ФИНАНСЫ, КРЕДИТ И СТРАХОВАНИЕ / FINANCE, CREDIT, INSURANCE

DOI 10.24182/2073-6258-2025-24-2-15-19

Обзорная статья / Review article
УДК 343.721

Уэйлинг и псевдофранчайзинг как новые виды финансового мошенничества: особенности и угрозы

М. И. Глухова

кандидат экономических наук, доцент
кафедра менеджмента и маркетинга,
Московский психолого-социальный университет,
Москва, Россия
miss4@yandex.ru

Аннотация: *Финансовое мошенничество в 21-ом веке приобретает новые виды. В современных условиях всё чаще атакам подвергаются юридические лица, противостояние нарастает. Для успешной практики отражения атак мошенников необходимо иметь знания о трансформации форм мошенничества и методах, с помощью которых можно избежать нападений и не стать жертвой преступников. Особую проблему в данном процессе играет информация, скрываемая самими предпринимателями в качестве попытки спасти имидж организации и собственный авторитет, а также мультисубъектность мошенников.*

Предмет исследования — уэйлинг и псевдофранчайзинг как новые формы финансового мошенничества, которому подвергаются юридические лица. Методы исследования — исторический и логический. Результат исследования — обоснования возможности уклонения от новых форм мошенничества на современном рынке.

Ключевые слова: *псевдофранчайзинг, уэйлинг, мошенничество, мультисубъектность, предпринимательство.*

Для цитирования: *Глухова М.И. Уэйлинг и псевдофранчайзинг как новые виды финансового мошенничества: особенности и угрозы. Ученые записки Российской академии предпринимательства. 2025. Т. 24. № 2. С. 15—19. https://doi.org/10.24182/2073-6258-2025-24-2-15-19.*

Wailing and pseudo-franchising as new types of financial fraud: features and threats

M. I. Glukhova

Cand. Sci. (Econ.), Assoc.Prof.
Department of Management and Marketing,
Moscow Psychological and Social University,
Moscow, Russia
miss4@yandex.ru

Abstracts: *Financial fraud in the 21st century is taking on new types. In modern conditions, legal entities are increasingly being attacked, and the confrontation is growing. To successfully repel fraud attacks, it is necessary to have knowledge about the transformation of fraud forms and methods by which attacks can be avoided and not become a victim of criminals. A special problem in this process is the information hidden by the entrepreneurs themselves as an attempt to save the image of the organization and their own credibility, as well as the multi-personality of the scammers.*

The subject of the study is whaling and pseudo-franchising as new forms of financial fraud to which legal entities are exposed. The research methods are historical and logical. The result of the study is to substantiate the possibility of avoiding new forms of fraud in the modern market.

Keywords: *pseudo-franchising, whaling, fraud, multisubjectivity, entrepreneurship.*

For citation: *Glukhova M.I. Wailing and pseudo-franchising as new types of financial fraud: features and threats. Scientific notes of the Russian academy of entrepreneurship. 2025. T. 24. № 2. P. 15–19. https://doi.org/10.24182/2073-6258-2025-24-2-15-19.*

Финансовое мошенничество — не новое явление в хозяйственной жизни стран и народов. Появившись на заре цивилизации в виде фальшивомонетничества, пройдя путь пирамид и школ коучинга, оно не осталось в прошлом тысячелетии, а стало заметной проблемой современности. Сегодня этой проблемы так или иначе касаются учебные пособия по экономике, юриспруденции, финансам.

Финансовое мошенничество — это совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения.[1]

Всеобщий интерес к финансовой грамотности в сегодняшних условиях обусловлен как раз желанием обезопасить себя от всех многочисленных форм финансового мошенничества.

Особенностью финансового мошенничества современности стала его ориентированность на «крупных игроков» рынка. Если раньше жертвами становились отдельные граждане, причём преимущественно из незащищённых слоёв населения (пожилые люди, студенты, школьники), то сейчас атакам подвергаются руководители важнейших функциональных структурных подразделений ведущих фирм и корпораций. Для обозначения данного явления не так давно появился специальный термин, пришедший из китобойного промысла — уэйлинг. На сегодняшний день не существует общепризнанного определения данного понятия. Так, некоторые источники трактуют его как форму фишинга.

Уэйлинг — это форма целевого фишинга. Целью мошенников являются высокопоставленные сотрудники организации, либо лица, имеющие доступ к конфиденциальной информации или финансам компании. Атаки часто тщательно планируются, в них могут использоваться фальшивые веб-сайты и другие средства убеждения цели в подлинности запроса.[2] Также уэйлинг рассматривается как один из типов фишинга: «whaling (уэйлинг) очень похож на spear phishing (спеарфишинг), но вместо того, чтобы преследовать любого сотрудника в компании, мошенники специально нацеливаются на руководителей (или «крупную рыбу», отсюда и термин «уэйлинг», что в переводе с английского языка означает «китобойный промысел»)».[3]

Некоторые источники выделяют уэйлинг в отдельную форму.

Уэйлинг — специфическая форма нападения на руководителей высшего звена, топ-менеджмент корпорации с целью похищения крупных баз данных и денежных сумм.[4]

Думается, что более точным является второй подход, хотя по своим методам он схож с классическим фишингом — используется электронная почта, «письма счастья», ссылки на сайты преступников, но фишинг не нацелен на определённых лиц, вбросы напоминают «закидывание сети» в ожидании больших и маленьких «рыбок», а уэйлинг имеет свою целевую аудиторию. Он изначально выстраивается под конкретного ответственного работника. Как правило, его атака бывает подготовленной и смертоносной.

Например, в 2016 году руководитель службы оплаты труда в Snapchat по корпоративной электронной почте получил письмо, отправленное якобы генеральным директором, который срочно требовал информацию о личных счетах и заработной плате персонала. Персональные данные работников оказались под угрозой. Часто подобные истории приводят к краху компании. Так, в 2024 году компания Mattel, выпускающая продукцию для детей, в основном игрушки подверг-

[1] Гордячкова, О. В., Калаврий Т.Ю. Личные финансы и финансовая безопасность. Учебное пособие. – М.: Мир науки, 2021. – Режим доступа: https://izd-mn.com/PDF/48MNNPU21.pdf .

[2] Целевой фишинг и уэйлинг: рыбалка по-крупному.

https://www.sberbank.ru/ru/person/kibrary/articles/celevoj-fishing-i-uehjling-rybalka-po-krupnomu.

[3] 11 типов фишинга и их примеры из реальной жизни. https://www.cloudav.ru/mediacenter/tips/types-of-phishing/.

[4] Что такое уэйлинг атака? Фишинг по-крупному. https://www.kaspersky.ru/resource-center/definitions/what-is-a-whaling-attack?ysclid=m9vop60069336195026.

лась кибер-уэйлинговой атаке после того, как финансовый топ-менеджер получил письмо с просьбой о переводе денег, отправленное мошенником от имени нового генерального директора.

В результате компания потеряла 3 миллиона долларов и погибла.[5]

Частыми являются атаки на бизнес, имеющий сложный комплекс межфирменных и внутрифирменных отношений. Например, франчайзинговые компании, испытывают атаки со стороны субъектов, получивших название «лжеРАФы». Так называют мошенников, маскирующихся под известную на финансовом рынке России Российскую ассоциацию франчайзинга.

Эта некоммерческая организация оказывает реальную помощь малому и среднему предпринимательству, вовлекая его в орбиту крупного бизнеса, предоставляя важную для развития информацию, оказывая различные формы содействия, такие как организация встреч, прогнозы, консалтинг, совместные обсуждения, опросы.

С 2010 года Ассоциация функционирует на основе Стратегии развития франчайзинга, в которой были сформулированы основные цели РАФ: обеспечение малых и средних фирм, работающих по системе франчайзинга ресурсами, прежде всего — информированным персоналом, выход российских малых и средних фирм на мировой рынок и генерация концепций, представленных в форме новых франшиз.

Сама Российская ассоциация франчайзинга была создана в 1997 году и сегодня объединяет свыше семидесяти всем известных франчайзинговых, консалтинговых и банковских организаций.

Она добилась международного влияния и признания, а также активно вносила и вносит актуальные изменения и дополнения в действующее хозяйственное законодательство.[6]

Именно РАФ впервые увидела проблему финансового мошенничества на рынке франчайзинга и поставила цель: освобождение рынка от мошенников и «липовых» франшиз.[7]

Уже 15 лет назад именно РАФ впервые было упомянула о существовании такого явления как «липовая франшиза», сегодня этот термин почти не используется, а активно используются термины «лжефраншиза» и «псевдофранчайзинг».

Под ним подразумеваются группы организаций, объединённые концессионными договорами, в которых нет важнейших атрибутов франчайзинговых правоотношений — паушального платежа, текущих платежей или «роялти», которые представляют собой основу конструкции франчайзинга.

Эту модель используют молодые фирмы, которые берут за основу не свой, самостоятельно разработанный и «раскрученный» товарный знак, а некий придуманный и несуществующий «брэнд», который «продемонстрировал эффективность» в каком-то мифическом регионе.

РАФ активно противодействовала мошенникам, помогая честному бизнесу, естественно, что она заработала имя и стала популярна в бизнес-кругах.

Ассоциация сегодня является объединяющим хабом для всех, кто так или иначе заинтересован в развитии франчайзинговых отношений, активно работает со средствами массовой информации, проводит PR-акции, информирует своих членов о важнейших событиях и публичных мероприятиях на рынке франчайзинга.

Но всё больше и больше возникает фирм, которым успех РАФ, как говорится, «не дает спать спокойно». Они пытаются выдать себя за Ассоциацию и представляют свой сайт как официальный сайт РАФ. Захватывая таким способом клиентов, они навязывают им платные услуги, рекомендуют сотрудничество со своими мошенническими подразделениями и похищают информацию конфиденциального характера.

К сожалению, многие представители молодого бизнеса, молодые неопытные руководители оказываются пойманными в подобные ловушки. Что бы этого не произошло, менеджеры просто обязаны знать, какие моменты должны их насторожить, так как это имеет прямое отношение к финансовой безопасности.

---

[5] Что такое уэйлинг атака? Фишинг по-крупному. https://www.kaspersky.ru/resource-center/definitions/what-is-a-whaling-attack?ysclid=m9vop60069336195026 .

[6] Стратегия РАФ. https://old.rusfranch.ru/about/strategiya_raf/ .

[7] Стратегия РАФ. https://old.rusfranch.ru/about/strategiya_raf/.

Например, очень многое скажет call-центр, каким образом, с использованием каких лексических форм его работники общаются с клиентом.

Необходимо обратить внимание, насколько ненавязчиво (или же навязчиво) работники центра предлагают с первых минут что-то приобрести.

Кроме того, необходимо понять, связаны ли предлагаемые услуги с данными отношениями франчайзинга именно по определённой франшизе. Если предлагаются услуги, не имеющие прямого отношения к предмету франчайзинга, безусловно, стоит сразу отказаться от сотрудничества.

Следует помнить, что любая Ассоциация имеет Президента, членов, почётных членов, она занимает активную позицию, связанную с социальной ответственностью бизнеса, проводит конференции, встречи в формате как онлайн, так и офлайн, открывает контакты, готова к сотрудничеству в разных формах. Если ничего этого нет, то сайт организации «пустой», фото мероприятий отсутствуют, анонсов событий нет, контакты немногочисленны и спрятаны. Скорее всего, подобная организация — интернет-магазин, цель которого реализовать наивному молодому бизнесмену лжефраншизу. От подобных коммуникаций сразу нужно отказаться.

Ещё одной особенностью финансового мошенничества в современных условиях является его мультисубъектность.

Если раньше преступления совершались в подавляющем большинстве героями-одиночками с невероятной харизмой, которые могли увлечь за собой жертву, то сегодня действуют целые группы, «цепочки», которые сознательно и профессионально психологически воздействуют на жертву. Так, в том же уэйлинге, вначале собирается вся доступная в открытых источниках информация о будущей жертве. Даётся прогноз типу личности — предпочтениях, степени экстраверсии или интроверсии, создаются модели атаки на личность. После этого пишется письмо, возможно, с использованием фото или с отсылкой о тех или иных событиях, имевших место в прошлом. Жертва должна быть введена в заблуждение, должна почувствовать, что общается с руководителем или коллегой, не заподозрить «чужого». IT-специалисты работают над «правдоподобным» сайтом с соответствующим интерфейсом, адресом электронной почты.

Практически то же самое можно сказать и о лжеРАФах. Здесь «трудятся» и маркетологи, и иные специалисты, которые ведут жертву, не давая ей никаких шансов, если она имела неосторожность к ним обратиться и начать сотрудничество. Так, параллельно с Российской Ассоциацией Франчайзинга, только в Москве есть несколько её копий — Международная Ассоциация Франчайзинга, Российский Консультант Франшиз, Русская Франшиза.[8]

При этом фирмы, корпорации, компании, пытаясь позаботиться о своём имидже, скрывают информацию о нападении. Они не обращаются в следственные органы, что делает ситуацию более сложной. Безусловно, здесь имеет место ложное понимание авторитета и отсутствие социальной ответственности бизнеса перед обществом. Бизнес должен проинформировать и предупредить участников рынка о финансовом мошенничестве, в борьбе с которым главное оружие — гласность.

Главная опасность финансового мошенничества — разрастание материального ущерба до небывалых размеров, превращение проблемы в макроэкономическую. Так, общий ущерб от деятельности мошенников по итогам девяти месяцев 2024 года достиг 150 млрд. руб., среди которых 15 млрд. руб. пришлось на банковские операции без участия и без согласия клиента.[9]

Среди преступлений в сфере информационно-коммуникационных технологий за девять месяцев 2024 года Следственный комитет РФ зарегистрировал 353 000 таких случаев, что на 25,6% больше, чем было за аналогичный период прошлого года (281 000).[10]

Ущерб от мошенничества исследовали специалисты Сбербанка.

[8] Мертвые души франчайзинга https://buybrand.ru/articles/1909/ .

[9] СК оценил ущерб от мошенничества. https://www.vedomosti.ru/finance/articles/2024/12/05/1079559-sk-otsenil-uscherb-ot-moshennikov.

[10] Там же.

Сбербанк общие потери российской экономики от мошеннических схем оценил в 1 трлн. руб. Об этом официально говорил в ноябре 2024 года заместитель председателя правления банка Станислав Кузнецов.[11]

Но никакими стоимостными характеристиками нельзя измерить разрушение доверия, которое превалирует в обществе. То, что воспитывалось в людях на протяжении почти всего двадцатого столетия, разрушается безвозвратно. Исследования социологов показали, что значимость такого социального фактора как «вера в силу добра» постоянно понижается.[12] Социальные потери этого явления неисчислимы.

Список литературы

1. Глухова М.И. Роль нетворкинга в преодолении «псевдофранчайзинга» как новой формы финансового мошенничества в современной экономике. Путеводитель предпринимателя. 2025. Т. 18. № 1. С. 60–64. https://doi.org/10.24182/2073-9885-2025-18-1-60-64.
2. Гордячкова, О. В., Калаврий Т.Ю. Личные финансы и финансовая безопасность. Учебное пособие. – М.: Мир науки, 2021. – Режим доступа: https://izd-mn.com/PDF/48MNNPU21.pdf. (дата обращения: 22.04.2025). – Текст: электронный.
3. Купрейченко А.Б. Психология доверия и недоверия. – М.: Изд-во «Институт психологии РАН», 2008, 564 с.
4. Мертвые души франчайзинга. https://buybrand.ru/articles/1909/ (дата обращения: 22.04.2025). – Текст: электронный.
5. Стратегия РАФ. https://old.rusfranch.ru/about/strategiya_raf/ (дата обращения: 22.04.2025). – Текст: электронный.
6. Что такое уэйлинг атака? Фишинг по-крупному. https://www.kaspersky.ru/resource-center/definitions/what-is-a-whaling-attack?ysclid=m9vop60069336195026 (дата обращения: 22.04.2025). – Текст: электронный.
7. 11 типов фишинга и их примеры из реальной жизни. https://www.cloudav.ru/mediacenter/tips/types-of-phishing/ (дата обращения: 22.04.2025). – Текст: электронный.

References

1. Glukhova M.I. The role of networking in overcoming «pseudo-franchising» as a new form of financial fraud in the modern economy. Entrepreneur's Guide. 2025. T. 18. № 1. P. 60–64. https://doi.org/10.24182/2073-9885-2025-18-1-60-64.
2. Gordyachkova, O.V., Kalavri, T.Y. Personal finance and financial security. Textbook. – Moscow: Mir Nauki, 2021. – Access mode: https://izd-mn.com/PDF/48MNNPU21.pdf.
3. Kupreichenko A.B. Psychology of trust and distrust. Moscow: Publishing house «Institute of Psychology of the Russian Academy of Sciences», 2008, 564 c.
4. Dead souls of franchising. https://buybrand.ru/articles/1909 / (date of access: 04/22/2025). – Text: electronic.
5. RAF strategy. https://old.rusfranch.ru/about/strategiya_raf / (date of access: 04/22/2025). – Text: electronic.
6. What is a whaling attack? Phishing in a big way. https://www.kaspersky.ru/resource-center/definitions/what-is-a-whaling-attack?ysclid=m9vop60069336195026 (accessed: 04/22/2025). – Text: electronic.
7. 11 types of phishing and their real-life examples. https://www.cloudav.ru/mediacenter/tips/types-of-phishing/.

Статья поступила в редакцию 25.04.2025; одобрена после рецензирования 12.05.2025; принята к публикации 15.05.2025.

The article was submitted 25.04.2025; approved after reviewing 12.05.2025; accepted for publication 15.05.2025.

[11] СК оценил ущерб от мошенничества. https://www.vedomosti.ru/finance/articles/2024/12/05/1079559-sk-otsenil-uscherb-ot-moshennikov

[12] Купрейченко А.Б. Психология доверия и недоверия. – М.: Изд-во «Институт психологии РАН», 2008. С. 125.