Содержание

Схемы мошенничества на маркетплейсах. Как определить мошенников

Начнем с описания схем мошенничества на маркетплейсах:

1. **Продажа подделок или неисправных товаров под видом подлинных**. Мошенник размещает фото и описание оригинальных вещей, а отправляет подделки по цене дорогостоящих товаров. В некоторых случаях покупатель получает даже не дешевый аналог, а мусор, камни и т.п., который подложили в коробку.

2. **Кража аккаунтов покупателей на маркетплейсе**. Мошенники регистрируются на площадке в качестве продавца и предлагают товар по очень привлекательной цене. После того как покупатель совершит заказ, с ним связывается продавец, и здесь схемы обмана могут варьироваться:

    - мошенники связываются с клиентами и сообщают, что оплата не прошла, после чего просят еще раз ввести данные от личного кабинета, но присылают ссылку на фишинговый сайт, который сложно отличить от реального;

    - мошенники отправляют рассылку с другими товарами и огромными скидками, а также ссылкой на оплату, по-прежнему ведущей на фишинговый сайт;

    - мошенники сообщают, что пункт доставки будет изменен, и предлагает продолжить разговор в мессенджере. Там у покупателя запрашивается код, который придет на смартфон, чтобы подтвердить смену пункта доставки. Код приходит с реального номера маркетплейса, что мешает жертве распознать обман. На самом деле, узнав номер телефона покупателя, мошенники используют его в качестве логина для входа в личный кабинет на маркетплейсе, а запрашиваемый код нужен для подтверждения.

Таким образом мошенники получают доступ к чужому аккаунту, с помощью которого можно:

- совершить покупки за счет обманутого покупателя;
- подать заявку на возврат денег за заказанный товар, но уже с реквизитами своей карты;
- получить информацию о данных банковских карт, привязанных к взломанному аккаунту.

3. **Обманные предложения заработать, поучаствовав в "продвижении" товара**. Мошенники предлагают купить определенный товар и написать на него отзыв; обещают вернуть затраты и выплатить вознаграждение. Как правило, первые недорогие покупки действительно вознаграждаются, но после оплаты дорогостоящего товара клиент не получает ни его, ни денег.

   В другой похожей схеме покупателю предлагают делать заказы, а затем их отменять, объясняя это тем, что подобная активность якобы увеличивает рейтинг магазина. Оплата производится со специального счета, который принадлежит мошенникам. Покупатель вносит туда постепенно увеличивающиеся денежные суммы, а мошенники позволяют несколько раз отменить заказ и возвращают со счета стоимость товара вместе с небольшим вознаграждением. Как только жертва проникается доверием к схеме, ее просят внести более крупную сумму, после чего все контакты с мошенником обрываются.

   В некоторых случаях покупателю, готовому оставлять отзывы за деньги или покупать/возвращать товары, сообщают, что он принят на работу и необходимо зарегистрироваться по ссылке от "куратора". Такая ссылка вновь ведет на фишинговый сайт, где клиент оставляет персональную информацию и данные о карте, чтобы получать на нее "зарплату". Первое время небольшие суммы даже могут переводиться, но в итоге все сводится к краже денег с карты.

4. **Фальшивая техподдержка**. Мошенники выискивают в соцсетях клиентов, которые оставляют жалобы на работу маркетплейса, в частности на некорректно списанные суммы комиссий. Под видом официальных представителей службы поддержки площадки они связываются с покупателем и предлагают компенсировать ущерб, вернув на карту излишне удержанные деньги, после чего присылают специальную форму для ввода реквизитов. Форма возврата ведет на поддельную страницу банка, а мошенники получают всю информацию о карте.

Задача определения продавцов-мошенников разбивается на два этапа:

- выявить на этапе регистрации и не допустить до продажи товаров;
- выявить среди уже активированных продавцов.

На этапах регистрации флагами могут быть следующие моменты. Часть мошенников регистрируется под названием и ИНН уже существующей компании/ИП, часть - создают фирму-однодневку. В любом случае маркетплейс должны насторожить:

- признаки подделки документов (учредительных, паспорта и пр.), прикрепленных к заявке на регистрацию;

- запись в ЕГРЮЛ о недействительности ЮЛ/ИП;

- подозрительные контактные данные (некоторые мошенники создают временные электронные адреса, которые самоуничтожаются через определенный промежуток времени. Очевидно, реальный продавец так делать не будет. Таким образом, можно отлавливать мошенников по подозрительному e-mail (@mfyax.com, @gufum.com и др.));

- ряд признаков, характерных для компаний-однодневок (выявляются с помощью сервисов для проверки контрагентов типа СПАРК Интерфакс, Контур.Фокус и др.: минимальный размер уставного капитала, частая смена генеральных директоров, нулевая или не сданная в ФНС отчетность, большое количество кодов ОКВЭД, отсутствие сайта, рекламы, недействительный юридический адрес и т.п.;

- небольшое количество товаров для продажи (может говорить о том, что реальных намерений работать на площадке нет);

Если же мошенник успешно прошел все этапы регистрации и начал работать, привлечь к нему внимание могут следующие факторы:

- жалобы в поддержку от покупателей на недобросовестные действия Рассматривать метрику лучше и в абсолютном (общее количество), и в относительном выражении (число жалоб по отношению ко всем заказам), ведь у крупных поставщиков неизбежно будет больше ошибок в работе, необязательно вызванных мошенническими действиями;

- негативные отзывы на продавца. Похоже на жалобы, однако стоит иметь в виду, что они могут быть сфальсифицированы, например, конкурентами, чтобы убрать продавца с площадки;

- различные уловки продавца связаться с покупателем в обход площадки: ссылки на другие сайты, номера телефонов. аккаунты в мессенджерах и социальных сетях. Это не обязательно будет характеризовать его как мошенника, поскольку многие продавцы собирают контакты для своих баз, например, для рассылки рекламы или для других вполне законных целей. Вместе с тем практически все мошеннические схемы начинаются с попыток заполучить контактные данные покупателя. Общение в личном кабинете на Мегамаркете не предусмотрено, однако продавец может отвечать на вопросы о товарах, что увидят все покупатели, а также указать информацию при заполнении карточек товаров. Несмотря на то,

что на маркетплейсе есть проверка и ответов на вопросы, и карточек, не стоит недооценивать способности мошенников;

- комбинация косвенных признаков, указывающих на мошенничество:
    - подозрительно низкая цена, особенно в сочетании с бонусами;
    - недавняя дата регистрации магазина;
    - стопроцентная предоплата;
    - доставка курьером продавца.

Продуктовые фичи, которые могут помочь клиентам избежать неприятных ситуаций с мошенничеством

1. **Сигнал покупателям о том, что цена существенно ниже средней**. Первая причина, из-за которой пользователи попадаются в ловушку мошенников, - это желание существенно сэкономить. Мошенники предлагают приобрести дорогостоящий товар чуть ли не вдвое дешевле, чем в других магазинах. Для обычных продавцов это очень невыгодно. Если маркетплейс будет сигнализировать покупателю, просматривающему такие предложения, о том, что настолько низкая цена не соответствует рынку и подозрительна, возможно, часть из них не станет рисковать. Информацию о средней цене маркетплейс может агрегировать со своей же площадки либо ориентироваться еще и на другие маркетплейсы.

2. **Рейтинг благонадежности от маркетплейса**. Наряду с рейтингом от покупателей, который бывает накручен, маркетплейс может по характерным для мошенников признакам выставить и свою взвешенную оценку. В качестве критериев можно использовать косвенные признаки мошенничества, перечисленные в предыдущем разделе: срок работы на площадке, качество заполнения карточек, соответствие продаваемым товарам кодов ОКВЭД, способ доставки, действительность юридического адрес, процент отмены заказов и пр.

3. **Оценка достоверности отзывов**. Когда пользователь принимает решение о покупке у того или иного продавца, он опирается в том числе и на отзывы других покупателей. Мошенники часто прибегают к публикации фальшивых отзывов о своем товаре, причем для недавно зарегистрированного магазина важно опубликовать большое их количество за короткое время. Несмотря на формальное прохождение модерации, заметно, что многие отзывы сгенерированы нейросетями. Можно было бы внедрить систему, которая оценивает качество отзывов, учитывает скорость публикации и дает ответ, насколько те достоверны.

4. **Создание системы оповещений о мошенничестве и обучение пользователей**. Какими бы надежными ни были способы распознавания мошенников у площадок, конечной целью мошенников является обман конкретного покупателя. И именно от доверчивости и поведения

покупателя зависит, попадется он на удочку или нет. На интернет-площадках, в социальных сетях постоянно жалуются обманутые пользователи, хотя указанные ими схемы мошенничества известны уже довольно давно. Маркетплейс мог бы снизить число пострадавших, если бы в превентивных целях чаще и больше распространял информацию о способах обмана, о предпринимаемых мерах для устранения мошенников, а также о том, куда обращаться в случае обмана. Это может быть сделано, например, в виде тестов при регистрации покупателя, еженедельных рассылок о новых схемах, мини-игр и пр.

Механика доступа мошенника к контактам покупателя и борьба с фродерами

Когда покупатель оформляет заказ, продавцу передаются его данные, в том числе и контакты для связи. Даже после отмены заказа информация остается на стороне продавца. Дальше мошенникам обычно не составляет труда найти покупателя в мессенджерах и обратиться к нему за пределами площадки.

В том случае, когда заказ был отменен по вине продавца, можно направлять покупателю предупреждение с кратким описанием схемы мошенничества и призывом к осторожности, если за пределами площадки продавец начнет предлагать заказать тот же товар по такой же или еще более низкой цене.

Можно блокировать аккаунт продавца до окончания разбирательства, если доля отмененных по вине продавца заказов начинает превышать определенное значение.

Имеет смысл отслеживать, не используется ли в качестве контактных данных для разных продавцов один и тот же номер телефона или e-mail. Если один из таких магазинов уже был пойман на фроде, то второй наверняка принадлежит той же группе мошенников и следует ожидать обманных действий в отношении покупателей. Над таким магазином можно установить дополнительный контроль.

Встречается и такая схема обмана: продавец присылает покупателю поддельный товар, а чтобы тот не сумел оставить отрицательный отзыв, удаляет карточку товара и создает похожую на нее новую. Поскольку пострадавший может оставить отзыв только на тот товар, который купил, с разоблачением мошенника возникнут сложности. В таких случаях маркетплейс мог бы отслеживать подозрительные активности при смене карточек товара и приостанавливать работу аккаунта до выяснения обстоятельств.

Мегамаркет входит в один холдинг со Сбером - крупнейшим банком в России. Многие физические и юридические лица были или являются его клиентами. Таким образом, репутацию некоторых продавцов Мегамаркета можно проверить еще на этапе регистрации, пользуясь информацией о его работе в Сбере. Если продавец совершал сомнительные операции в банке, то это может быть сигналом, что и на маркетплейсе он не будет соблюдать правила.

Также в глобальном плане одним из возможных действий по препятствию недобросовестным продавцам может быть создание структуры, которая бы объединяла информацию о мошенниках с разных маркетплейсов, по аналогии с тем, как это сделано в банках: ООО и ИП, несколько раз уличенные в сомнительных операциях, больше не имеют возможности полноценно работать по расчетным счетам ни в одном банке, соблюдающем рекомендации Росфинмониторинга и ЦБ.

Анализ датасета и дизайн теста

Выводы, полученные в ходе EDA

Для начала приведем выводы, полученные на этапе предварительного анализа датасета:

- исходные данные содержат id продавца, информацию о датах регистрации и активации, форму организации бизнеса (ИП или ООО), а также признак мошенника, который проставляется в ходе ручной проверки при регистрации либо уже после поступления жалоб на продавца;
- в датасете находится информация о 35000 продавцах, начавших процедуру регистрации в период 02.01.2023 - 31.12.2023;
- дубликатов нет;
- удалены строки с некорректной либо не имеющей ценности для исследования информацией:
    - 194 строки с неправильно указанными датами: в базу не подтянулась дата регистрации либо дата активации превышает дату регистрации, что явно ошибочно (это 0,55% датасета); доля удаляемых мошенников среди всех мошенников датасета - 0,49%;
    - 700 строк без указания целевого признака (мошенник или нет); это 2% датасета; Таким образом, для анализа осталась информация о 34 108 клиентах (97,4% датасета);
- сделаны следующие заключения:
    - доля продавцов-мошенников в очищенном датасете - 8,2%. Добросовестных продавцов - 91,8%.
    - в среднем в день на платформе регистрируется 96 продавцов, из них 8 мошенников;
    - в течение всего 2023 года каждый месяц регистрировалось примерно одно и то же число продавцов (2900-3000), однако число мошенников среди них росло с января (200) по август. В сентябре и ноябре количество мошенников снижалось, но октябрьский и

декабрьский показатели совпадают с тем, что было в августе (250); таким образом, за год число мошенников увеличилось с 200 до 250 в месяц;

- определенный день недели не влияет на количество регистрирующихся продавцов в общем, однако среди мошенников несколько более популярны четверг, суббота и особенно пятница;
- средний период от регистрации до активации составляет 6 дней для обеих групп (вообще говоря, для мошенников он получился ниже - 5,9 дней против 6 для не мошенников, но различие оказалось статистически незначимым);
- 72% продавцов оформлены как ИП, 28% - как ООО. Доля ИП среди мошенников существенно выше - 84% против 71% среди добросовестных продавцов;
- среди неактивированных клиентов доля мошенников выше на 0,38% (8,46% против 8,08% среди активированных), однако различие не является статистически значимым;
- весь датасет можно разделить на 4 группы:
  - мошенники, которые сумели пройти регистрацию (4,7%);
  - мошенники, которые не сумели пройти регистрацию (3,6%);
  - добросовестные продавцы, которые активировались (53,3%);
  - добросовестные продавцы, которые не довели процесс регистрации до конца (38,4%).

- Стоит обратить внимание, что очень большой процент продавцов не проходит этап регистрации до конца. Это не является темой текущего исследования, но следовало бы пересмотреть процесс и выяснить, где возникают проблемные места и почему так происходит.

Дизайн теста. Определение метрик и разделение на группы

Итак, проблема, которую обозначает маркетплейс, - это успешная регистрация продавцов-мошенников на площадке. В настоящий момент признак неблагонадежного продавца проставляется в ходе ручной проверки при регистрации либо уже после поступления жалоб на продавца.

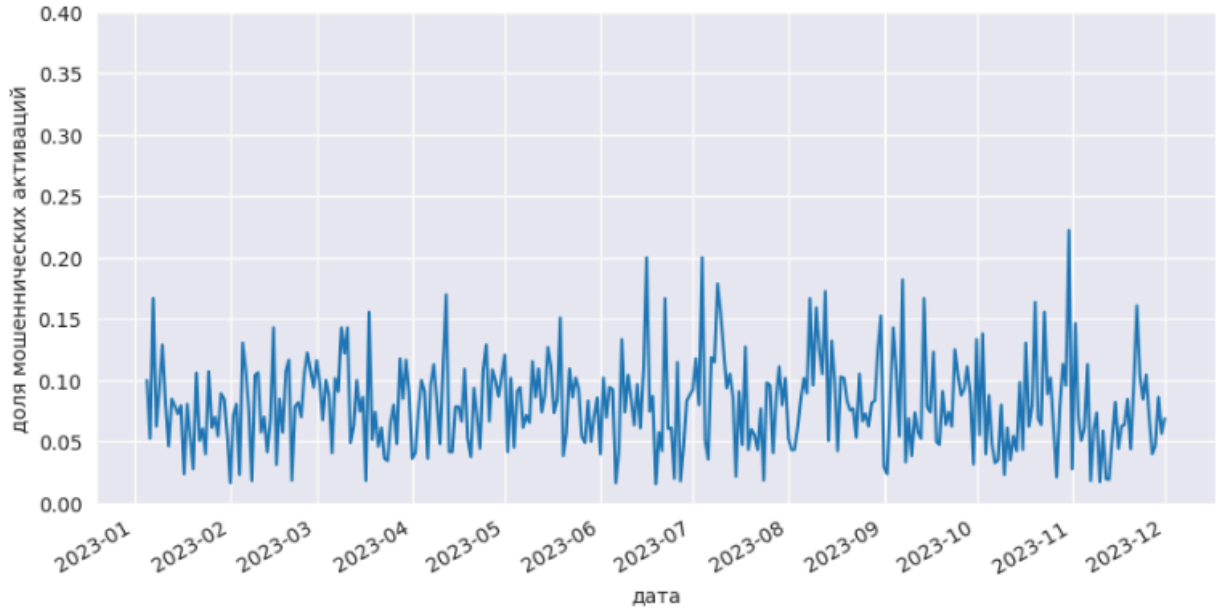
ML-команда предлагает внедрить в процесс регистрации модель автоматического определения продавцов-мошенников. Ее цель - обнаружить максимальное количество фродеров на этапе регистрации.

С помощью **А/Б-тест**а предлагается проверить качество и функциональность модели.

Гипотеза, которую будем проверять в ходе теста, заключается в следующем: новая модель снизит количество продавцов-мошенников, которые смогут пройти регистрацию на площадке.

В качестве **ключевой метрики** выберем отношение количества продавцов-мошенников, прошедших все этапы регистрации и активировавшихся, к общему количеству активированных продавцов за определенный период.

График указанной метрики за 2023 год выглядит следующим образом:



В среднем в день активируется 54 продавца, из них четверо (8%) оказываются мошенниками.

Барьерной метрикой будет количество ежедневных регистраций продавцов. Если модель применяет слишком жесткие критерии и часто ошибается, блокируя еще и добросовестных продавцов, они не смогут пройти этап регистрации и уйдут на другие площадки, что приведет к потере выручки и прибыли маркетплейса.

За **прокси-метрику** возьмем ежедневную долю жалоб, приходящихся на одного продавца: если новая модель работает эффективно и фильтрует мошенников на этапе регистрации, это в первую очередь скажется на количестве негативных обращений от покупателей.

В качестве **метода тестирования** будем использовать односторонний Z-тест для двух пропорций. Для него требуется, чтобы выборки из генеральной совокупности были случайны и независимы (о разделении на группы поговорим далее). Распределение z-статистики стремится к нормальному закону при больших объемах выборок, что позволяет использовать таблицу с критическими значениями стандартного нормального распределения. Для того чтобы принять решение, отвергнуть H0 или нет, необходимо знать размер выборок, число "успешных" исходов в обеих группах (в нашем случае -

количество найденных мошенников), а также уровень статистической значимости.

В качестве **уровня значимости и мощности** теста выберем традиционные значения - 0,05 и 80% соответственно.

Основываясь на данных за 2023 год, мы знаем, что в среднем в день регистрируется 96 продавцов, среднее число активаций 53,6, среднее число мошеннических активаций - 4,3 (8%). Разделять новых продавцов необходимо пополам случайным образом на две группы - тестовую и контрольную - так, чтобы выборки были стратифицированы. В нашем случае это означает, что в них соблюдаются максимально возможно близкие пропорции по следующим признакам:

- форма организации бизнеса (ООО или ИП);
- время с момента регистрации бизнеса;
- географический регион.

Расчет MDE

Рассчитаем MDE. Для этого нам понадобятся уровень значимости, мощность, а также размер выборки.

Размер выборки можно определить, имея представление о продолжительности теста. По условию задачи эта информация не дана. Предположим, что у нас есть возможность продолжать тест три недели. Тогда размеры выборок будут равны 54 * 21 / 2 = 567 продавцов.

Рассчитаем MDE по формуле:

$$MDE = \frac{\sqrt{2}\sigma(z_{\alpha/2} + z_{\beta})}{\overline{X}\sqrt{n}}$$

Размер выборки известен (567). Среднее значение и стандартное отклонение выбранной метрики (отношение числа продавцов-мошенников, прошедших все этапы регистрации и активировавшихся, к общему количеству активированных продавцов) составляют 0,08 и 0,03 соответственно. Z-значения для заданных alpha и beta также определяются. Получаем значение **MDE = 0,068 = 6,8%**. Подробные расчеты можно найти в приложении по ссылке:

https://colab.research.google.com/drive/1TunBybZJkzi44hu9oZ9qLXowW_R0vPz0?usp=sharing