GRACERS LAW FIRM

Цифровая эволюция

«Переход государства в цифровую плоскость вывел на поле рейдерской войны нового игрока — хакера»

ОБРАЩАЕТ ВНИМАНИЕ СЕРГЕЙ ЛЫСЕНКО, УПРАВЛЯЮЩИЙ ПАРТНЕР GRACERS LAW FIRM

— Представители органов в сфере государственной регистрации констатируют уменьшение количества жалоб по вопросам защиты бизнеса от рейдерства. Ощущается ли «потепление» во взаимоотношениях бизнеса и государства, в частности, в работе вашей компании?

— Уменьшение количества обращений в государственные органы отнюдь не свидетельствует об уменьшении количества рейдерских атак. Противодействие законной хозяйственной деятельности — это системная проблема для национального бизнеса. И далеко не всегда эта проблема связана с задействованием государственных органов. Из пяти кейсов только в одном случае давление на бизнес исходит от правоохранительных органов. Подавляющее большинство атак инициируют недобросовестные конкуренты или лица, которые соблазнились чужим бизнесом и хотят им завладеть. Конечно, они задействуют властные инструменты для достижения своих целей: привлекают органы государственной регистрации или нотариата для тех или иных регистрационных действий. Однако возлагать ответственность за рейдерство исключительно на государство ныне не приходится.

Уменьшилось ли количество жалоб относительно защиты бизнеса от рейдерства? Поверьте, представители госорганов, озвучивая такую статистику, не лукавят. Но этот факт не имеет ничего общего с повышением эффективности работы органов по противодействию рейдерству. Наоборот, их манера работы вынуждает потенциальных заявителей прибегать к иным путям защиты. Приведу пример. Не так давно, защищая клиентку в, казалось бы, тривиальной ситуации, мы столкнулись с довольно показательной ситуацией в Офисе противодействия рейдерству. Незаконность перерегистрации жилого дома с последующей продажей этого дома без подписей владелицы недвижимости доказана рядом экспертиз, осталось решить «регистрационный момент». Жалобу в интересах клиентки Офис противодействия рейдерству рассмотрел в конце августа, но решения не принял до сих пор. Что это: блокирование принятия решения нашими оппонентами или жернова бюрократической машины — вопрос остается открытым.

— Что в таком случае делать бизнесу? Куда обращаться за защитой?

— Единственно верный путь — обращаться за защитой в суд. Но этот путь в условиях острого кадрового дефицита в судебной системе и непрогнозируемой судебной практики также не является легким и быстрым.

СЕРГЕЙ ЛЫСЕНКО

Родился в 1984 году в Киеве. В 2006 году окончил Национальную юридическую академию имени Ярослава Мудрого.

В 2006—2015 годах работал в органах прокуратуры. С 2015 года начал заниматься частной юридической практикой. В 2019 году основал юридическую фирму GRACERS law firm. Специализируется на правовом сопровождении сложных уголовных кейсов (White Collar Crime) и комплексной защите бизнеса.

Победитель конкурса «Адвокат года — 2020» в номинации «White Collar Crime».

Часто рейдеры разворачивают целую информационную кампанию против законных владельцев бизнеса, поэтому немаловажной составляющей защитной стратегии является реакция в публичной плоскости. В результате активная публичная коммуникация, обжалование всех незаконных регистрационных действий в судебном порядке, получение обеспечительных судебных документов до решения вопроса по существу станут залогом эффективной стратегии защиты с целью достижения необходимого результата.

— Методы давления на бизнес и рейдерских атак эволюционируют? Прибегают ли злоумышленники к креативным инструментам, усложняющим работу защитников?

— Все новое — это хорошо забытое старое. В отдельных случаях можно наблюдать возврат к методам если не 90-х, то начала «нулевых». Хотя такие банальные способы атак, как подделка судебных решений, документов или переписывание объектов недвижимости на бездомных лиц, встречаются все меньше и меньше.

Но с другой стороны, переход государства в цифровую плоскость вывел на поле рейдерской войны нового игрока — хакера. За последнее время значительно участились случаи использования действий хакеров для несанкционированного вмешательства в государственные реестры с целью изменения цифровой реальности. Эта проблема будет лишь усугубляться. И только представьте ее масштабы: теперь, чтобы изменить собственника или осуществить факт регистрации, даже не нужно задействовать так называемых черных нотариусов или регистраторов. Достаточно одного искусного хакера.

В таких случаях главное — быстро зафиксировать цифровые следы незаконного вмешательства в госреестры. К подобным ситуациям можно привлекать правоохранительные органы, однако методы уголовно-правовой защиты все же ограничены определенным рамками, поэтому и восстановить нарушенное право быстро нелегко.

— Часто можно услышать фразу о том, что безопасность бизнеса — дело самого бизнеса. Вы согласны с таким мнением? По вашим наблюдениям, у бизнеса есть осознанная стратегия в части организации мер по собственной защите?

— Доля правды в этом утверждении есть. Бизнес должен сделать все возможное для того, чтобы обезопасить себя от рисков. Стратегия организации собственной защиты должна содержать ряд предохранительных мер. Риски можно выявить и дать конкретные рекомендации по их нивелированию только после тщательного юридического аудита деятельности бизнеса.

Есть очень много общедоступных ресурсов, позволяющих отслеживать тревожные звоночки, которые в дальнейшем могут обернуться настоящими проблемами. Единый государственный реестр судебных решений необходимо проверять на предмет вынесения определений не только в отношении ваших контрагентов и не только в пределах территории месторасположения вашего бизнеса. Бывают случаи, когда определение следственным судьей выносится во Львове, а обыск проводится в компании из Харькова. Такие моменты необходимо вылавливать заблаговременно, ведь «маски-шоу» предупреждать о своем визите не будут. Впрочем, никто с обысков не начинает. Сперва происходит сбор информации и документов, причем не обязательно о компании, которая попала в поле зрения правоохранителей. Даже если та иная ситуация прямо вас не касается, вы должны оставаться начеку.

Всю эту мониторинговую систему необходимо тщательно выстраивать и настраивать. Нужно четко определить группу рисковых компаний (конкурентов и контрагентов) и понимать самые «болезненные» места бизнес-процессов.

— Что еще можно отнести к превентивным мерам для защиты бизнеса?

— Одним из предохранителей является введение комплаенс-программы на предприятии. Несмотря на то что компании внедряют их весьма неохотно, поскольку часто их (особенно в антикоррупционной части) насаждает государство, эти политики могут стать эффективным подспорьем для предотвращения проблемы. Комплаенс-программы позволяют уменьшить бизнес-риски во взаимоотношениях с «проблемными» контрагентами.

Немаловажным превентивным элементом также является налоговый аудит предприятия — вычисление слабых мест, которыми могут в дальнейшем заинтересоваться контролирующие органы. Также не стоит забывать об аудите кадровой составляющей предприятия на выявление сотрудников, которые могут быть восприимчивыми к вербованию как правоохранительными органами, так и конкурентами; о коммерческой разведке, контрразведке, информационной безопасности.

Все зависит от пожеланий клиента и того, сколько он готов заплатить. А тут уже включается украинский менталитет: все желают получить максимум за минимальную цену. Даже большой бизнес экономит на превентивной юридической защите, а потом удивляется, когда к нему наведываются «гости».

Понять происхождение проблемы и предотвратить ее — в этом и заключается профилактика захвата. А для этого бизнесу необходимо начинать диалог с юридической компанией задолго до наступления часа «Ч». Каждое звено бизнеса должно понимать свою роль, риски, за которые отвечает, и меры для защиты.

— Каким видам бизнеса следует опасаться рейдеров, необоснованных проверок контролирующих органов и правоохранителей больше всего?

— На сегодняшний день более восприимчивы к атакам рейдеров аграрные и фармацевтические компании — те бизнесы, которые активно развиваться. Все более и более интересной для рейдеров будет становиться IT-сфера. Сегодня она достаточно сложная в контексте понимания процессов структурирования, да и в Украине, как правило, этот бизнес присутствует только физически, а регистрируется за рубежом, что усложняет возможности для рейдерских манипуляций. Однако эта отрасль будет значительно усилена на счет прихода IT-бизнеса из Беларуси. Белорусский бизнес захватит большой объем национального рынка. Соответственно, такой аппетитный кусок будет привлекать преступников.