Анализ проблем платежной системы/банка по представленному дата-сету  
  
*Выполнил: Горбунов Дмитрий Сергеевич*

Оглавление

[1. Основные характеристики 2](#_Toc204617330)

[2. Предположительный источник 4](#_Toc204617333)

[3. Ключевые находки разведочного анализа: 4](#_Toc204617334)

[4. Бэклог проблем 5](#_Toc204617335)

[5. Гипотезы возникновения проблем 5](#_Toc204617336)

[6. Гипотезы решений, стоимость реализации 5](#_Toc204617337)

[7. Приоритизация решений по RICE 5](#_Toc204617338)

[Заключение 6](#_Toc204617340)

### 1. Основные характеристики

**Размер и масштаб:**

* **7,483,766 транзакций** за 31 день (сентябрь-октябрь 2024)
* **4,869 уникальных клиентов**
* **5,000 уникальных карт**
* **12 стран** присутствия
* **11 валют** поддержки

**Основные поля:**

* transaction\_id - уникальный ID транзакции
* customer\_id - ID клиента
* card\_number - маскированный номер карты
* timestamp - дата и время транзакции
* amount - сумма транзакции
* currency - валюта (11 валют: USD, EUR, GBP, JPY, AUD, BRL, CAD, MXN, RUB, SGD, NGN)
* country / city - география транзакции
* is\_fraud - метка мошенничества

**Категории вендоров (равномерно распределены по 12.5%):**

* Healthcare (здравоохранение)
* Restaurant (рестораны)
* Entertainment (развлечения)
* Retail (розница)
* Travel (путешествия)
* Gas (топливо)
* Grocery (продукты)
* Education (образование)

**Типы карт:**

* Basic Debit (20.7%)
* Premium Debit (20.6%)
* Platinum Credit (20.5%)
* Gold Credit (19.3%)
* Basic Credit (18.9%)

**Каналы обслуживания:**

* Web (61.0%) - веб-платформа
* Mobile (30.3%) - мобильные приложения
* POS (8.7%) – терминалы

**Страны присутствия:**

* Европа: UK, Germany, France
* Америка: USA, Canada, Brazil, Mexico
* Азия: Japan, Singapore
* Африка: Nigeria
* Австралия: Australia
* Россия: Russia

### Безопасность и мошенничество

* **19.97% транзакций** помечены как мошеннические
* Высокий уровень мошенничества в развивающихся странах:
* Mexico: 38.03%
* Russia: 37.72%
* Brazil: 37.11%
* Nigeria: 35.14%
* Низкий уровень в развитых странах (6-7%)

### Финансовые характеристики

**Суммы транзакций:**

* Средняя сумма: 47,924.68
* Медианная сумма: 1,177.45
* Мошеннические транзакции в среднем в 4 раза дороже легитимных

**Активность за час:**

* В среднем 80 уникальных продавцов
* 409 транзакций
* Общая сумма: 19,917,188

### 

### 2. Предположительный источник

По характеру данных я делаю предположение, что этот датасет принадлежит **крупной международной финансовой компании**, скорее всего:

1. **Международный банк** с развитой платежной инфраструктурой
2. **Платежная система** типа Visa, Mastercard, PayPal
3. **Финтех-компания**, специализирующаяся на обработке платежей

### 3. Ключевые находки разведочного анализа:

1. **Географические паттерны:**

* Мошенничество в 5 раз выше в развивающихся странах (35-38%) vs развитых (6-7%)
* Кросс-граничные транзакции имеют 56.78% мошенничества vs 2.49% внутри страны
* Мексика, Россия, Бразилия, Нигерия - самые рискованные страны

1. **Временные паттерны:**

* Ночные часы (1-4 утра) имеют 59% мошенничества vs 20% днем
* Выявлены аномалии в данных (POS-транзакции и транзакции с присутствием карты показывают 100% мошенничества)

1. **Финансовые паттерны:**

* Мошеннические транзакции в 4 раза дороже легитимных
* Экстремальные суммы (>99%) имеют 82% мошенничества
* Travel и Retail - самые дорогие категории

1. **Поведенческие паттерны:**

* Высокая активность коррелирует с мошенничеством
* Уникальные страны за час - сильный индикатор риска

# 4. Бэклог проблем

* Высокий уровень мошенничества: 19,97% (1 494 719 транзакций), ущерб ~177,5 млн $. Превышение рыночных показателей в 60–200 раз.
* Географические проблемы: до 56,78% мошенничества в кросс-граничных транзакциях. Топ-страны: Мексика, Россия, Бразилия, Нигерия.
* Временные проблемы: 59% фрода ночью (1–4 утра). Аномалия: 100% мошенничества в POS-транзакциях.
* Финансовые проблемы: мошеннические транзакции в 4 раза дороже легитимных.
* Отсутствие современных инструментов защиты: нет 3D Secure, RBA, биометрии, SMS/E-mail верификации.
* Отсутствие воронки платежей: нет данных о попытках, статусах и метриках конверсии.

# 5. Гипотезы возникновения проблем

* Отсутствие 3D Secure 2.0 и RBA → устаревшая архитектура.
* Недостаточная географическая защита → единая стратегия для всех регионов.
* Нет усиленного мониторинга ночью → статические правила.
* Ошибки в мониторинге данных (POS = 100% фрод).
* Нет аналитики по воронке платежей – невозможно провести валидацию, какая доля и каких фродовых транзакций отбрасывается.

# 6. Гипотезы решений, стоимость реализации

* 3D Secure 2.0 — снижение фрода на 60–80%, срок 3–6 мес.
* RBA — снижение трения, срок 6–12 мес.
* Географическое профилирование — минус 40% ложноположительных, срок 2–4 мес.
* Ночной мониторинг — +25% детекции, срок 1–2 мес.
* Воронка платежей — +15% конверсии, срок 2–3 мес.
* SMS/E-mail верификация — минус 30–50% фрода, срок 1–3 мес.
* Биометрическая аутентификация — улучшение UX, срок 3–6 мес

# 7. Приоритизация решений по RICE

## 

# Заключение

Воронка платежей — приоритет №0.

В рамках кейса рассматривается только данные по проведенным платежам, мы не знаем, сколько транзакций не прошло – отсек антифрод, у пользователя возникли технические проблемы, и другим причинам. Для анализа эффективности необходимо смотреть не только на долю фродовых совершенных платежей, но и на эффективность систем безопасности (сколько фродовых платежей успешно не пропустили). С другой стороны – нам важно качественно детектировать фродовые и легитимные платежи, чтобы обеспечивать высокий уровень качества для легитимных пользователей, что напрямую влияет на эффективность нашей компании на рынке.

Рекомендуется начать именно с нее, а затем параллельно внедрять технические меры защиты.