

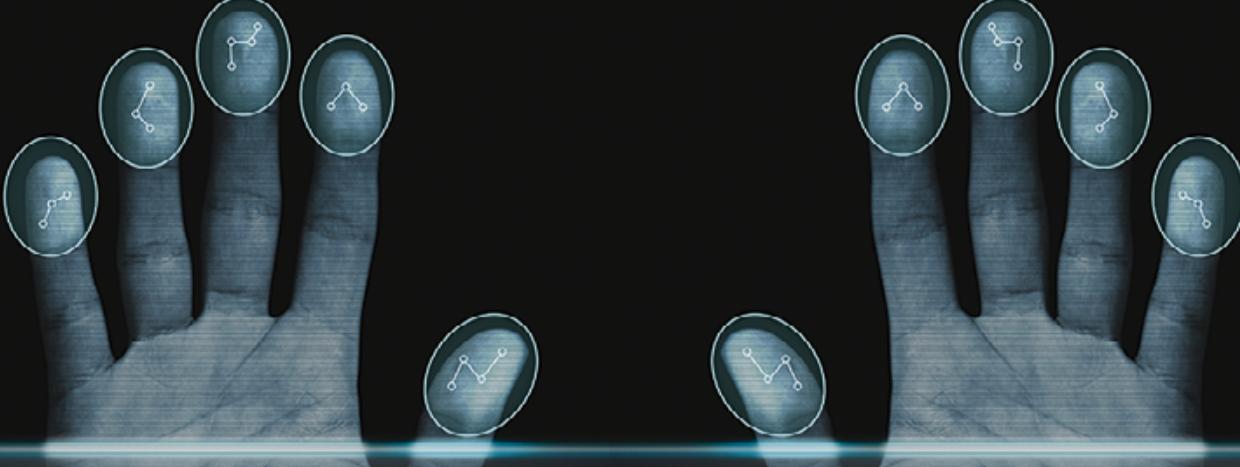


БЕЗОПАСНОСТЬ И ЗАЩИТА ПЛАТЕЖЕЙ: ПОДХОД MASTERCARD

Глобальный срез данных



Более 40 лет MasterCard лидирует в сфере безопасных платежей. Мы разрабатываем инновационные решения на основе данных и аналитических выводов, чтобы повысить безопасность и защищенность электронных платежей.



Наша гарантия безопасности и защиты платежей:

Мы заботимся о спокойствии потребителей, чтобы они платили с уверенностью; наша цель – построить мир без наличных, где каждый клиент, каждый платеж и каждое устройство надежно защищено.

Потребителям необходима простота и безопасность, независимо от того, в какой точке мира они находятся и как они платят – картой с магнитной полосой, с чипом или с технологией бесконтактных платежей. MasterCard постоянно совершенствует технологии по выявлению и предотвращению мошенничества, вкладывая в эту работу время и средства, чтобы держатели карт MasterCard были уверены в надежной защите их денежных средств.

В тех редких случаях, когда мошенничество¹ все же имело место, мы обеспечиваем уверенность держателей карт, ограничивая или вовсе устранивая их ответственность².

ОСНОВНЫЕ ПОЛОЖЕНИЯ

MasterCard – ведущая технологическая компания, работающая в индустрии электронных платежей, один из лидеров в сфере безопасности и защиты платежей.

- Технологии и средства оплаты меняются с каждым днем – платежи осуществляются быстрее, становятся все более интеллектуальными и сложными.
- Банковские карты по-прежнему являются одним из самых безопасных способов оплаты: из каждого \$100, потраченных по картам крупнейших глобальных платежных систем, лишь 6 центов теряются в результате мошенничества. Меры защиты и безопасности, осуществленные MasterCard, уже привели к снижению этих потерь до 5 центов.
- Мы вкладываем средства в развитие инновационных решений, направленных на защиту платежей, чтобы потребители могли рассчитыватьться легко, удобно и безопасно.

Защита и безопасность – наш главный приоритет. Интеллектуальные технологии MasterCard обеспечивают защиту и безопасность, помогая нам всегда быть на шаг впереди мошенников.

1. Мы защищаем клиентов от мошеннических действий еще до того, как они произойдут.
2. Универсального средства в борьбе с мошенниками не существует, но MasterCard внедрила несколько уровней защиты, чтобы существенно снизить угрозу мошенничества:

- Незаметные инструменты, применяемые по всей сети MasterCard, позволяют торгово-сервисным предприятиям и эмитентам выявлять и предотвращать мошенничество;
- Новые решения и продукты надежно защищают платежные операции, проводимые клиентами;
- Клиенты защищены гарантиями ограниченной/нулевой ответственности, причем в настоящее время компания предпринимает шаги по расширению такой защиты, сотрудничая с регулирующими органами, банками и торговыми компаниями на разных рынках;
- MasterCard возглавила инициативы по внедрению стандарта EMV (наиболее заметной отличительной чертой которого является встроенная микросхема) и технологии SecureCode, направленные на резкое сокращение случаев мошенничества;
- Наша сеть обрабатывает 1,8 млрд операций в месяц, чтобы помочь выявить и предотвратить мошеннические действия и другую подозрительную активность;
- Мы собираем данные, анализируем их и получаем ценные выводы, чтобы укрепить защиту всех устройств при оплате в любой точке мира;
- Мы тестируем инновационные решения для распознавания голоса, отпечатков пальца и черт лица, чтобы обеспечить надежную защиту платежей.

1. Важно учитывать, что мошенничество не является синонимом компрометации информации о расчетном счете (т. е. незащищенности данных перед посторонним воздействием). Благодаря разнообразным мерам безопасности, внедренным представителями отрасли и самой MasterCard, только малая доля случаев компрометации приводит к мошенничеству, особенно если для операции требуется аутентификация (т.е. подтверждение).

2. К примеру, все операции с картами в США защищены нашим обязательством нулевой ответственности, что устраняет финансовый риск клиента в случае мошенничества. MasterCard работает над тем, чтобы распространить такое обязательство и на другие рынки/регионы.

КЛЮЧЕВЫЕ ИДЕИ ПО ГРУППАМ СТЕЙКХОЛДЕРОВ

Наша главная идея звучит так: Мы стремимся построить мир без наличных, где каждый клиент, каждый платеж и каждое устройство надежно защищено.



МНОГОУРОВНЕВАЯ ЗАЩИТА MASTERCARD

С изменением и распространением способов оплаты и используемых устройств, меняются и разные аспекты нашей жизни, будь то покупки в розничных магазинах или онлайн с компьютера или мобильного устройства. MasterCard также преобразовала и адаптировала свои инициативы в сфере безопасности так, чтобы обеспечить защиту электронных платежей вне зависимости от времени и места оплаты.

Аутентификация имеет решающее значение для предотвращения мошенничества как в **физической** (Card Present, в присутствии карты), так и в **виртуальной** (Card Not Present, в отсутствие карты) среде.

Эта операция позволяет установить следующее:

1. Карта/платежное устройство является подлинным (проверка подлинности карты/устройства) и
2. Человек, который осуществляет транзакцию, – авторизованный пользователь (проверка подлинности держателя карты).

Несмотря на то, что средства для полного устранения мошенничества не существует, согласованное применение многоуровневого подхода представителями отрасли помогает существенно снизить эту угрозу. EMV, SecureCode+, сервис предоставления платежных реквизитов для мобильных устройств (MasterCard Digital Enablement Service, MDES), токенизация, а также принятие решений с учетом фактора риска – вот лишь несколько примеров инициатив, реализуемых MasterCard для борьбы с непреходящей угрозой мошенничества при платежах обоих типов, как Card Present, так и Card Not Present. MasterCard использует мощности своей сети таким образом, чтобы выявить случаи мошенничества, отслеживая операции по всему миру. EMS (Expert Monitoring Solutions, экспертные решения по мониторингу) и FRM (Fraud Rules Manager, система управления правилами выявления мошенничества) лежат в основе усилий MasterCard по предотвращению мошенничества. Они обеспечивают способность MasterCard обнаруживать подозрительную деятельность и операции, а также предоставлять эмитентам инструменты для укрепления их собственных систем защиты от мошенничества.



Мы обрабатываем более **1100 операций в секунду** – порядка 108 операций в мгновение ока.

Мы сканируем **1,8 млрд. операций в месяц** в режиме реального времени, чтобы помочь выявить и предотвратить мошеннические действия



мошенничеству. Оно позволяет свести к минимуму вероятность возврата платежей, одновременно защищая покупателей. Это решение использует сложные многоуровневые технологии, например, тщательно проработанные правила, базы данных общего пользования, идентификацию устройств и т. п., чтобы с высокой степенью точности установить уровень риска операции. По транзакциям с высоким уровнем риска автоматически происходит отказ, а операции с низким уровнем принимаются.

Небольшая доля операций, характер которых невозможно установить с высокой степенью точности, проходит проверку вручную посредством интуитивно понятного интерфейса, позволяющего провести дополнительный анализ для принятия окончательного решения. Решение настраивает команду профессионалов с обширными знаниями о тенденциях мошенничества в различных отраслях, обеспечивающая результаты самого высокого уровня.

MasterCard в сотрудничестве с Visa, American Express, JCB и China UnionPay разработала и внедрила [спецификацию EMV](#) для операций по банковским картам, оснащенным чипом. MasterCard выпустила платежные приложения M/Chip и M/Chip Advance, чтобы защитить свои платежи по всему миру. Встроенная в пластиковую карту микросхема, а также платежное приложение MasterCard существенно надежнее, чем карты с магнитной полосой. Введение EMV сократило количество случаев мошенничества с поддельными картами на 60-80%.



■ Потери от мошенничества (в млн канадских долларов, CAD) — Мошенничество, от трат

Источник: статистика Interac по дебетовым картам, январь 2014 года

В Канаде, где повсеместно используются системы самообслуживания на основе платежных карт с чипом и авторизацией ПИН-кодом (окхват более чем 90%), масштабы мошенничества за 4 года сократились на 73%: с 142 млн. долларов в 2009 г. до 39 млн. долларов в 2012 г. (2,06.п.от объема локальных операций по дебитным картам).

MasterCard постоянно продвигает повсеместный переход на EMV. Платежная система провела ряд инициатив в США для реализации к концу 2015 г. переноса ответственности в случае мошенничества – это последний крупный рынок, где пока не произошел переход на стандарт EMV.



СЕРВИС ПРЕДОСТАВЛЕНИЯ РЕКВИЗИТОВ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ (MASTERCARD DIGITAL ENABLEMENT SERVICE, MDES) К концу 2014 г. MasterCard представит новую безопасную платформу для осуществления как Card Present, так и Card Not Present платежей мобильными устройствами. MDES заменяет настоящий номер карты на другую комбинацию цифр, токен. В момент покупки MasterCard соотносит токен с подлинным номером счета, чтобы эмитент мог правильно обработать операцию. При компрометации злоумышленники не смогут воспользоваться токеном. Еще одно преимущество платформы состоит в том, что торговое предприятие получает только токен и никогда – реальные платежные реквизиты, что обеспечивает дополнительную защиту платежей.



В 2013 г. MasterCard запустила SECURECODE+, последнюю модификацию технологии SecureCode, позволяющую торговым компаниям добавить к защите онлайн-транзакций еще один уровень безопасности, который предполагает введение одноразового пароля. Пароль SecureCode+ известен только владельцу счета, а торговые предприятия могут выбрать, для каких именно операций он потребуется. Они не обязаны использовать SecureCode+, если операция надежная – таким образом можно регулировать необходимость в авторизации в зависимости от того, насколько необходима дополнительная проверка.

SecureCode+ также позволяет реализовать перенос ответственности с магазинов на банки-эмитенты: чем больше усилий они прилагают, защищая потребителя дополнительными способами подтверждения оплаты, тем больше преимуществ получают.

В 2013 г. SecureCode была использована для осуществления более 1,4 млрд. операций по всему миру – на 28% больше, чем в 2012 г. В долларовом выражении SecureCode обеспечил безопасность порядка 29% всех онлайн-платежей по всему миру.

ПРИНЯТИЕ РЕШЕНИЙ С УЧЕТОМ РИСКА – это третий уровень защиты Card Not Present транзакций. Он будет использовать адрес электронной почты клиента, информацию об устройстве и номер счета для создания уникального «онлайн-профиля». Мы можем авторизовать операции на основе таких «следов» пользователей в сети, не требуя дополнительных усилий с их стороны. Со временем профилю будет присвоен рейтинг надежности, учитывая который торговые предприятия и эмитенты смогут подтверждать платежи.

К примеру, постоянные клиенты с высоким рейтингом могут произвести оплату, минуя процесс аутентификации – в результате процесс займет меньше времени, а клиент с меньшей вероятностью откажется от покупки и скорее останется довольным.

НАШ ОСНОВНОЙ ПРИОРИТЕТ – ЗАЩИТА И БЕЗОПАСНОСТЬ ПОТРЕБИТЕЛЕЙ

В случае мошенничества мы обеспечиваем частичную или полную защиту потребителя от материальной ответственности или потерь. Ответственность клиента обычно устанавливается местными регуляторами, и MasterCard сотрудничает с государственными органами по всему миру, чтобы обеспечить внедрение передовых принципов работы для защиты потребителей. Правила установления ответственности торговых точек и эмитентов в случае мошенничества сложны и многообразны, но они направлены на то, чтобы в большей степени освободить от риска сторону, которая приложит максимальные усилия для защиты транзакции.

ЗАЩИТА КЛИЕНТОВ ОТ МОШЕННИЧЕСТВА ПО-ПРЕЖНЕМУ ВАЖНЕЕ ВСЕГО

Мы задействуем свой бренд, репутацию и возможности, чтобы оградить клиентов от мошенничества. Благодаря усилиям MasterCard ответственность держателей карт по всему миру уже была успешно снижена, а в США нам удалось гарантировать нулевую ответственность. В наших планах – реализация этой политики для держателей карт MasterCard по всему миру и продолжение сотрудничества с местными регулирующими органами, банками и торговыми предприятиями для защиты клиентов.

ПРИЛОЖЕНИЕ

МОШЕННИЧЕСТВО: КРАТКАЯ СПРАВКА

Мошенничество – это материальные убытки, связанные с неправомерным использованием счета для покупки товаров, перевода средств, снятия наличных или получения иной финансовой выгоды.

Для потребителей защита и безопасность платежей на первом месте как с бытовой, так и с психологической точки зрения. Широкое распространение и популярность банковских карт обусловлены в том числе способностью отвечать этим требованиям.

В 2012 г. было подсчитано, что на мошеннические действия пришлось лишь 66 п. потраченных по платежным картам средств, причем показатели MasterCard, лидера с точки зрения безопасности, составили всего 56 п. (п.).

ЦЕНА МОШЕННИЧЕСТВА

- ▶ На США приходится **45%** случаев мошенничества в мире, но всего **24%** расходов
- ▶ На Card Not Present платежи приходится **45%** случаев мошенничества в мире, но всего **8%** расходов
- ▶ Мошенничество с Card Not Present платежами происходит в **3** раза чаще, чем с Card Present транзакциями, несмотря на то, что их отклоняют в **6** раз чаще



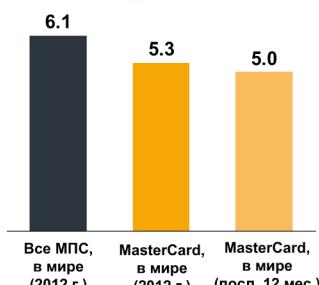
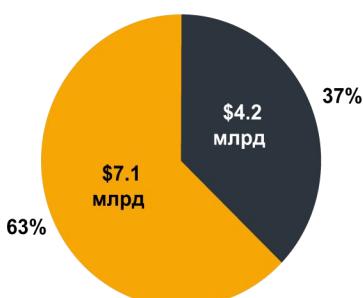
Источник: Данные MasterCard, 2013 г.

Потери от мошенничества в глобальной платежной индустрии в 2012 г. составили более 11 млрд долларов США.

Несмотря на то, что на США приходится менее четверти (24%) от мирового объема платежей, эта страна несет почти половину (47%) от всех убытков в результате мошенничества, теряя 5,3 млрд долларов от действий злоумышленников. Особенно сложную проблему представляет собой быстро развивающаяся сфера онлайн-торговли. Несмотря на то, что Card Not Present (CNP) платежи проверяются и отклоняются почти в 6 раз чаще, чем Card Present (CP) транзакции, мошенничество с ними происходит в 3 раза чаще.

Убыток от мошенничества в мире в 2012 г. 11.3 млрд долл. США

- Потери эмитентов от мошенничества
- Потери торговых точек от мошенничества



В 2012 г. объем мошеннической деятельности по платежкам MasterCard был на 14% меньше общемирового уровня

В последние 12 месяцев этот показатель оказался еще ниже

Источник: Отчет The Nilson Report за 2013 г., данные MasterCard; показатели за последние 12 месяцев представлены до 3 кв. 2013 г. Показатели по всем картам (мировым) включают MasterCard, Visa, American Express, China Union Pay, Diners Club и JCB.

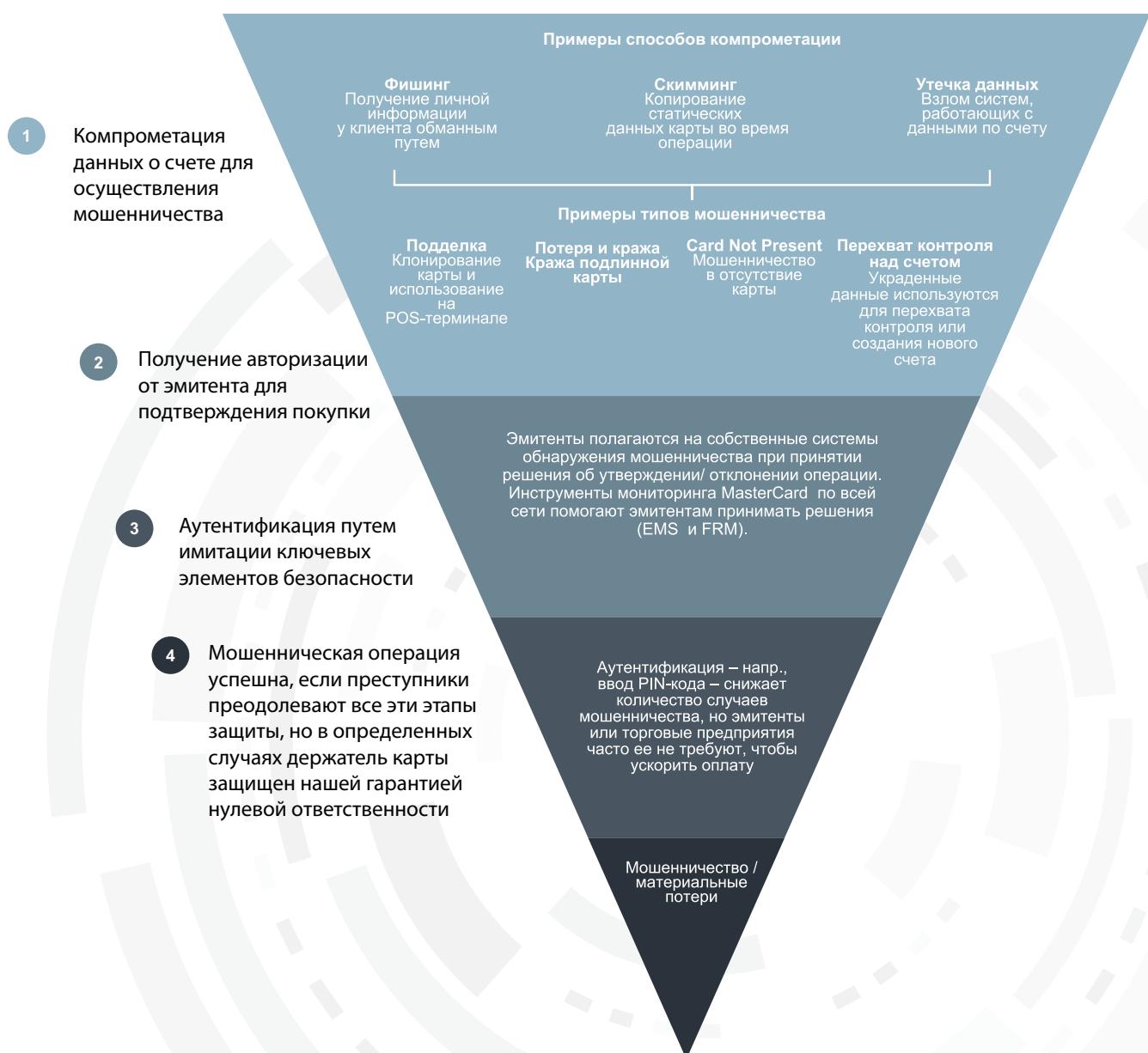
Когда возможно мошенничество:

1. Платежные реквизиты утеряны, украдены или скомпрометированы и
2. Эмитент одобрил операцию.
3. В ряде случаев от преступника потребуется подтвердить платеж (т.е. доказать, что он является законным держателем карты).

Иными словами, при попытке совершить мошенническую операцию преступник должен сначала узнать платежные реквизиты, а затем повести себя похоже на законного пользователя.

Этапы авторизации и аутентификации уникальны для каждой карты; поэтому, **только малая доля случаев компрометации платежных реквизитов ведет к мошенничеству**

СХЕМА: МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ



МЕРЫ ПО ЗАЩИТЕ ОТ МОШЕННИЧЕСТВА: ДВА ПРИМЕРА

Чтобы проиллюстрировать описанные выше тезисы, мы представляем для примера из практики: (1) фишинг-атака для обнаружения данных и последующей оплаты в интернете, и (2) кража данных из платежной системы с целью продажи информации по счету и создания поддельных карт.

ПРИМЕР №1: КОМПРОМЕТАЦИЯ ПУТЕМ ФИШИНГА; ЗАЩИТА CARD NOT PRESENT ПЛАТЕЖЕЙ



Потребители получают электронную рассылку, предположительно из надежного источника (например, от друга, надежной компании и т. п.), в которой клиента просят перейти по ссылке.



В результате перехода по ссылке на компьютере устанавливается вредоносное ПО, или при помощи социальной инженерии клиента обманнным путем вынуждают раскрыть данные о карточном счете.



Информация используется для онлайн-покупок или клонирования карт. Однако благодаря SecureCode+ счета защищены надежным паролем клиента.

Хотя фишинг несложен в техническом плане, от него трудно защититься, поскольку часто сам клиент раскрывает информацию о счете. Тем не менее, такие инновации, как SecureCode+, существенно затрудняют деятельность мошенников.

НАГЛЯДНЫЙ ПРИМЕР

Компрометация учетной записи администратора

Установка вредоносного ПО на платежных терминалах

Получение данных о карточном счете

Неправомерное использование данных

Действия злоумышленников

- Получение преступниками доступа к технологическим системам торговой точки с помощью скомпрометированной учетной записи администратора (напр., полученной переборным методом, фишингом и т. п.)
- Установка вредоносного ПО в системе, к которой подключен POS-терминал, для сбора данных о картах; при считывании карта обменивается данными с терминалом
- Однако данные хранятся или передаются в системе в виде обычного текста, и в некоторых случаях шифруются слишком поздно
- Теперь данные уязвимы для перехвата вредоносным ПО
- Платежные реквизиты продаются на черном рынке в сети или напрямую используются для мошеннических покупок

Защита от мошенничества

- Терминалы считывают только те данные, которые необходимы для обработки операции, напр., без CVC2 мошенничество в интернете (CNP) затрудняется
- Эмитенты, эквайеры и торговые предприятия могут отслеживать подозрительную деятельность
- MasterCard может информировать эмитентов о случаях компрометации; эмитенты могут принять решение о закрытии счетов и повторном выпуске карты, или о наблюдении за счетом
- В случае мошенничества клиенты полностью или частично защищены, в зависимости от местного законодательства
- Если в карте использован стандарт EMV, клонирование микросхемы очень сложно выполнить, а использование в ней динамической защиты сделает повторное проведение операций практически невозможным

Атаки, направленные на технологические системы ритейлеров, могут привести к компрометации миллионов счетов, средства защиты, используемые MasterCard и другими представителями индустрии, могут пресечь до 90% попыток мошенничества, а уровень материальных потерь будет еще ниже. Микросхема EMV и ее динамические свойства дополнительно затрудняют процесс клонирования карт для мошенников. Кроме этого, использование таких новых разработок, как MDES и токенизация, лишает такие атаки смысла, обеспечивая дополнительную защиту потребителей и торговых предприятий от мошенников.

Несмотря на то, что прямые убытки от мошенничества относительно низки, на деле последствия компрометации данных значительны. Среди них – потеря уверенности в платежной экосистеме, снижение продаж в сфере розничной торговли, негативное влияние на бренд и репутацию и т. д. Хотя масштабные случаи мошенничества встречаются редко, одно такое событие может привести к убытку розничного продавца на сумму до 100 млн долл. США, не говоря уже о других негативных последствиях, например, падении рыночной капитализации / котировок акций.