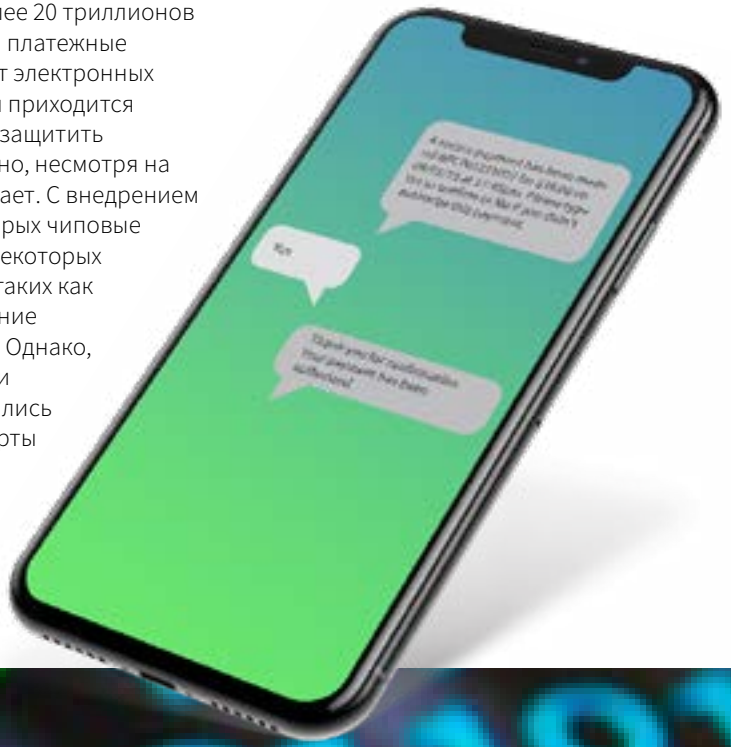
bpc
banking • payments • context

Решение Fraud Management

Мошенничество в открытом цифровом платежном пространстве

Начиная с 2014 года, держатели банковских карт ежегодно тратят с их помощью более 20 триллионов долларов. Потребителям нравятся платежные карты, и они все больше зависят от электронных платежей. В этих условиях отрасли приходится прилагать немалые усилия, чтобы защитить потребителей от мошенничества, но, несмотря на это, угроза мошенничества нарастает. С внедрением передовых технологий, среди которых чиповые карты стандарта EMV, статистика некоторых разновидностей мошенничества, таких как копирование данных и клонирование банковских карт, резко снизилась. Однако, это привело к тому, что мошенники сменили приоритеты и переключились на операции без предъявления карты (CNP).



Несмотря на внедрение стандарта EMV, в 2016 году убытки от мошенничества в сфере карточных платежей превысили 22 миллиарда долларов, а к 2020 году, по оценкам авторов доклада The Nilson Report, общемировой показатель потерь, вызванных этим явлением, перевалит за 35 миллиардов. Происходит «перетекание» мошенничества в среду CNP, причем страдают от этого в равной степени и физические, и юридические лица. Между тем мошенники все чаще обращают свои взоры на новые платежные технологии. Представители платежной индустрии тесно сотрудничают друг с другом, чтобы вместе противостоять мошенничеству. Но и мошенники действуют все более организованно – их приемы становятся более изощренными и целенаправленными. По мере усложнения платежной экосистемы у мошенников появляются дополнительные возможности для отработки новых мошеннических схем.

SMARTVISTA®

Banking Payments eCommerce

Мошенничество чревато не только финансовыми потерями. Оно влечет за собой значительный ущерб для репутации и как следствие отток клиентов. В результате финансовым учреждениям приходится стратегически инвестировать в средства противодействия мошенничествам. Современные надежные средства профилактики мошенничества играют важную роль в борьбе с этим явлением и помогают защитить потребителей. Поставщики платежных услуг должны прилагать усилия к уменьшению рисков, анализировать каждую транзакцию в реальном масштабе времени и осуществлять мониторинг мошенничества во всех каналах обслуживания. Несмотря на то, что каждому каналу присущи свои специфические риски, обусловленные его характеристиками, профилактика мошенничества по всем каналам дает свои плоды.

Не только финансовые потери

Не просто традиционный набор правил

Машинное обучение играет важнейшую роль во всех современных системах предотвращения мошенничества, таких как решение SmartVista “Fraud Management”. Эта технология обеспечивает скорость, эффективность и масштабируемость, которые необходимы для противодействия этому явлению в условиях повсеместного применения сетевых соединений и онлайновых сервисов. Машинное обучение дает возможность выявлять мошеннические транзакции и одновременно помогает уменьшить число ложноположительных результатов анализа. Машина умеет обрабатывать большие массивы данных гораздо лучше и быстрее, чем человек. Она способна выявлять и узнавать закономерности в поведении плательщиков намного тщательнее, чем это делают системы, действующие только на основе заложенных в них правил. За последние несколько лет вычислительные мощности компьютерной техники значительно выросли и сделались доступнее, а алгоритмы машинного обучения стали совершеннее. Как следствие улучшились показатели выявления мошенничества, а системы противодействия мошенничеству на основе искусственного интеллекта наконец стали отвечать требованиям производительности и масштабируемости. ИИ помогает не только уменьшить угрозу мошенничества, но и существенно снизить вероятность получения ложноположительных результатов, защищая клиентов от необоснованных отказов в обслуживании. В результате бороться с мошенничеством становится проще, одновременно уменьшается зависимость от специалистов в этой области. А у последних, в свою очередь, высвобождается время для того, чтобы заняться усовершенствованием своих процессов принятия решений и сокращением числа ошибок, обусловленных человеческим фактором, что также способствует повышению качества обслуживания клиентов.

Fraud Management

Решение SmartVista Fraud Management

Решение “Fraud Management” от компании БПЦ помогает эмитентам, эквайерам и другим пользователям в реальном времени выявлять и предотвращать мошенничество во всех каналах приема платежей.

Решение SmartVista “Fraud Management” предназначено для мониторинга транзакций в реальном масштабе времени и позволяет осуществлять статистический анализ на любом уровне, включая уровень карт, терминалов, ТСП и отдельных устройств. В состав его аналитического инструментария входит модуль анализа на основе бизнес-правил, который отличается высокой надежностью и дает возможность осуществлять скоринг транзакций, выявлять угрозы мошенничества и моделировать различные ситуации с использованием технологии машинного обучения. А информационная панель позволяет оператору в реальном времени получать основные статистические данные. При выявлении мошеннической транзакции оператор может воспользоваться инструментальными средствами реагирования на мошенничество. Кроме того, решение SmartVista “Fraud Management” позволяет генерировать сигналы тревоги и посылать их по разным каналам, включая SMS и электронную почту.

Эффективный и простой в использовании модуль обработки транзакций на основе правил

SB состав решения SmartVista “Fraud Management” входит эффективный модуль обработки транзакций на основе правил. Каждая транзакция проверяется на соответствие набору заданных пользователем критериев. Таким образом можно проверять сотни параметров, от простейших, таких как место осуществления транзакции, до более сложных, рассчитываемых на основе транзакционных данных карты за прошлые периоды. Правила могут устанавливаться на любом уровне: для отдельно взятых клиентов, клиентских сегментов, групп ТСП или групп банкоматов. По результатам каждой проверки рассчитывается значение, характеризующее степень рискованности транзакции. На основе этого значения принимается решение об осуществлении одного из следующих действий:

- Авторизация транзакции
- Постановка транзакции в очередь для дальнейшего расследования
- Оповещение эмитента, эквайера или держателя карты посредством электронной почты или SMS-сообщения
- Отклонение подозрительной транзакции
- Блокировка карты, счета, терминала или ТСП при выявлении подозрительного поведения.

Со временем правила оттачиваются, что способствует более эффективной профилактике мошенничества без увеличения числа ложноположительных результатов, которые препятствуют осуществлению добросовестных транзакций.

Оптимизированный процесс рассмотрения подозрительных случаев

В решении SmartVista “Fraud Management” автоматизированная обработка транзакций обеспечивается интеллектуальным модулем производственных процессов (Intelligent Workflow Engine), который закрепляет подозрительные транзакции за операторами на основе установленных приоритетов. При этом транзакции с высоким приоритетом помещаются в начало очереди для немедленного проведения расследования, а транзакции особо ценных клиентов – в отдельные очереди для обработки специально подготовленными операторами.

Система противодействия мошенничеству, ориентированная на будущее

По мере того, как платежная экосистема усложняется, а объемы данных растут, выявлять факты мошенничества становится труднее - поэтому развитие систем противодействия мошенничеству в направлении машинного обучения представляется вполне логичным. Скоринг рисков на основе статистического и машинного обучения помогает повысить пропускную способность и масштабируемость систем, работающих с большими массивами данных. Это не означает, что вмешательство человека перестает быть нужным – оно по-прежнему необходимо при проведении расследований и точечных проверок.

Решение SmartVista “Fraud Management” предусматривает применение машинного обучения для анализа платежных транзакций в режиме, близком к реальному времени. После того, как машина научилась распознавать подозрительные транзакции с использованием большого объема данных за прошлые периоды, ее можно применять для анализа платежей на основе разных критериев. Можно сравнивать поведение держателей карт с другими группами клиентов со схожими характеристиками и составлять профили действий, осуществляемых держателями карт. То же самое в полной мере относится и к ТСП. При прогнозировании мошенничества можно учитывать внешние факторы. Наконец, машинное обучение позволяет составлять профили поведения мошенников для предсказвания мошшеничеств в режиме, близком к реальному времени.

SmartVista “Fraud Management” – автоматическое генерирование правил для уменьшения статистики ложно-положительных результатов. Оно начинается с углубленного анализа данных за предшествующие периоды. Перед применением все автоматически сгенерированные правила проверяются. В результате пользователи платформы SmartVista получают в свое распоряжение действенные наборы правил мгновенно. По результатам применения автоматически сгенерированных правил, как и любых других правил, посылаются сигналы оповещения или открываются дела, подлежащие расследованию.

Полный контроль клиентом

Современный потребитель желает сам отвечать за себя и быть готовым к любой ситуации. Каким бы платежным инструментом он ни пользовался, будь то традиционная карта с магнитной полосой, карта стандарта EMV или альтернативное средство оплаты, такое как носимое устройство или «мобильный кошелек», потребитель неизменно хочет иметь возможность действовать на упреждение. Каналы доступа к сервисам SmartVista легко интегрируются с решением SmartVista “Fraud Management”, позволяя клиенту самостоятельно решать, когда, где и как использовать свои карты, чтобы это было сопряжено с минимальным риском.

Основные характеристики SmartVista “Fraud Management”

1. Современные механизмы выявления и предотвращения мошенничества, на основе данных из разных источников, включая карты SmartVista, данные ТСП и отчеты о фактах мошенничества
2. Выявление мошенничества в реальном времени, в режиме, близком к реальному времени, и в офлайн режиме
3. Эффективный модуль обработки транзакций на основе правил, использующий результаты проверки данных за прошлые периоды, матрицы, лимиты и статистику
4. Поддержка нескольких финансовых учреждений: каждая обслуживаемая организация может настраивать и применять собственные наборы правил обработки транзакций с признаками мошенничества
5. Противодействие мошенничеству во всех каналах доступа к услугам
6. Богатый инструментарий ведения дел о мошенничестве
7. Оповещение и отчетность по нескольким каналам
8. Поддержка нейронных технологий (опция)
9. Пропускная способность до 2000 транзакций в секунду

Преимущества – почему SmartVista?

Современное комплексное решение
В состав решения SmartVista “Fraud Management” входит современный модуль обработки транзакций на основе правил, который позволяет оперативно локализовывать подозрительные транзакции, защищая клиентов от действий мошенников. Решение использует данные разных типов, такие как данные о клиенте и его карте, данные ТСП, данные о возвратах платежей и данные отчетов о мошенничестве (включая данные MasterCard SAFE и Visa RIS).
Обеспечивая надежную защиту платежных транзакций и убеждая клиентов в их защищенности, решение SmartVista “Fraud Management” не только предотвращает убытки от мошенничества – оно также защищает будущие доходы, поступающие в виде комиссии и процентов. И при этом оно отличается простотой применения, интуитивной понятностью и адаптивностью.

Мониторинг всех транзакций и каналов обслуживания
Решение SmartVista “Fraud Management” обеспечивает мониторинг 100% транзакций во всех без исключения каналах обслуживания, включая банкоматы, POS-терминалы, киоски, систему IVR, центр обработки вызовов, каналы электронной коммерции. Данное решение может быть интегрировано с платежными системами сторонних разработчиков, функционировать в составе комплекса, включающего другие модули SmartVista, и применяться в сочетании с другими мерами предотвращения мошенничества и регулирования рисков.

Исключительная гибкость и адаптивность
Решение SmartVista “Fraud Management” позволяет быстро адаптироваться к ухищрениям мошенников, чтобы успешно противостоять их тактике.

Быстрое внедрение, быстрая отдача
Решение SmartVista “Fraud Management” может функционировать как автономный модуль или в составе более крупной системы, но в обоих случаях его развертывание не займет много времени и доходы на вложенные в него средства не заставят себя долго ждать.

Решение Fraud Management

Хотите узнать больше?

Если Вы хотите узнать подробнее о нашем решении - наши эксперты готовы помочь:
bpcbt.com/ru | info@bpcbt.com

bpc banking • payments • context

SMARTVISTA

Банки

Платежи

Электронная коммерция