Выявление фродовых сценариев

Анализ транзакций пользователей

Метод

Анализ и визуализация данных

Инструменты

Библиотеки python:

- pandas, numpy
- networkx
- matplotlib
- folium

Сценарий 1: Кардинг

Связь аккаунтов: все аккаунты зарегистрированы на одну почту

Особенности:

1. Отличие регионов по ip и регионов карт
2. Перебор большого количества номеров карт
3. Большое количество отклоненных транзакций

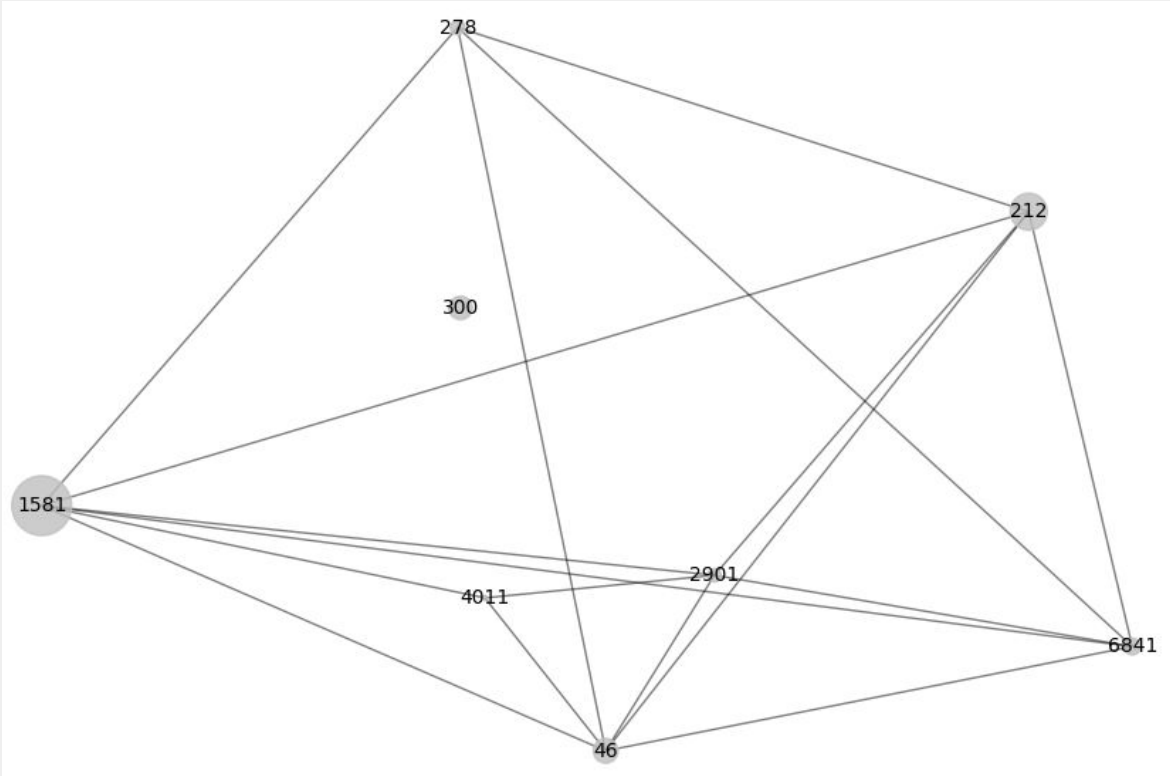
Сценарий 1: Кардинг

В наших данных главный фродстер – пользователь с почтой duuudin85@mail.ru

Количество транзакций – 869

Успешных – 3 на сумму $162,37

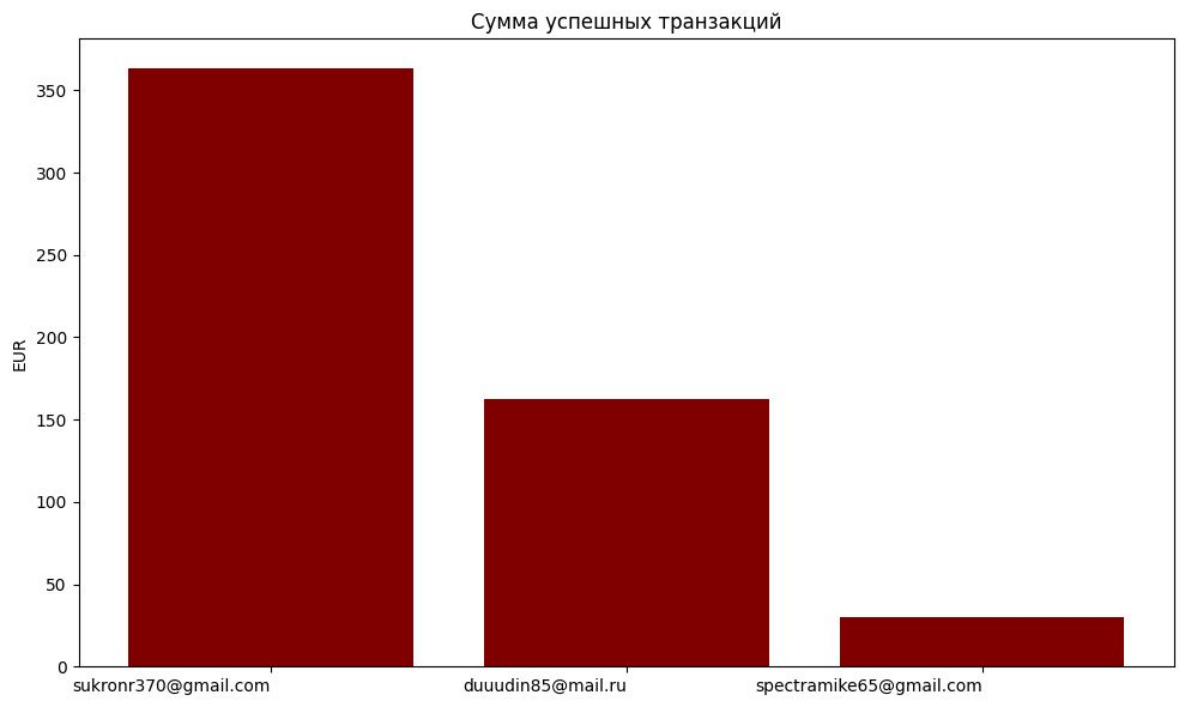
На графе – id мерчантов, связи означают использование идентичных номеров карт, размер вершин – количество транзакций у мерчанта



Сценарий 1: Кардинг

По данному сценарию можно идентифицировать и другие почты – с меньшим количеством транзакций, однако даже более успешными

Еще одним последствием сценария является использование карт реально зарегистрированных у мерчанта пользователей (таких обнаружилось 2, но транзакции неуспешны)



Сценарий 1: Кардинг

Митигация рисков:

1. Использование машинного обучения для оценки вероятности фрода, что позволит автоматически выявлять подозрительных пользователей без необоснованных блокировок.
2. Фильтрация по ключевым признакам фрода:
    a. Различие между страной по IP и страной эмитента карты
    b. Использование различных IP-адресов для транзакций
    c. Несоответствие имен владельцев карт и пользователей
3. Периодическая ручная проверка для подтверждения фрода в случае ограниченного числа подозрительных аккаунтов
4. Гибкая настройка фильтров для избегания чрезмерной блокировки и улучшения пользовательского опыта

Сценарий 2: Джон Доу

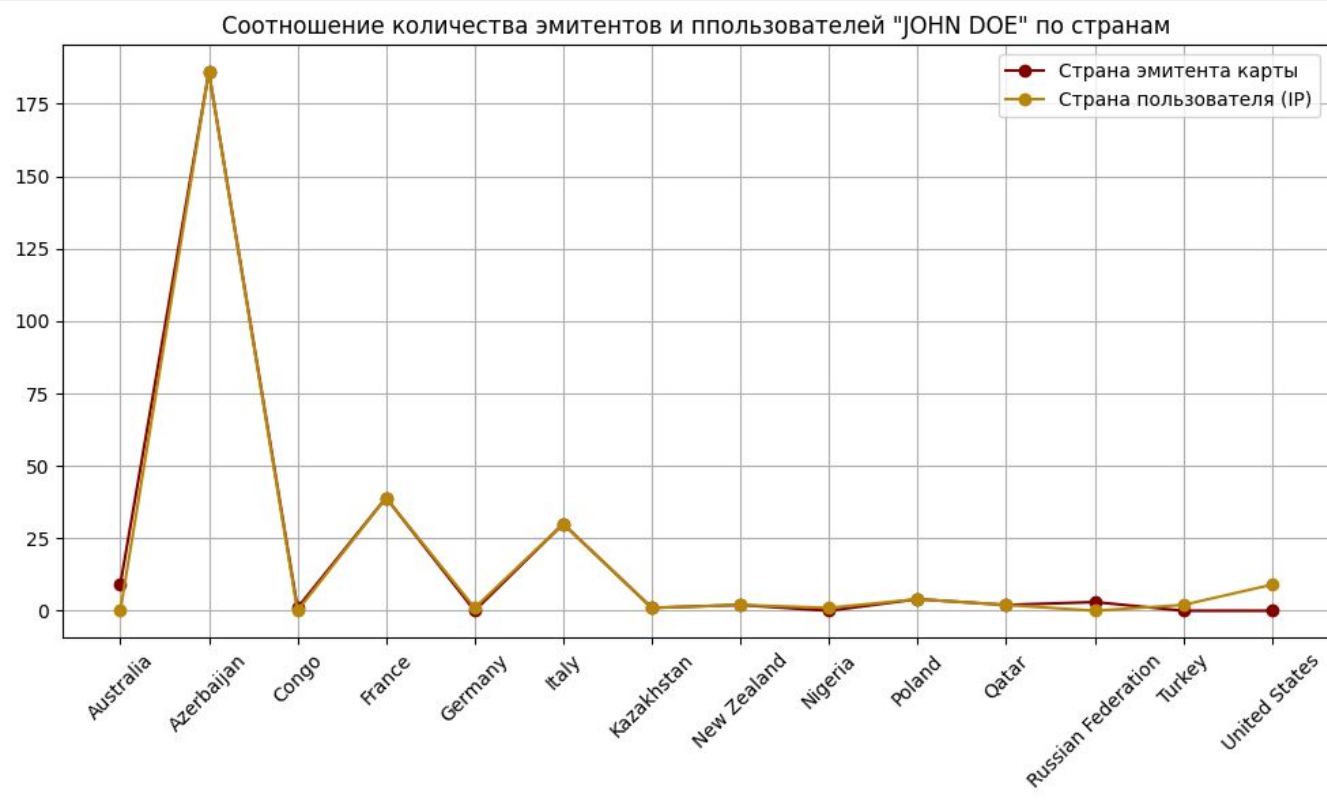
Связь аккаунтов: в реквизитах оплаты указывается одно и то же вымышленное имя – в нашем случае Джон Доу

Особенности:

1. Все платежи в один день через одного платежного провайдера у одного мерчанта
2. Используются названия электронных почт явно не свойственные обычному юзеру (payway.system@gmail.com, anonymous@tranzzo.com)
3. Платежи с данных аккаунтов идут из разных стран (которые сходятся со странами эмитентов карт)
4. На каждом аккаунте используется только одна карта

Сценарий 2: Джон Доу

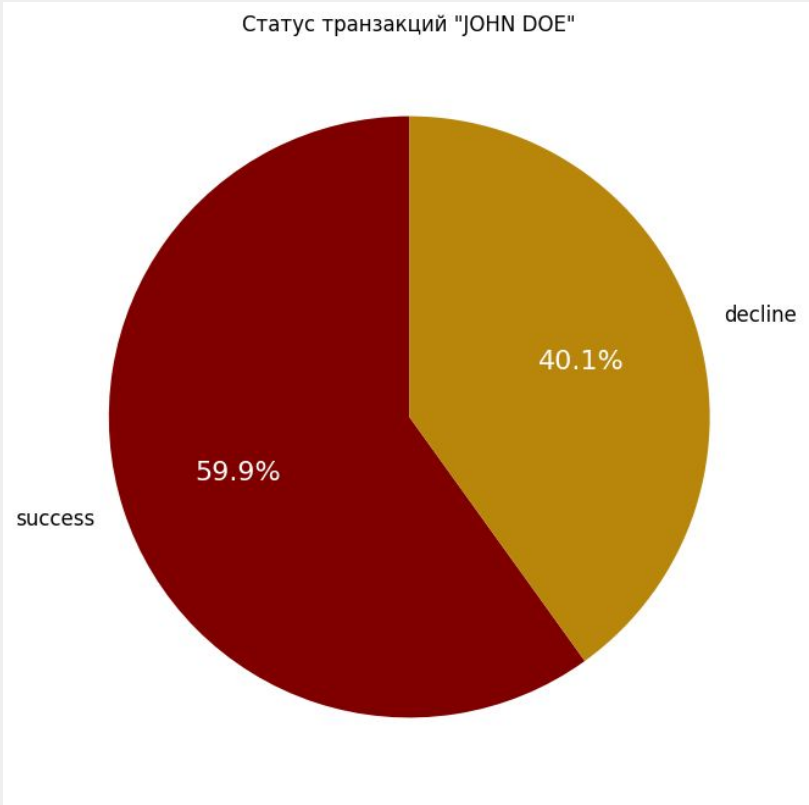
Количество ip адресов почти идентично количеству карт из определенной страны. Это может быть как ошибкой, так и попыткой обойти антифрод-систему – чтобы сгруппировать и идентифицировать фродовые транзакции было сложнее



Сценарий 2: Джон Доу

Данный сценарий можно также отнести к кардингу, но фродстер, в данном случае, имел явно более достоверные данные о платежных счетах пользователей (включая информацию о стране эмитента карт) так как большая часть платежей оказалась успешной на сумму €4517.96.

Также стоит отметить, что все транзакции проводились через платежного провайдера 1293, что важно в контексте следующего сценария и у одного мерчанта с id 212



Сценарий 2: Джон Доу

Митигация рисков:

1. Анализ вымышленных имен: идентификация и дополнительная проверка подозрительных имен держателей карт: могут совпадать с именами персонажей или в принципе не являться именами собственными, представлять набор символов
2. Выявление и блокировка транзакций на одно имя с разных аккаунтов за короткий промежуток времени (особенно если это новые аккаунты или на них не было ранее платежей)
3. Идентификация подозрительных шаблонов email, не содержащих личных данных (только в совокупности с другими факторами)
4. Пересмотр условий взаимодействия с платежными провайдерами, на долю которых приходится значительное количество фродовых транзакций, включая ужесточение требований к проверке операций и анализу рисков

Сценарий 3: Обман системы?

Связь аккаунтов: большое количество платежей через одного провайдера (в нашем случае 1293)

Особенности:

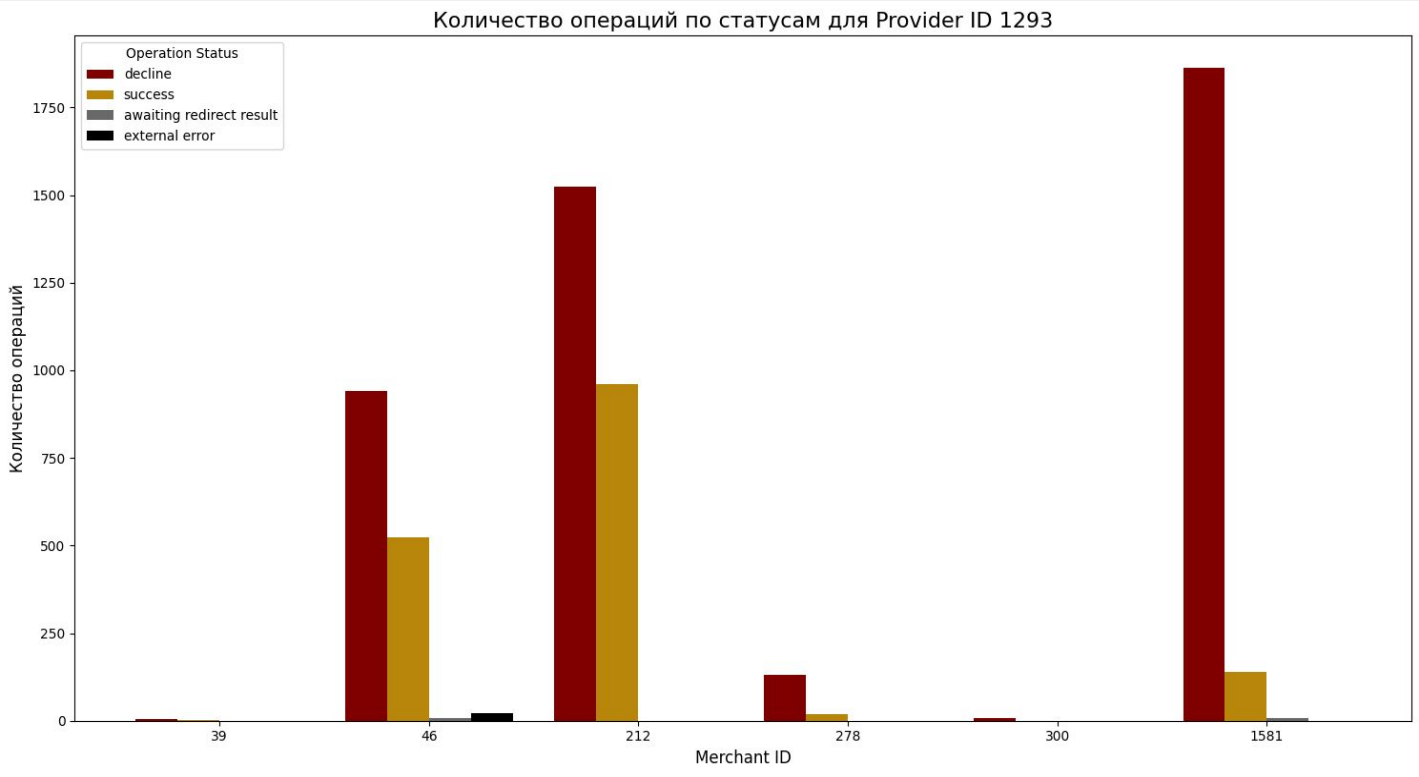
1. Большая часть транзакций отклонены
2. Покупки на близкие и не кратные 10 суммы
3. Платежи сильно разбросаны территориально

Сценарий 3: Обман системы?

На карте видно, что платежи совершаются из разных регионов, в основном регион совпадает с регионом эмитента карты, что на первый взгляд выглядит не подозрительно. Складывается впечатление, что это просто баг со стороны провайдера

Сценарий 3: Обман системы?

Однако, подозрение вызывает то, что подобный паттерн наблюдается только у одного мерчанта – 1581. У других мерчантов также много отклоненных операций, но разница в соотношении не такая огромная



Сценарий 3: Обман системы?

Сумма успешных транзакций - €8353.38, что очень много, если это действительно фрод

Данный сценарий может быть направлен:

1. На вызов бага на стороне платежной системы – большое количество транзакций в одно время
2. На создание проблем в работе, как провайдера, так и мерчанта

Сценарий 3: Обман системы?

Митигация рисков

В данном случае есть сомнения в том, что данные транзакции являются фродовыми, но, учитывая “репутацию” провайдера стоит быть внимательным и предпринять следующие шаги:

1. Связаться с провайдером и уточнить был ли сбой на его стороне, чтобы определить являются ли транзакции фродовыми
2. В случае отсутствия сбоя на стороне провайдера:
    a. Обсудить возможность ужесточения контроля со стороны провайдера или отказ от его услуг
    b. Выявление паттерна фродового сценария, а также использование машинного обучения для его дальнейшего предотвращения