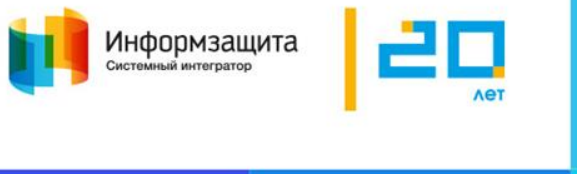


Карточный антифрод: слагаемые успеха

Гольдштейн Анна,
Директор по развитию бизнеса
ЗАО НИП «Информзащита»

Проблематика

Карточный бизнес и фрод: тренды

Год	млн. карт	оборот эмиссия трл.руб	оборот эквайринг в РФ, трл.руб	объем мошеннических операций, млрд. руб
2010	137	12.2	12.1	1.396
2011	162	16.2	16	2.368
2012	191	21.5	21.3	3.589
2013	217	26	25.9	4.58
2014	228	30.3	30.2	
2015 (01.10.2015)	240	23.6	23.6	

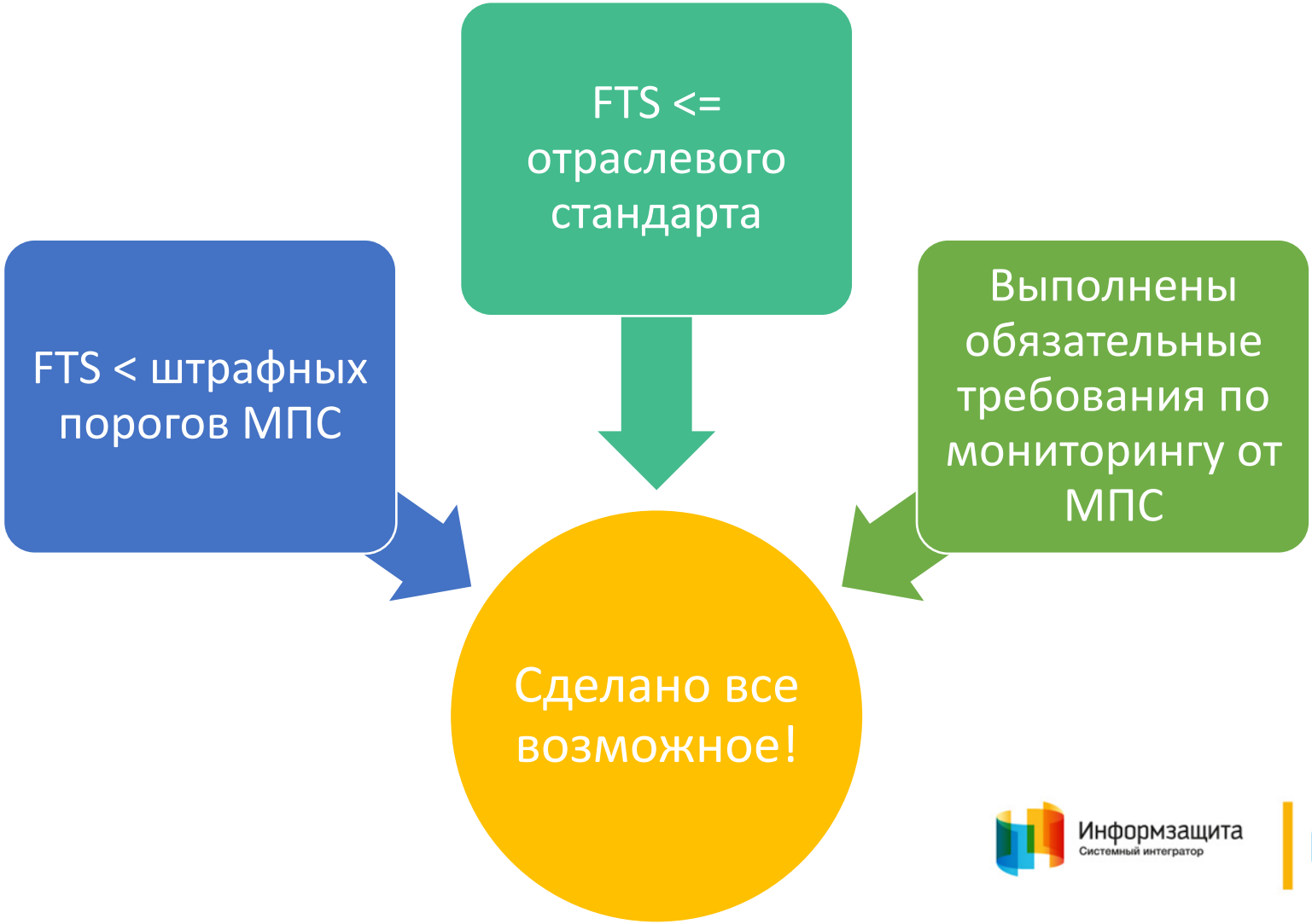
Прямые финансовые риски:

- Возмещение фрода клиентам (или страхование)
- Штрафные программы МПС

Информзащита
Системный интегратор

20 лет

Частые заблуждения



Информзащита
Системный интегратор
20 лет

Отраслевой FTS (fraud-to-sales)

	REGION BASIS POINTS	WORLDWIDE BASIS POINTS
2015Q1	6,42	9,04
2015Q2	5,94	8,97
2015Q3	6,71	9,27
2015	6,35	9

Basis points = FTS*10 000

- Общая статистика без разбивки по видам бизнеса
- Средневзвешенный -> отражает показатели малого числа игроков рынка

Эталон???

Информзащита
Системный интегратор

20 лет

Штрафные программы

- Программы
  - Visa Fraud Monitoring Program (VFMP) - контроль уровня мошенничества в ТСП (с 01/01/2016)
  - Visa Acquirer Monitoring Program (VAMP) -контроль уровня мошенничества в банке в целом
  - Mastercard Global Merchant Audit Program (GMAP) - контроль уровня мошенничества в ТСП
- Контролируемые параметры
  - Количество, сумма мошеннических операций
  - FTS (только международные операции)
- Финансовый ущерб от невыполнения
  - Mastercard – затраты на реализацию программы устранения
  - Visa – дополнительно прогрессивные штрафы за критичные нарушения

Обязательные требования по мониторингу. Эквайринг –оффлайн мониторинг

- Контролируемые параметры (для каждого ТСП)
  - количество предъявленных за неделю чеков операций;
  - общая расчетная сумма за неделю;
  - средняя сумма операции;
  - количество возвратов платежей по спорным операциям за неделю;
  - период между датой операции и датой расчетов.
- Алгоритм контроля – существенный рост относительно средне-недельных показателей
- Пороговые значения установлены МПС
- Глубина выборки для определения средних показателей - месяц

Информзащита
Системный интегратор
20 лет

Обязательные требования по мониторингу. Эквайринг – онлайн мониторинг

- Контролируемые параметры (для каждого ТСП)
  - количество, общая сумма транзакций
  - количество, общая сумма транзакций по одной карте
  - количество, общая сумма транзакций по картам одного эмитента
  - количество возвратов платежей;
  - количество, сумма по авторизационным запросам
  - множественные авторизационные запросы по одной карте
- Алгоритм контроля – отклонение относительно вычисляемых средних или установленных показателей
- Пороговые значения устанавливает эквайер
- Период вычисления среднего – день
- Глубина выборки для определения средних показателей – 3 месяца

Информзащита
Системный интегратор
20 лет

«Обязательный» мониторинг: результат

➢Хорошо детектируется:

- Массовый фрод, характеризующийся существенными отклонениями от статистических показателей
- Пример – «фейковые» ТСП

➢Плохо детектируется:

- Мошеннические операции, носящие единичный характер, и по характеристикам операции не сильно отличающейся от средних (например, от среднего чека)
- Пример – мошенничество в ТСП, торгующем сотовыми телефонами
- Не хватает: анализа принадлежности БИНа определенной стране или банку, частоты проведения операций, дней недели, времени суток и др.

Информзащита
Системный интегратор
20 лет

Что ЕЩЕ можно сделать?

Слагаемые успеха

Выявление фрода: повышаем эффективность правил

Расширение набора анализируемых данных:

- Анализ данных о клиентах, а не только об операциях (возраст, место прописки, дата регистрации в системе), данные с сервера ACS и т.п..
- Использование данных HLR

Учет результатов предыдущей обработки системы антифрод:

- Были ли алерты по клиенту/карте за последние N часов
- Результаты звонков этому клиенту
- Блокировалась ли карта

Информзащита
Системный интегратор
20 лет

Работаем над правилами: Кейс

- Мошенничество по картам иностранных эмитентов на заправке с хорошей проходимостью
- Мошенничество выявлено по результатам анализа отчетов МПС
- Стандартные правила мониторинга не работают (отклонение от среднего чека невелико, частота операций не превышает обычных средних по иностранным картам)

Информзащита
Системный интегратор

20 лет

Работаем над правилами: Аналитика

- Выявляем характерные признаки:
  - периодичность раз в 4 дня,
  - время суток -разное,
  - 80% операций - по картам одного и того же банка Южной Америки (банк А), остальные – по картам других банков континента

- Предположение:
  - сговор кассира с мошенниками,
  - операции во время смены одного и того же кассира

Информзащита
Системный интегратор

20 лет

Работаем над правилами: Настройка

- Занижаем/обнуляем пороги срабатываний для операций (частота операций и сумма) по иностранным картам в даты предполагаемых смен кассира – мошенника
- Занижаем/обнуляем пороги срабатываний для операций по картам банков северной и южной Америки в любые даты
- Включаем срабатывание на все операции по картам банка А в любые даты
- Включаем запросы эмитентам (security check)

Информзащита
Системный интегратор
20 лет

Обработка алертов: ничего нового

- Все процедуры, выполняемые операторами должны быть задокументированы.
- Инструкции должны быть понятными и прозрачными
- Максимальная автоматизация процесса
  - аналитика в правиле
  - автоматическая блокировка карт
  - действия оператора – простые функции (позвонить клиенту, подтвердить операцию, разблокировать карту и тп)

Информзащита
Системный интегратор
20 лет

Прочие меры реагирования

Меры реагирования на выявление фрода:

- остановка возмещения средств от Банка в пользу ТСП (эффективно при выявлении фейковых ТСП);
- блокировка терминалов;
- блокировка проведения операций по определённому БИНу или группе БИНов.

Ограничение активности терминалов по количеству операций в единицу времени (на определенный терминал или всю сеть):

- для терминала электронной коммерции - не более 3х операций/час по иностранным картам без поддержки 3d secure.
- для классического эквайринга: не более 2х операций по иностранным картам без ввода ПИНа (SBT – signature based transaction) в час.

Информзащита
Системный интегратор
20 лет

Анализ инцидентов

Источники – претензионная работа, результаты собственного мониторинга, отчеты ПС

Предмет анализа

- ✓Был ли фрод выявлен правилами?
- ✓Насколько эффективно (своевременно) был выявлен фрод?
- ✓Как отработаны процедуры обработки алертов ?
- ✓Есть ли связанные мошеннические операции, которые были пропущены?

Информзащита
Системный интегратор
20 лет

Идеальная модель - «зрелые» правила

- Рост процента выявляемого фрода
- Раннее выявление – включаем оперативное блокирование
- FTS: 0,0007->0,0002
- Минимизация ресурсов на мониторинг (= снижение затрат)

Информзащита
Системный интегратор
20 лет

Спасибо. Вопросы?

Гольдштейн Анна
goldanna@infosec.ru