно ваш реальный поставщик требует плату за продление.

3.5 Использование активов и информации. Мошенничество с счетами

Использование активов и информации

Это когда активы организации используются для неофициальных целей. Мошенничество, связанное с эксплуатацией активов и информации, может включать мошенничество

тех, кто предоставляет информацию аутсайдерам для личной выгоды. Этот тип мошенничества не включает в себя кражу у компании инсайдерами, например, кражу стационарных объектов.

Мошенничество с счетами

Поддельные мошенничества со счетами случаются, когда мошенники отправляют счет в компанию, запрашивая оплату товаров или услуг.

В счете-фактуре может быть указано, что срок платежа прошел или вам угрожают, что неплатеж повлияет на кредитный рейтинг. Фактически, счет-фактура является поддельной и предназначена для товаров и услуг, которые не были вами заказаны или получены.

3.6 Ложное мошенничество в бухгалтерском учете. Фиксированное мошенничество

Ложное мошенничество в бухгалтерском учете

Ложное мошенничество в бухгалтерском учете происходит, когда активы компании завышены или обязательства занижены, чтобы сделать видимость, что бизнес финансово сильнее, чем он есть на самом деле.

Ложное мошенничество с учетными записями включает

сотрудников или организации, которые изменяют, уничтожают или деформируют любую учетную запись; или представление счетов от отдельного лица или организации так, чтобы они не отражали истинную стоимость или финансовую деятельность этой компании.

Ложный учет может иметь место по ряду причин:

для получения дополнительного финансирования от банка; ради сообщения о нереалистичных прибылях;

для раздувания цен акций;

ради сокрытия потерь;

для привлечения клиентов, чтобы показать себя более успешными, чем есть на самом деле;

для получения бонуса, связанного с производительностью; чтобы скрыть кражу.

Каковы бы ни были причины ложного учета, все они мотивированы необходимостью фальсификации записей, изменения цифр или, возможно, сохранения двух наборов финансовых счетов.

Трудно обнаружить действия, связанные с фальсификацией аккаунтов, особенно если вы управляете организацией. Некоторые примеры ложного учета мошенничества включают:

работника, делающего завышенные расходы;

клиента или сотрудника, фальсифицирующего счета, чтобы украсть деньги;

служащего, использующего ложный учет для прикрытия

убытков, возникших в результате торговли или мошеннической деятельности.

Если вас не предупредят о проблеме, вы не узнаете о каких-либо потерях или о преступной деятельности, которая их вызывает.

Находящееся в «крайнем конце шкалы» мошенничество может означать, что компания понесла серьезные финансовые убытки и/или торгуется в то время как она неплатежеспособная.

Что делать, если вы стали жертвой ложного мошенничества?

Ложный учет является уголовным преступлением. Поэтому необходимо обратиться в соответствующую инстанцию, и не важно, о каком количестве украденных денег идет речь.

Ваша организация также может рассмотреть вопрос о принятии мер для возмещения любых убытков сотрудниками, совершившими мошенничество. Вам нужно выяснить природу и масштабы любых потерь. Это может быть сделано вашими собственными бухгалтерами или внешними консультантами, но не ждите, пока они не закончат свою работу, прежде чем вы сообщите об их мошенничестве.

Защитите себя от ложного учета мошенничества. Ваша организация может предпринять следующие шаги, чтобы защитить себя от ложного учета:

постановка на обсуждение;

контроль доступа к зданиям и системам с использованием

уникальной идентификации и паролей;

ограничение и внимательное слежение за доступом к конфиденциальной информации;

обеспечение четкого разделения обязанностей рассмотрение вопроса о ротации работ; использование многоуровневых полномочий и уровней подписей для платежей; регулярная сверка банковских выписок и других счетов; осуществление время от времени процессов и процедур аудита;

пропаганда культуры осведомленности о мошенничестве среди сотрудников; принятие и внедрение политики абсолютной нетерпимости к мошенничеству сотрудников; подготовка четкого плана реагирования в случае обнаружения мошенничества.

Фиксированное мошенничество

Фиксированная линия или мошенничество с премиальными ставками – это когда мошенничество совершено против телефонных компаний. Фиксированное мошенничество может быть сделано несколькими способами.

В некоторых случаях мошенники получают доступ к коммутатору и продают другим людям возможность совершать звонки через коммутатор. Это называется Dial Through Fraud (DTF) или мошенничеством с прямым внутренним доступом к системе (DISA).

Фиксированное фиктивное мошенничество может включать мошенничество с тарифами Premium Rate, которое происходит, когда мошенники значительно увеличивают количество звонков на премиум-номер, чтобы увеличить доход,

получаемый от него.

Мошенничество с продажей рекламы – еще одна форма мошенничества с фиксированной линией. Это когда мошенники берут телефонную услугу и продают другим людям возможность совершать звонки через нее.

Мошенник не намерен оплачивать счет. Окончательная форма мошенничества с фиксированной линией включает мошеннические приложения. В этом типе мошенничества мошенник представляет себя телефонной службой с ложным именем и оставляет плохую задолженность.

3.7 Мошенничество «правительственного агентства». Страховое мошенничество

Мошенничество «правительственного агентства»

Правительственные аферисты – мошенники, которые отправляют официальные письма или электронные письма для запроса денег или личной информации. В переписке создается впечатление, что они из правительственного отдела и подразумевается, что они имеют определенную форму полномочий.

Письмо или электронное письмо может сообщить, что вы должны зарегистрироваться для того, чтобы соблюдать какие-то законы – за определенную плату.

Конец ознакомительного фрагмента.