Мошенничество в сфере платежных инструментов и сервисов в 2025 году: общая статистика и тенденции

Банковский
Процессинговый
Центр

Содержание:

Отчет подготовлен ОАО «Банковский процессинговый центр» на основании имеющейся информации по операциям с банковскими платежными карточками. Данные не охватывают всю территорию Республики Беларусь, однако, учитывая долю рынка ОАО «Банковский процессинговый центр», могут свидетельствовать об основных тенденциях в Республике Беларусь. **При сравнении данных в абсолютных значениях используются значения в условных единицах.**

Общая информация:

В 2025 году основная доля мошенничества в Республике Беларусь приходилась на мошенничество с банковскими платежными карточками в среде без физического присутствия карточки при проведении операции. Случаев установки скимминговых устройств и массовой компрометации данных держателей карточек на территории Республики Беларусь в 2025 году зафиксировано не было.

Эмиссия (данные по операциям с банковскими платежными карточками, выпущенными банками, которые обслуживаются в ОАО «Банковский процессинговый центр»):

Характерными тенденциями 2025 года являются мошенничество без присутствия карточки, социальная инженерия, а также единичные случаи мошенничества по поддельным и утерянным/украденным карточкам. Главным трендом мошенничества с банковскими платежными карточками в 2025 году стала социальная инженерия — 63% случаев связано с ее различными инструментами. Значительная доля мошенничества с применением социальной инженерии свидетельствует о том, что данный вид мошенничества приносит быстрый доход злоумышленникам при минимальных финансовых затратах.

В рамках методов мошенничества, связанных с социальной инженерией, мошенники, представляясь сотрудниками банков, правоохранительных органов, государственных структур или служб технической поддержки, выходили на связь с держателями преимущественно по телефону или через мессенджеры. Их целью являлось получение личных данных держателей карточек, доступов к счетам, системам дистанционного банковского обслуживания, МСИ и мобильным устройствам. Завладев этой информацией, злоумышленники совершали несанкционированное списание денежных средств.

По-прежнему наблюдались инциденты, при которых использовались предлоги «спасения» или «легализации» денег, вынуждающие жертв к крайним мерам: оформлению кредитов, продаже недвижимости или изъятию всех накоплений с последующей передачей наличных денежных средств курьеру либо переводом через платежный терминал. После того как потерпевший, следуя указаниям, лишался всех средств, мошенники прекращали любое взаимодействие.

Появилась новая мошенническая схема, известная как «NFC Gate», которая позволила преступникам дистанционно снимать наличные в банкоматах, а также осуществлять оплаты в торгово-сервисных предприятиях. Ее основой целью является установка на телефон жертвы приложения для удаленного доступа (например, злоумышленник представляется службой технической поддержки). Далее под различными предлогами мошенник убеждает пользователя приложить свою карточку к NFC-модулю смартфона и ввести PIN-код. В этот момент данные карточки считываются и ретранслируются на устройство злоумышленника. Последний использует свой смартфон с полученными данными и осуществляет несанкционированное снятие денежных средств в банкомате или совершает оплату покупок в торгово-сервисных предприятиях.

Активно использовались схемы мошенничества с токенизацией скомпрометированных карточек.Посредством методов социальной инженерии злоумышленники получают доступ к данным карточки держателя и привязывают ее к собственному мобильному устройству. Это позволяет беспрепятственно совершать мошеннические платежи в сети Интернет, в торгово-сервисных предприятиях, а также снимать наличные в банкоматах как в Беларуси, так и за рубежом.

Схема мошенничества, основанная на перенаправлении на фишинговые сайты-двойники, продолжает оставаться актуальной в рамках социальной инженерии. Создав точный аналог интернет-банкинга финансового института, сайта компании, мошенники обманным путем получают доступ к конфиденциальной информации: данным для входа или платежным реквизитам. Введенные пользователем на поддельной странице сведения попадают к злоумышленникам, что позволяет им незамедлительно воспользоваться денежными средствами.

Атаки методом подбора номеров банковских платежных карточек, включая атаки на банковские идентификаторы (BIN), представляют собой одну из ключевых угроз для электронной коммерции. Суть метода заключается в массовой автоматической проверке валидности сгенерированных комбинаций путем проведения небольших тестовых транзакций. Данные атаки нацелены преимущественно на интернет-магазины с недостаточно надежными системами валидации платежей и противодействия мошенничеству.

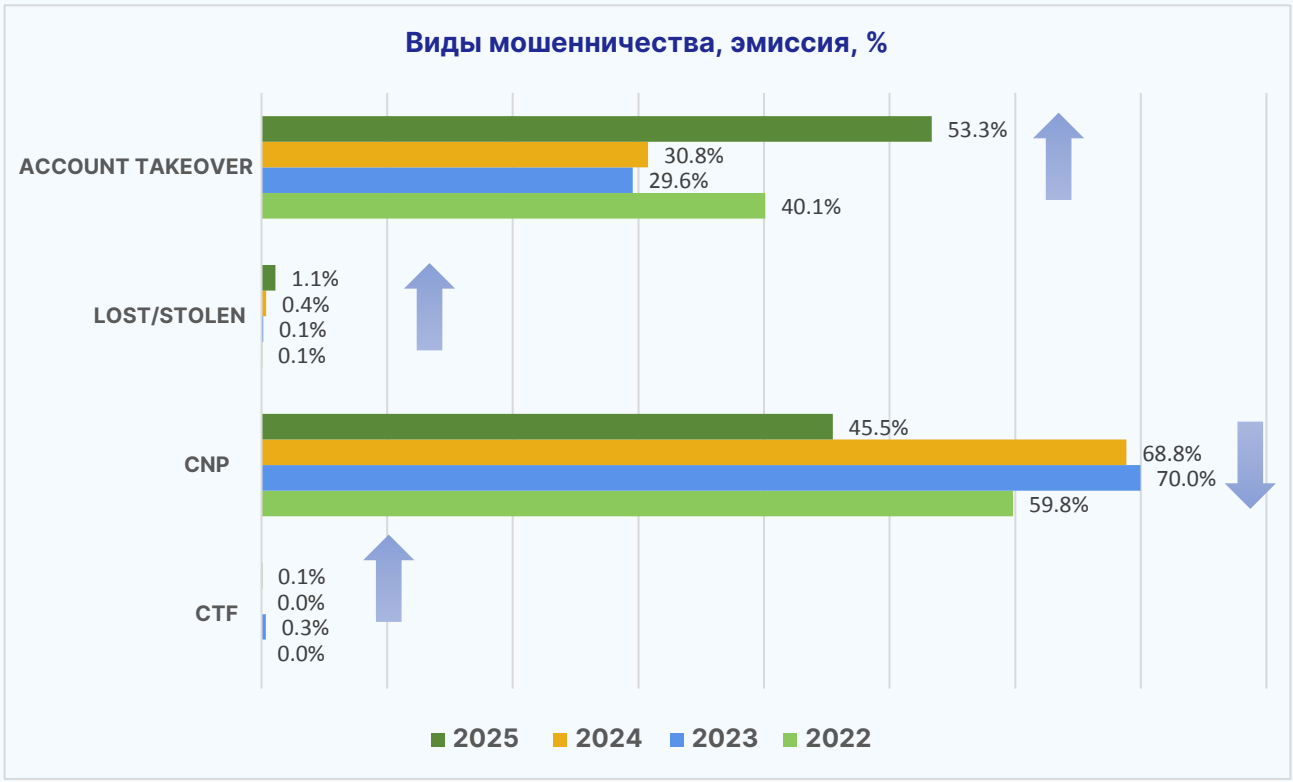
Финансовое мошенничество под видом инвестиций остается актуальной угрозой. Злоумышленники, представляясь брокерами, активно предлагают гражданам в сети Интернет «высокодоходные» вложения с гарантией быстрой прибыли. После перевода средств на открытый под предлогом инвестирования счет доступ к нему блокируется, а контакты мошенников становятся недоступными, в результате чего пострадавшие теряют все вложенные средства.

Мошенничество в сфере онлайн-знакомств – метод основан на построении эмоциональной связи: злоумышленники целенаправленно формируют доверительные отношения с жертвой, используя манипуляции и знаки внимания. Конечной целью таких действий является либо хищение денежных средств под различными предлогами, либо получение конфиденциальной информации для кражи личных данных и последующих мошеннических операций.

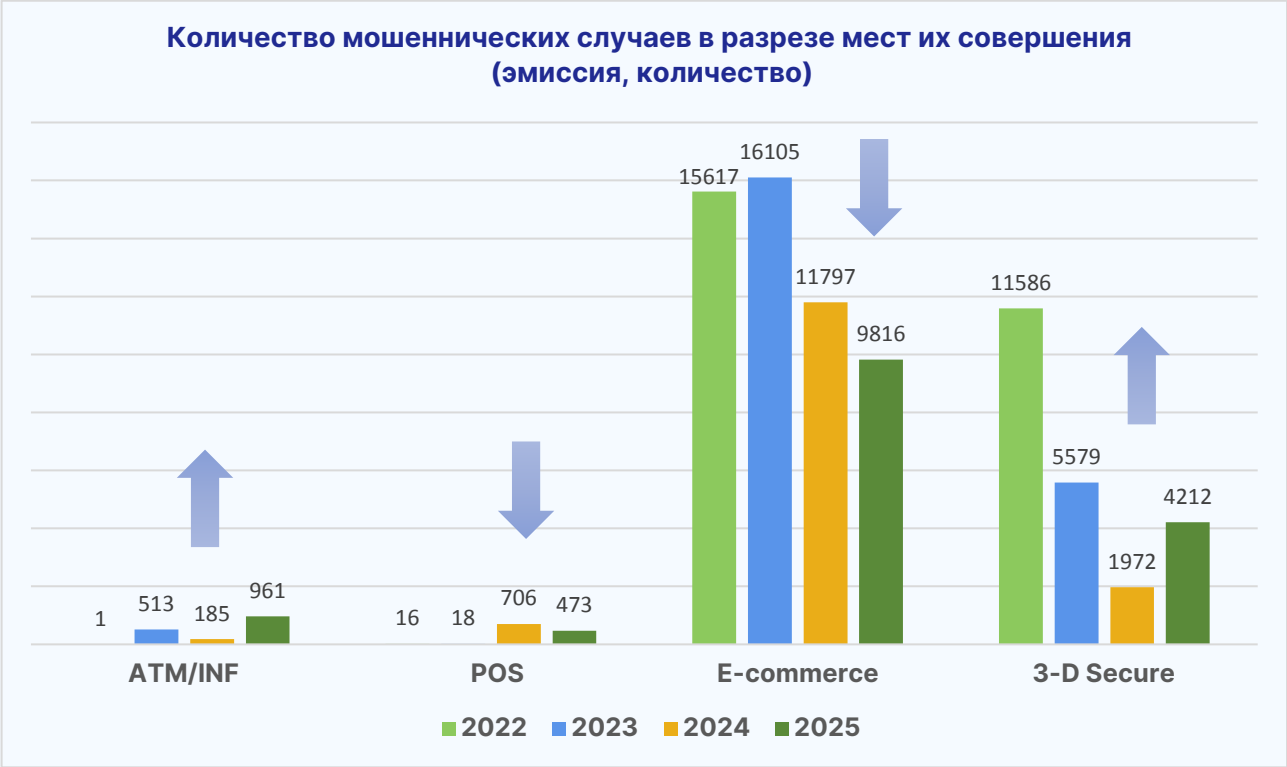
В последнее время отмечена активизация мошенничества на рынке Бразилии с использованием метода манипуляции платежными данными. Согласно данным от международных платежных систем, атака является характерной для данного региона. Суть схемы заключается в технической подмене данных при проведении операции. Это позволяет мошенникам искусственно изменить способ обработки транзакции. Таким образом, атака обходит стандартные средства защиты, связанные с проверкой типа используемой технологии. Хотя подобный метод не является абсолютно новым, в текущий момент он демонстрирует значительный рост.

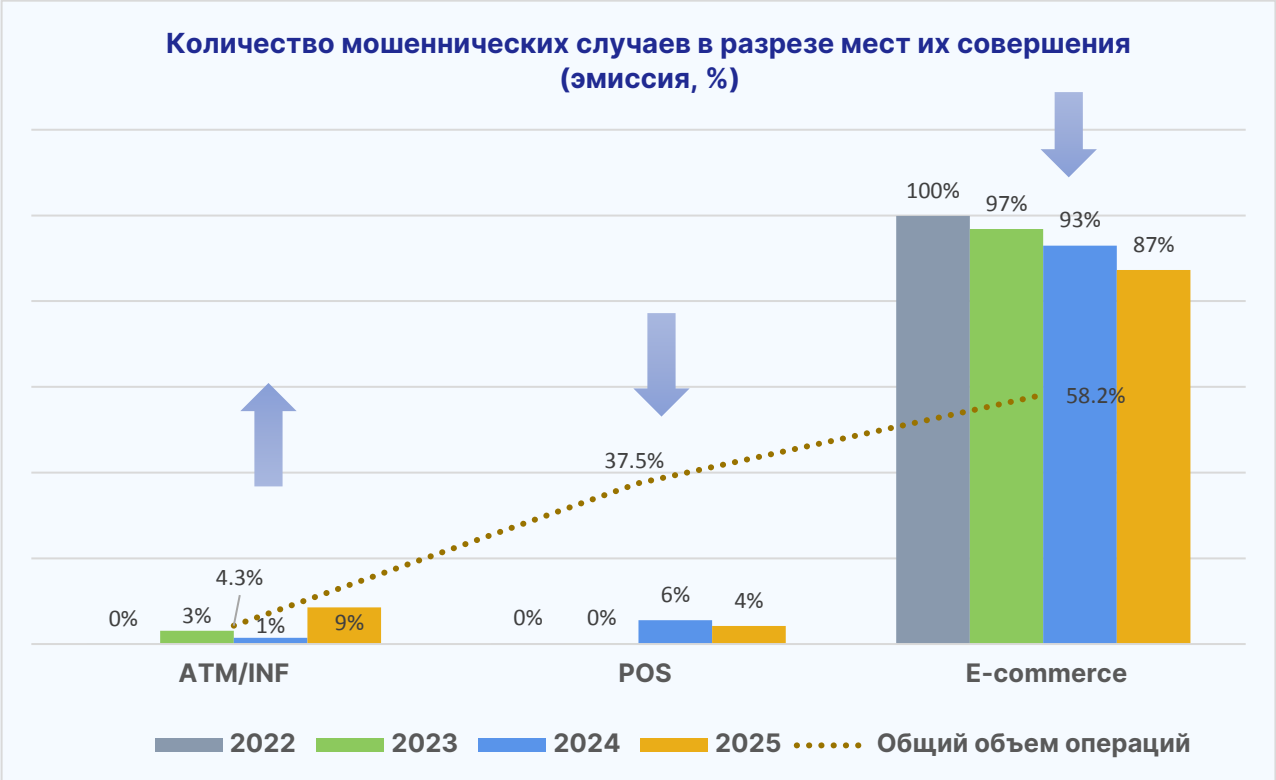
По итогам 2025 года количество успешных мошеннических операций по карточкам банков, которые обслуживаются в ОАО «Банковский процессинговый центр», по типу мошенничества распределилось следующим образом: **53,3%** незаконных операций с банковскими платежными карточками приходится на **account takeover (перехват счета), 45,5%** мошеннических операций приходится на мошенничество **с использованием реквизитов карточек**, **1,1%** приходится на операции по **утерянным/украденным карточкам**, на успешные мошеннические операции по **поддельным карточкам – 0,1%.**

По итогам 2025 года на 27% увеличилось общее количество успешных мошеннических операций, заявленных в платежные системы, общая сумма успешных мошеннических операций увеличилась на 496%, а средняя сумма 1 мошеннической операции составила 385 долларов США (82 доллара США в 2024 году). Увеличение в 2025 году количества и суммы успешных мошеннических операций, заявленных в международные платежные системы, обусловлено ростом доли мошенничества с использованием средств социальной инженерии и появлением таких новых схем, как NFC Gate, токенизированные мошеннические операции. При использовании данных методов мошенничества средняя сумма мошеннической операции также значительно выше, чем средняя сумма операции в электронной коммерции.

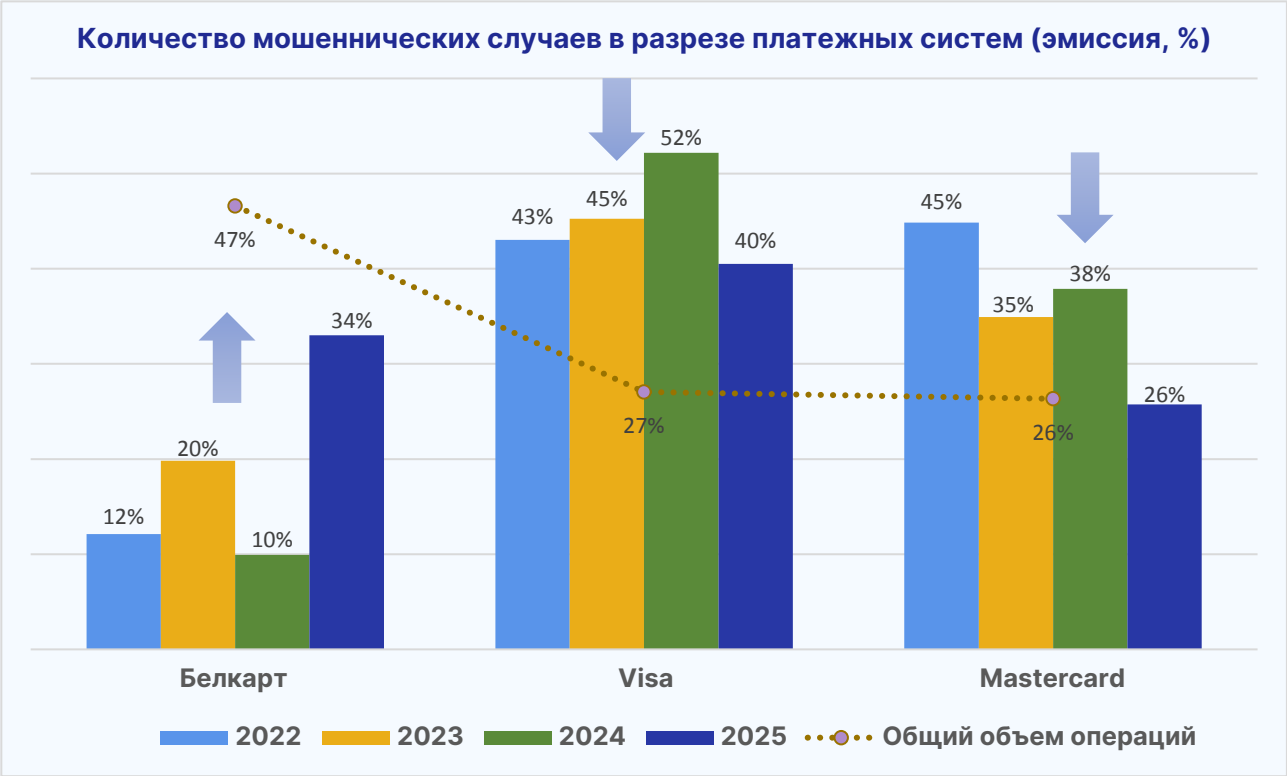


В 2025 по количеству мошеннических случаев в разрезе мест их совершения 87% мошеннических случаев приходится на среду без присутствия карточки, в АТМ прошло 9% случаев мошенничества, из которых 99% связаны с социальной инженерией (снятие наличных по NFC Gate и по токенизированным карточкам, а также переводы денежных средств злоумышленникам посредством инфокиосков), случаи с поддельными карточками составили только 1%. При этом в 2025 году количество мошеннических случаев в ОТС составило 4% случаев. Данная тенденция в отчетном периоде свидетельствует о росте интереса злоумышленников в получении наличных денежных средств, использование которых сложно отследить.





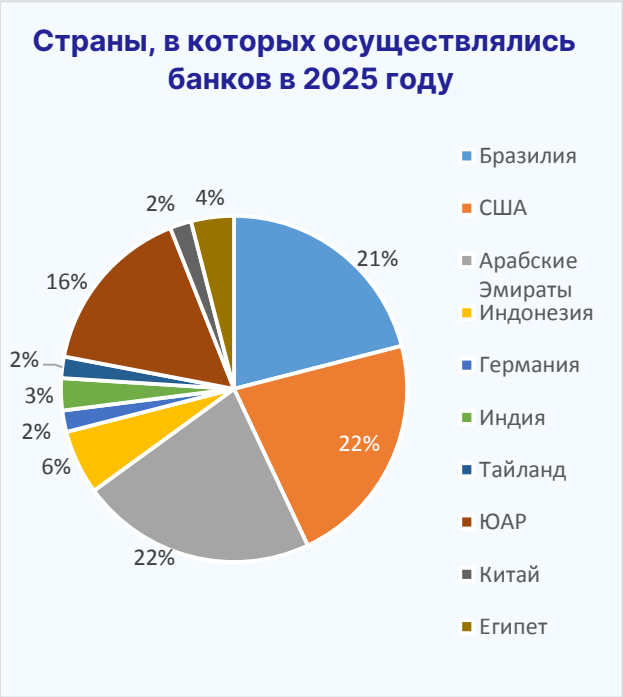
В связи с широким распространением в 2025 году схем мошенничества с использованием социальной инженерии, манипуляцией данными при помощи технологии «NFC Gate», а также с токенизацией карточек, до 33% увеличилась доля мошенничества по карточкам платежной системы Белкарт (в 2024 году – 10%), на МПС Visa пришлось 41% случаев, на МПС Mastercard – 26%. По карточкам платежной системы Белкарт преимущественно проходили несанкционированные снятия денежных средств в банкоматах на территории Республики Беларусь и в Российской Федерации.



Операции по поддельным карточкам:

В 2025 году количество мошеннических случаев с использованием поддельных карточек увеличилось в 1,2 раза относительно 2024 года, было выявлено 33 неуспешных случая проведения мошеннических операций с использованием поддельных карточек в организациях торговли и сервиса в таких странах, как Бразилия, ЮАР, Арабские Эмираты, США, Индонезия, Китай и Таиланд. Успешные случаи проведения мошенниками операций с использованием поддельных карточек были зафиксированы в розничном магазине и на паркинге на территории США, в ресторане на территории Германии и в магазине, реализующем товары недлительного пользования, на территории Бразилии. При этом, в 2024 году по поддельным карточкам были выявлены случаи неуспешных попыток оплаты в организациях торговли и сервиса на территории Японии, Венгрии, США и Китая, а также случаи сгенерированных операций в организациях торговли и сервиса Бразилии и Мексики.

В 2025 году было зафиксировано 2 случая неуспешного использования поддельных карточек в АТМ на территории Индии и Египта. В 2024 году мошенники проводили операции по поддельным карточкам в АТМ на территории Бразилии, Вьетнама, Филиппин и Египта.



Мошеннические операции с использованием реквизитов карточек:

Основными тенденциями мошенничества с использованием реквизитов карточек в 2025 году являются:

- рост мошеннических операций, основанных на методах социальной инженерии. В 2025 году количество случаев данного вида мошенничества увеличилась практически в 2 раза по сравнению с уровнем 2024 года. Мошеннические схемы в рамках социальной инженерии демонстрируют высокую степень адаптивности, постоянно видоизменяясь в соответствии с актуальным контекстом и уязвимостями. Основной вектор атак направлен на прямое психологическое воздействие, в результате которого граждане не только добровольно передают преступникам всю конфиденциальную информацию, доступные денежные средства, но и берут кредиты, оформляют займы, а в отдельных случаях соглашаются на продажу имущества. Что касается инструментов обналичивания, в отчетном периоде прослеживалась тенденция к активному использованию злоумышленниками внутренних платежных сервисов и каналов. Для вывода похищенных средств в первом звене цепочки преимущественно прибегали к системам, зарегистрированным на территории Республики Беларусь: услугам ЕРИП, платформам для P2P-переводов, а также использовали возможности криптовалютных бирж.

- мошенничество по токенам, рост мошенничества на 15% относительно 2024 года. Посредством методов социальной инженерии злоумышленники получали данные карточки держателей и привязывали ее к собственному мобильному устройству. Это позволяло беспрепятственно совершать платежи в сети Интернет, организациях торговли и сервиса, а также снимать наличные в банкоматах. В 2025 году 16% всех мошеннических операций по токенам пришлось на операции оплаты в интернет-сервисах, зарегистрированных на территории США, Кипра, Ирландии и Арабских Эмиратов; 26% - на токенизированные операции в физических ОТС, зарегистрированных в таких странах как Арабские Эмираты, Польша, Казахстан, Узбекистан, Бразилия и Чили и др.; 58% - обналичивание денежных средств в АТМ, зарегистрированных в таких странах как Российская Федерация, Словакия и Беларусь.

- мошенничество с использованием технологии «NFC Gate». NFC-ретрансляция опирается не столько на технические уязвимости, сколько на доверие пользователей. В 2025 году в доле социальной инженерии около 2,5% мошеннических случаев пришлось на мошенничество с использованием технологии «NFC Gate». Всплеск мошенничества по «NFC Gate» наблюдался в 3 квартале 2025 года. При этом внедрение финансовыми институтами в течение года ограничительных и антифрод мер способствовало снижению случаев данного вида мошенничества уже в 4 квартале 2025 года.

- рост случаев компрометации систем дистанционного банковского обслуживания (СДБО) клиентов в результате применения методов социальной инженерии. По итогам отчетного периода количество подобных инцидентов возросло на 18% по сравнению с аналогичным периодом 2024 года. Перехват учетных данных (логинов и паролей) от систем ДБО предоставляет злоумышленникам полный доступ к управлению финансами жертвы.

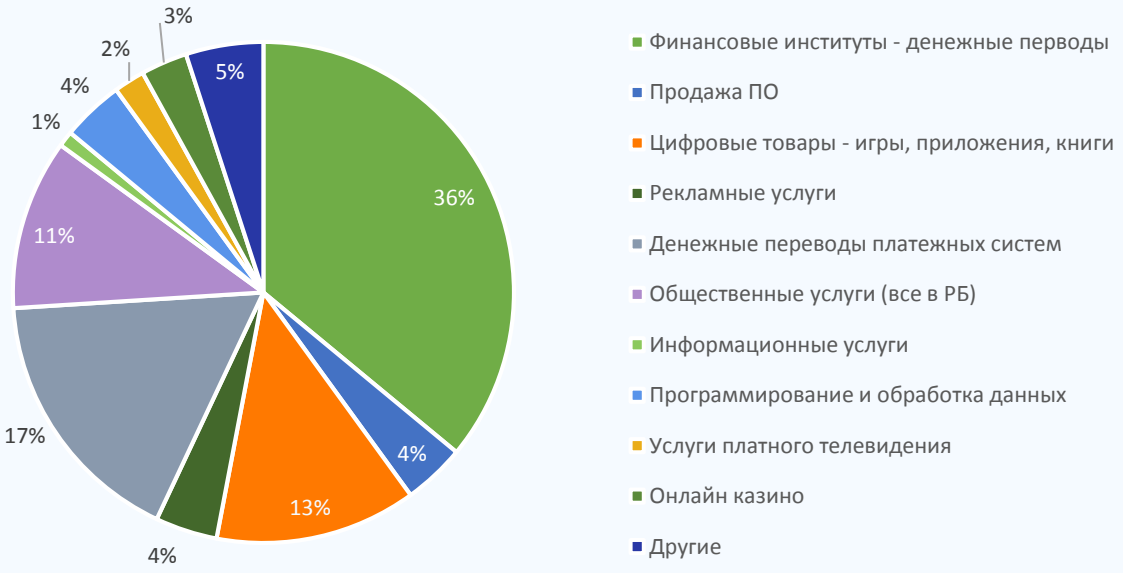
- зафиксировано снижение более чем в 2 раза количества случаев мошенничества с карточными реквизитами в среде e-commerce по сравнению с 2024 годом. Основной сценарий — компрометация данных держателей и последующие транзакции на сайтах, которые занимаются продажей цифровых товаров;

- наличие тестовых мошеннических операций, включая атаки на банковские идентификаторы (BIN) с использованием сгенерированных номеров карточек. Целью данных атак является проверка и выявление валидных платежных реквизитов для их последующего использования в мошеннических целях. В 2025 году для проведения таких транзакций преимущественно использовались онлайн-сервисы и организации торговли и сервиса, зарегистрированные на территории США, Великобритании, Канады, Объединенных Арабских Эмиратов и др.

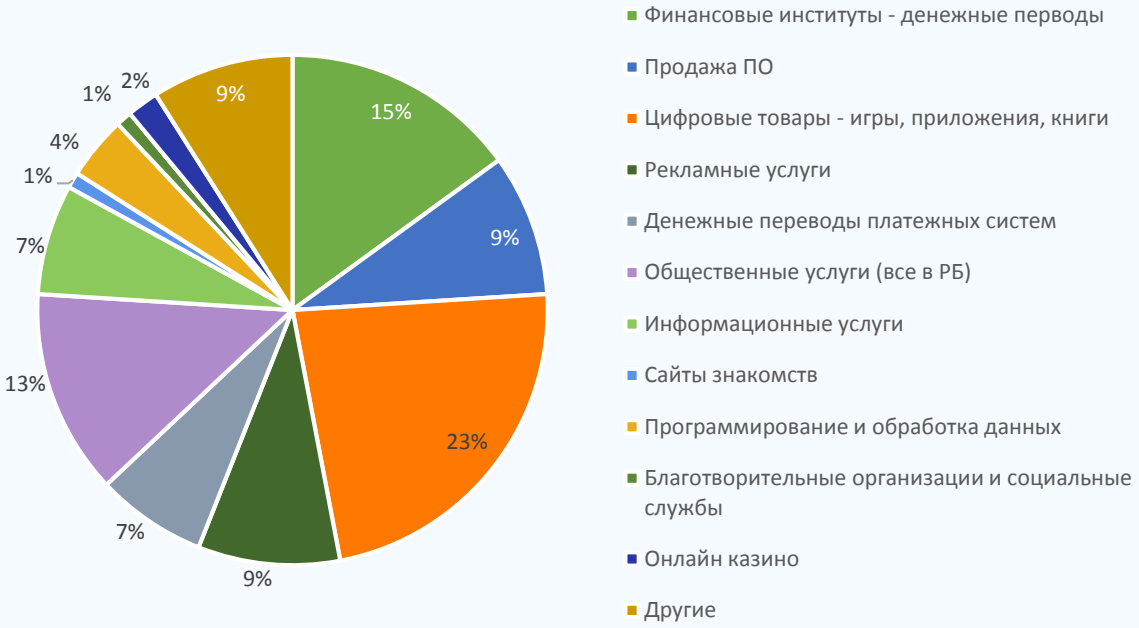
- случаи мошенничества по схеме «friendly fraud» («дружественное мошенничество»). Его суть заключается в том, что законный держатель карточки или лица из его ближайшего окружения, совершив и получив оплаченный товар или услугу, намеренно инициируют процедуру чарджбэка (возврата платежа), ложно заявляя о несанкционированной транзакции или компрометации своих платежных данных.

Виды мошенничества CNP, %

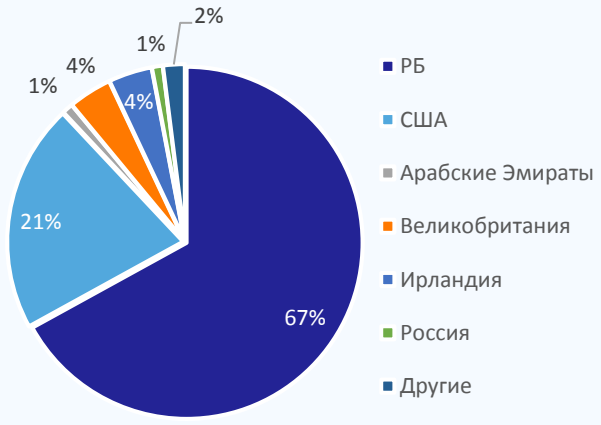
В каких ОТС (категориях ОТС) осуществлялись мошеннические операции с использованием реквизитов карточек в 2025 году



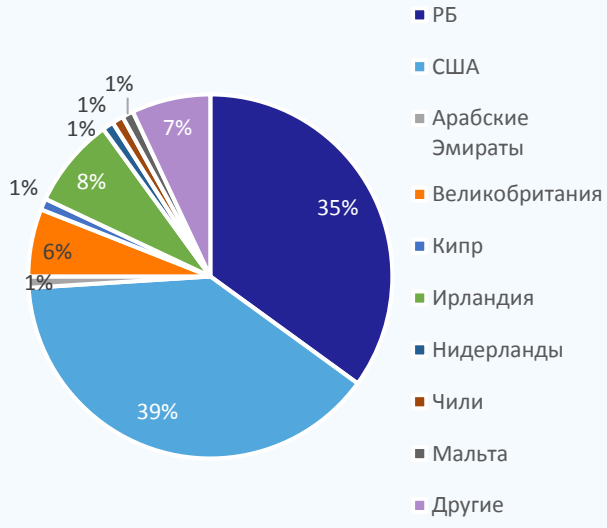
В каких ОТС (категориях ОТС) осуществлялись мошеннические операции с использованием реквизитов карточек в 2024 году



Страны, в которых осуществлялись мошеннические операции с использованием реквизитов карточек в 2025 году



Страны, в которых осуществлялись мошеннические операции с использованием реквизитов карточек в 2024 году



Банковский Процессинговый Центр

Рекламации эмиссия (данные по операциям с банковскими платежными карточками, выпущенными банками, которые обслуживаются в ОАО «Банковский процессинговый центр»):

В 2025 году общее количество рекламаций эмиссии снизилось в 1,4 раза относительно 2024 года, что обусловлено снижением количества оспоренных несанкционированных операций, при этом операции преимущественно оспаривались на сайтах APPLE.COM, FACEBK, GOOGLE, PAYPAL, aliexpress и др. В рамках процесса оспаривания сохраняется тенденция роста количества оспоренных мошеннических операций без присутствия карточки, при этом с развитием технологий в сфере безопасности платежей мошенники стали использовать не только реквизиты карточек, но и реквизиты токенов для несанкционированного списания денежных средств со счетов держателей карточек.

В 2025 году рекламации по причинам оспаривания распределились следующим образом:

71,8% от общего количества рекламаций были инициированы по причине мошенничества (89,1% в 2024 году).

4,8% составляют операции, оспоренные по причине неполучения держателем карточки товаров/услуг (6,2% в 2024 году).

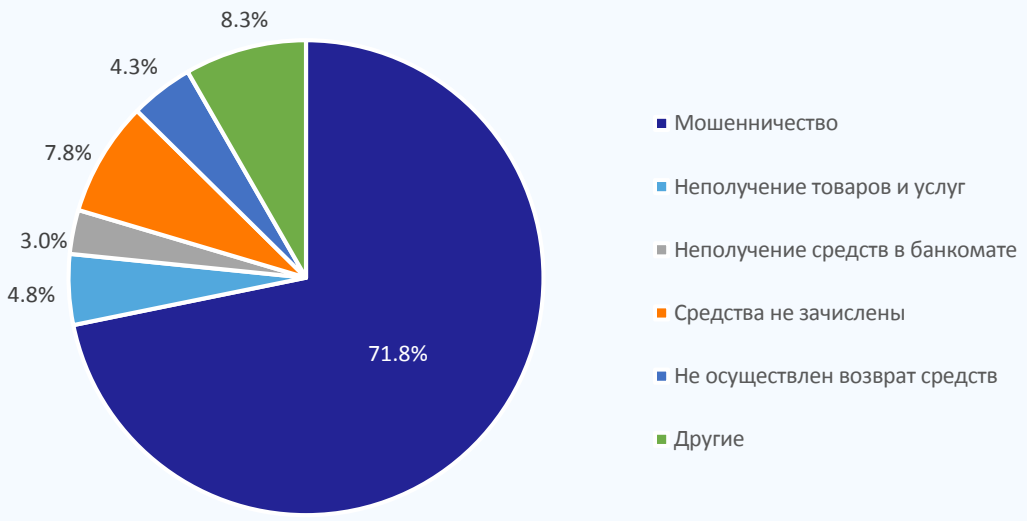
4,3% - операции, оспоренные по причине неполучения возврата денежных средств (0,5% в 2024 году).

3,0% приходится на долю рекламаций по операциям неполучения денежных средств в банкоматах (1,6% в 2024 году).

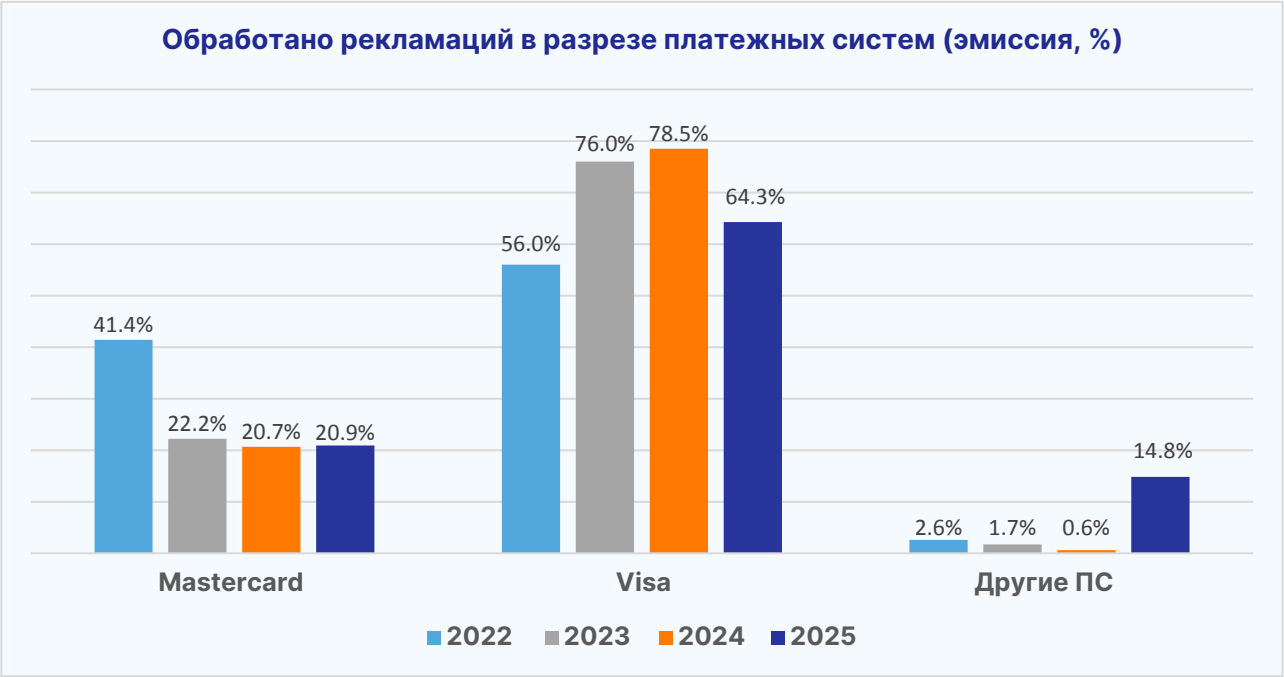
7,8% составляют рекламации по причине «Средства не зачислены» по операциям пополнения наличными денежными средствами с предъявлением карточки (0,3% в 2024 году).

8,3% от общего количества оспоренных операций составили остальные виды рекламаций (2,6% в 2024 году).

Распределение рекламаций по причине оспаривания в 2025 году (эмиссия, %)



Распределение рекламаций по платежным системам: Visa – 64,3%, Mastercard – 20,9% и другие ПС – 14,8%.



Эквайринг (данные по операциям в эквайринговой сети банков, подключенных к ОАО «Банковский процессинговый центр»):

В 2025 году в 1,6 раза увеличилось количество операций мошеннического характера в эквайринговой сети банков, которые обслуживаются в ОАО «Банковский процессинговый центр», что больше показателя 2024 года. Из них **16%** составляют мошеннические операции **без присутствия карточки; 75% - другие виды мошенничества: 63,5%** составляет мошенничество с перехватом данных держателей, 34,4% - мошенничество, связанное с манипуляцией владельцем счета, 1,8% - мошенничество, связанное с выпуском карточки по поддельным данным, 0,3% - карточка не получена в том виде, в котором выпущена; **7%** приходится на долю мошеннических операций **по утерянным/украденным карточкам** и **2%** приходится на мошеннические операции с использованием **поддельных карточек.**

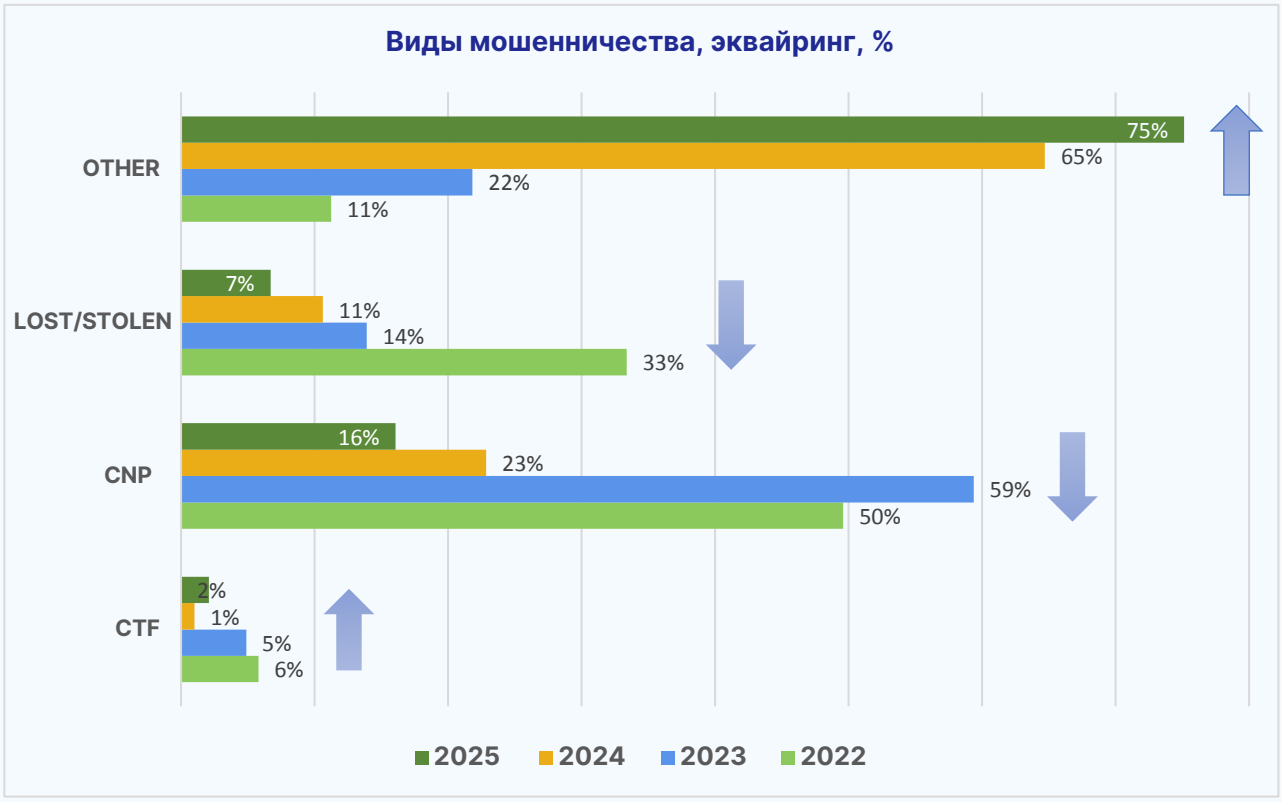
Мошеннические операции **без присутствия карточки** в 43% случаев прошли с использованием реквизитов карточки в среде e-commerce, 50% — это операции с использованием технологии 3-D Secure, 5% — это операции в ОТС с физическим или бесконтактным использованием карточки, 2% — это операции с вводом ключа.

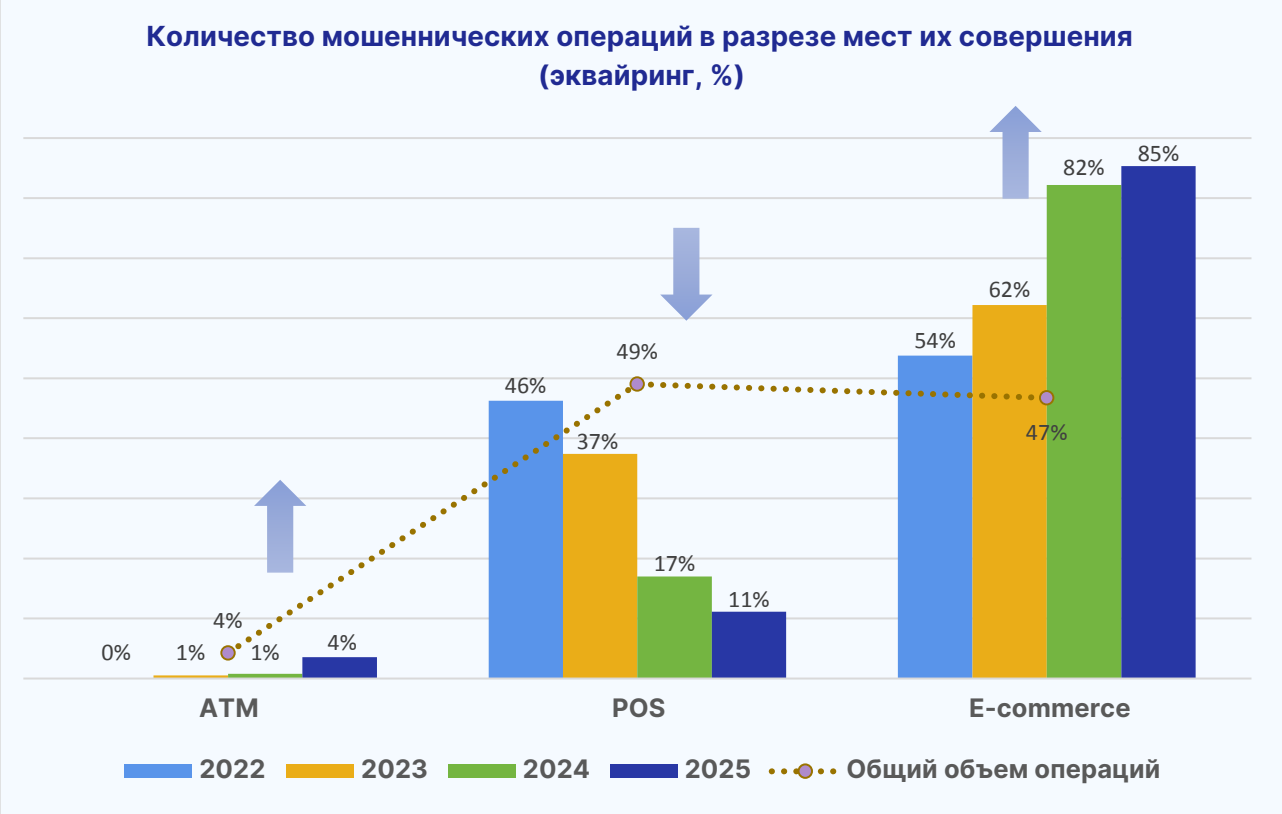
Мошеннические операции **по утерянным/украденным карточкам** в 92% случаев были осуществлены с физическим или бесконтактным использованием карточки, 6% — это операции с использованием 3-D Secure, 2% пришлось на операции с использованием реквизитов карточек.

Мошенничество по поддельным карточкам в 57% случаев проходило с физическим или бесконтактным использованием карточки, 16% из заявленных операций прошли с использованием реквизитов карточек, 28% — это операции с использованием 3-D Secure. В 2025 году в эквайринговой сети банков не было зафиксировано ни одного реального случая использования поддельных карточек.

В 2025 году общее количество мошеннических операций в эквайринговой сети увеличилось на 62%, а общая сумма мошеннических операций по сравнению с 2024 годом увеличилось на 263%, средняя сумма 1 мошеннической операции составила 374 доллара США (168 долларов США в 2024 году).

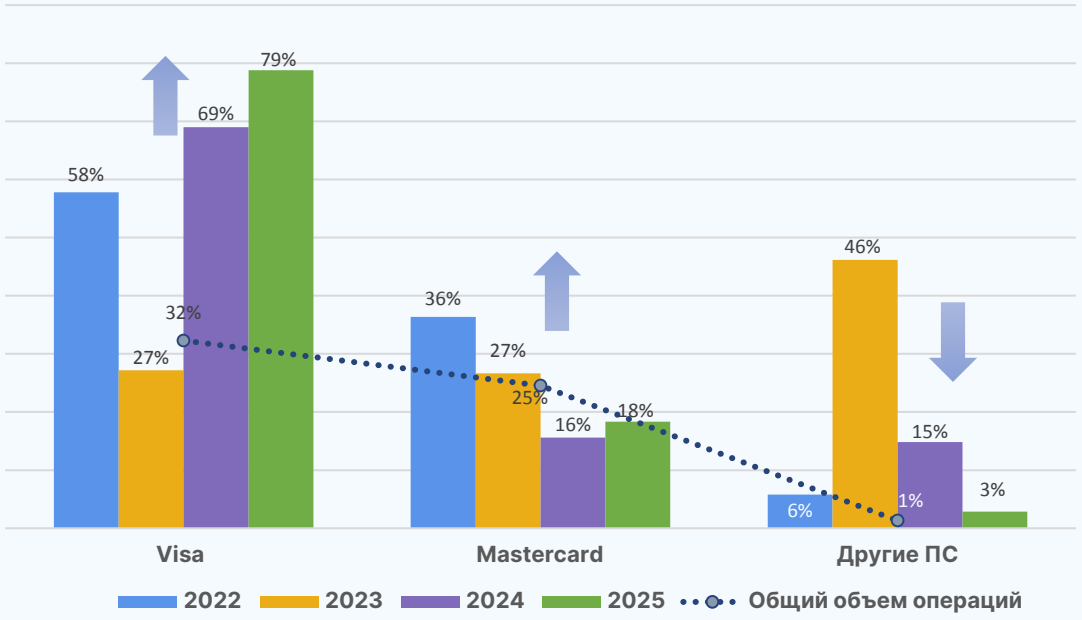
Увеличение количества и суммы мошеннических операций обусловлено ростом случаев мошенничества с использованием методов социальной инженерии, таких как взлом аккаунта и манипулирование держателем карточки.





Банковский Процессинговый Центр

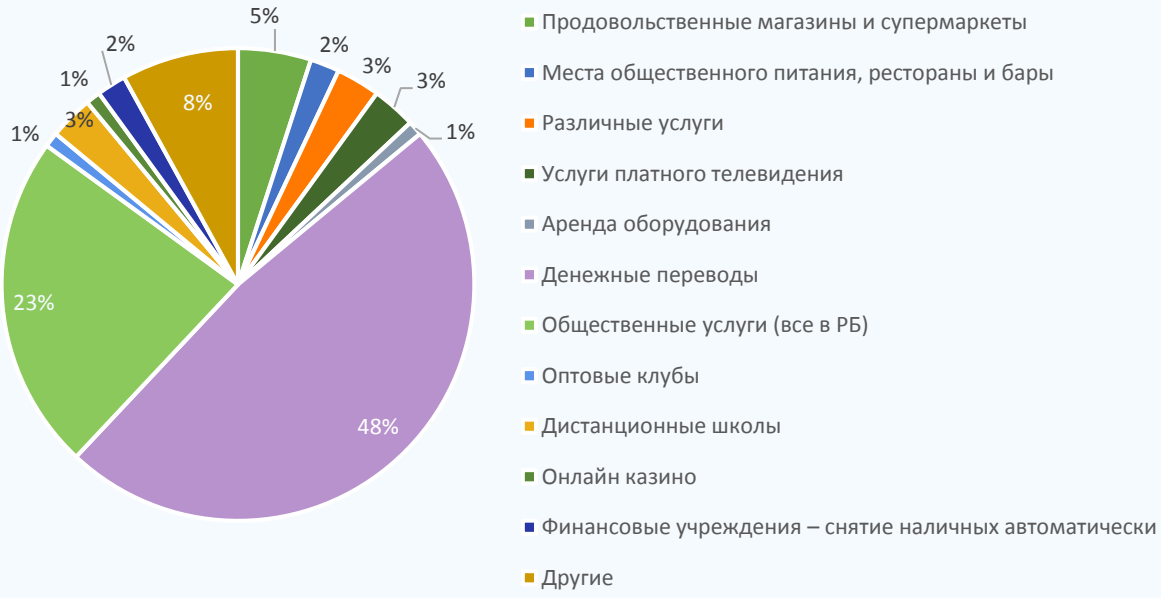
Количество мошеннических операций в разрезе платежных систем (эквайринг, %)



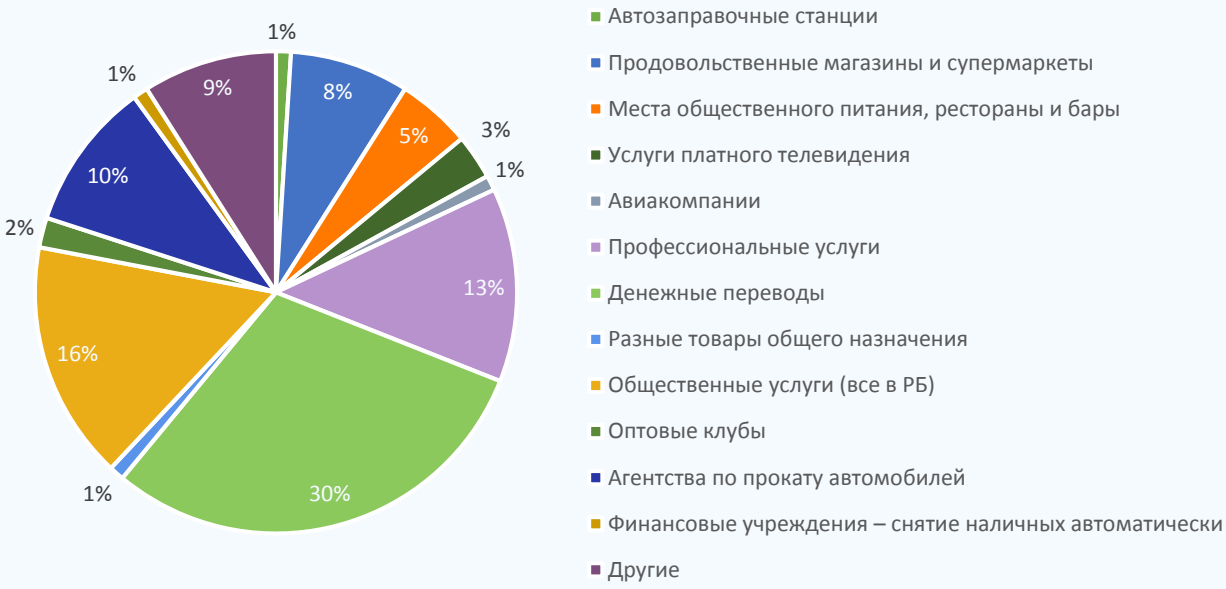
Рейтинг MCC, в которых осуществлялись мошеннические операции в эквайринге, распределился следующим образом: 48% мошеннических операций пришлось на денежные переводы; 23% на общественные услуги; 5% - продовольственные магазины и супермаркеты; по 3% на услуги платного телевидения, различные профессиональные услуги и дистанционные школы; по 2% на места общественного питания, рестораны и бары и финансовые учреждения – снятие наличных автоматически; по 1% приходится на аренду оборудования, оптовые клубы и онлайн казино; 8% - другие ОТС.

Наиболее часто в 2025 году в эквайринговой сети в мошеннических целях использовались карточки, эмитированные банками Беларуси, США и России.

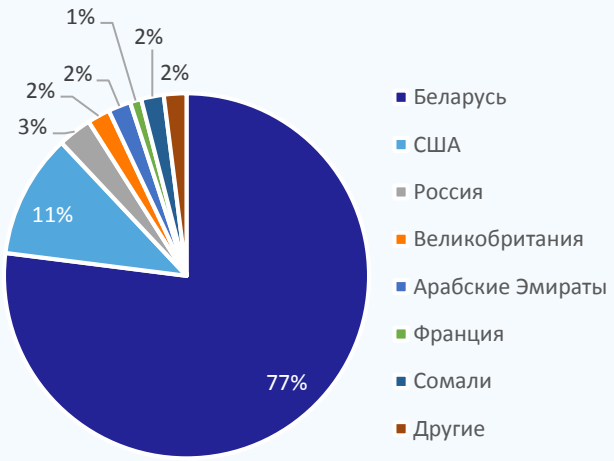
В каких ОТС (категориях ОТС) осуществлялись мошеннические операции в эквайерской сети по карточкам банков в 2025 году



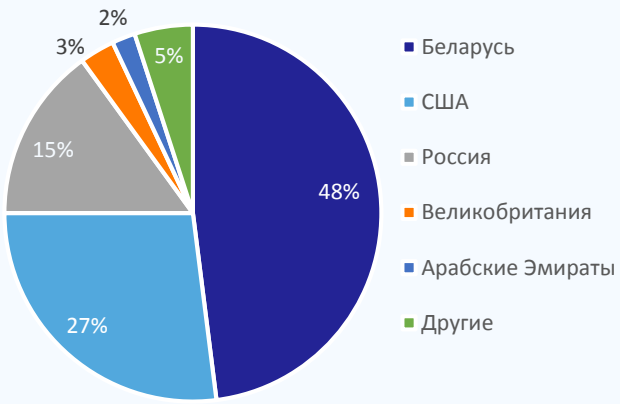
В каких ОТС (категориях ОТС) осуществлялись мошеннические операции в эквайерской сети по карточкам банков в 2024 году



Страны банков-эмитентов, по карточкам которых проходили мошеннические операции в эквайринговой сети в 2025 году



Страны банков-эмитентов, по карточкам которых проходили мошеннические операции в эквайринговой сети в 2024 году



Банковский Процессинговый Центр

Рекламации эквайринг (данные по операциям в эквайринговой сети банков, подключенных к ОАО «Банковский процессинговый центр»):

В 2025 году было обработано эквайерских рекламаций в 15,7 раз меньше, чем в 2024 году. Большинство операций, оспоренных по причинам неполучения товаров/услуг – это рекламации, инициированные по операциям оплаты образовательных курсов, доставки цветов и билетов на различные мероприятия. Рекламации, инициированные по несанкционированным операциям, преимущественно были совершенны на маркетплейсах, в ОТС, оказывающих услуги платного телевидения.

В 2025 году рекламации по причинам оспаривания распределились следующим образом:

27,1% оспоренных операций относятся к операциям неполучения товаров и услуг (91,5% в 2024 году).

17,2% – не получен возврат денежных средств (4,9% в 2024 году).

13,8% от общего количества рекламаций были оспорены по причине мошенничества (1,9% в 2024 году).

13,2% составляют операции, оспоренные по причине «Duplicate Processing» и «Оплачено иным способом». Держатели иностранных карточек утверждали, что за одну покупки денежные средства были списаны несколько раз.

10,4% - нарушение технологии проведения операций (0,5% в 2024 году).

6% от общего числа рекламаций составили операции, оспоренные по причине неполучения денежных средств в банкомате (0,2% в 2024 году).

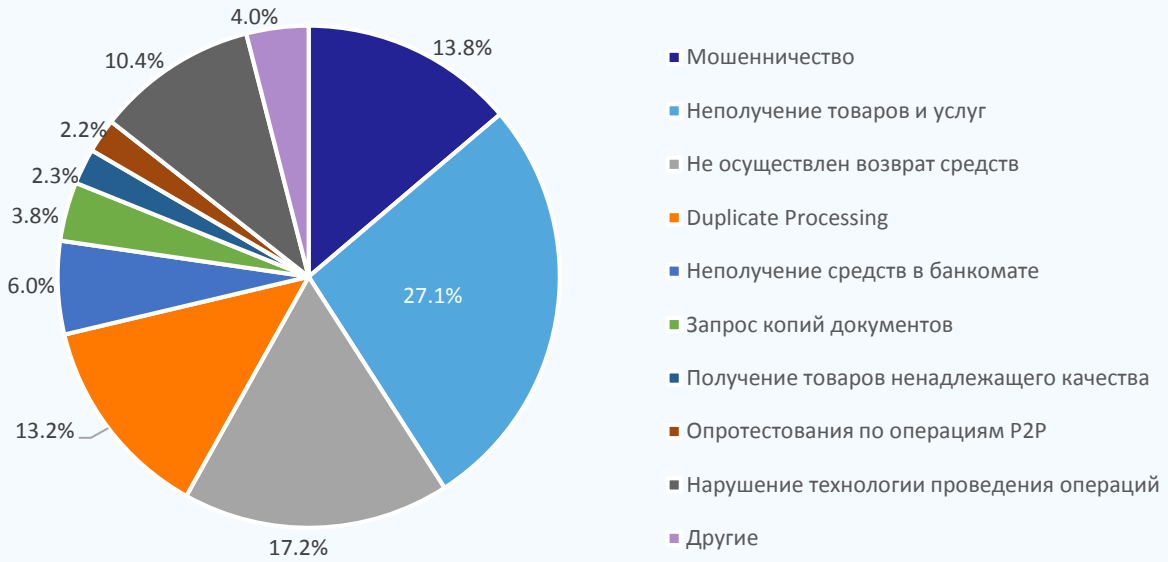
3,8% составляют запросы копий документов, подтверждающих совершение операций.

2,3% оспоренных операций относятся к операциям получения товаров и услуг ненадлежащего качества.

2,2% составляют опротестования по операциям P2P – держатели иностранных карточек отказываются от зачисленных денежных средств.

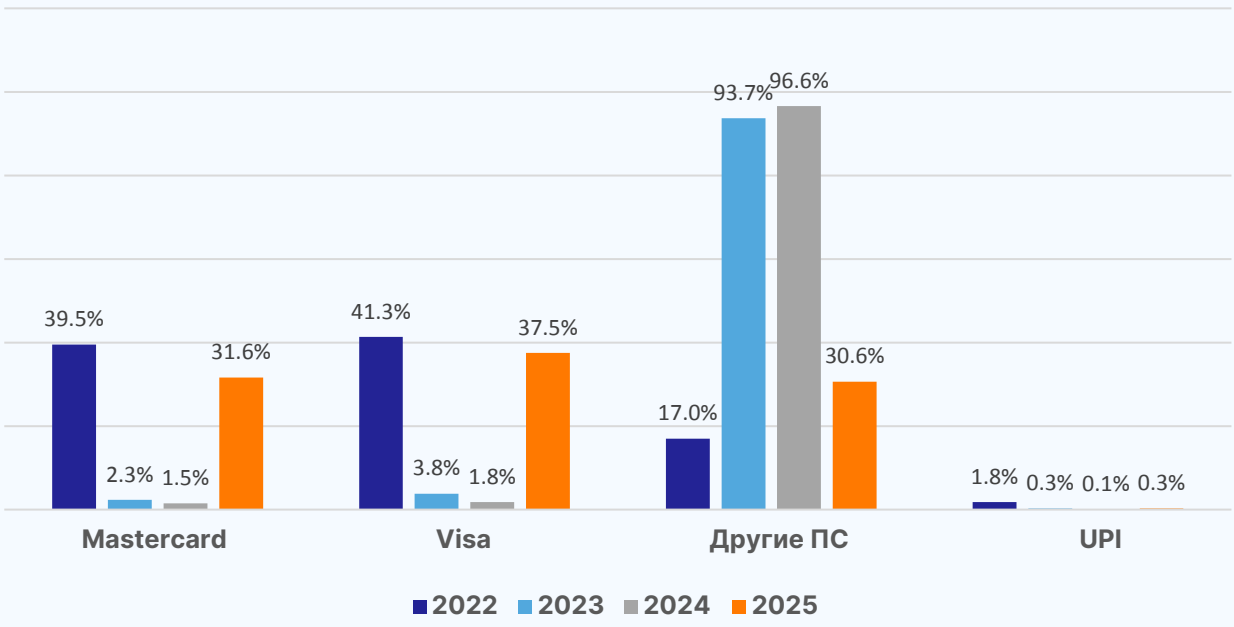
4,0% от общего количества оспоренных операций приходится на остальные виды рекламаций (1,0% в 2024 году).

Распределение рекламаций по причине оспаривания в 2025 году (эквайринг, %)



Распределение рекламаций по платежным системам: Visa – 37,5%, Mastercard – 31,6%, UPI – 0,3%, другие ПС – 30,6%.

Обработано рекламаций в разрезе платежных систем (эквайринг, %)



Банковский Процессинговый Центр

Прогноз:

На основе анализа текущих трендов и экспертных оценок можно выделить следующие ключевые прогнозы по мошенничеству с банковскими платежными карточками на 2026 год:

- Гиперперсонализация фишинга и вишинг. Мошенники будут активнее использовать утекшие базы данных и искусственный интеллект для создания максимально персонализированных фишинговых сообщений, дипфеков голоса в телефонных звонках и таргетированных атак на граждан, а также особый интерес будут представлять сотрудники компаний (CEO-фрод).

- Эксплуатация новых каналов доверия. Рост мошенничества через официальные аккаунты брендов в мессенджерах, где злоумышленники имитируют службу поддержки, а также через платформы для поиска услуг и исполнителей (например, сценарии с «заказом услуг»).

- Развитие мошенничества с токенизацией. Угроза все больше будет смещаться в сторону кражи данных для их последующей токенизации в мобильных кошельках злоумышленников. Сценарии с удаленной установкой вредоносного программного обеспечения для принудительной токенизации карточки жертвы станут более распространенными.

- Интеллектуализация и масштабирование BIN-атак. Прогнозируется рост автоматизированных атак на банковские идентификаторы (BIN) с использованием искусственного интеллекта для более эффективной генерации и верификации номеров карточек, а также для анализа уязвимостей онлайн-магазинов.

- Использование криптовалютных сервисов и P2P-платформ. Ожидается дальнейший рост использования мгновенных P2P-платежей, криптообменников и NFT-маркетплейсов для быстрого отмывания и вывода украденных средств, что усложняет их трассировку.

- Смещение мошенничества в высокодоходные онлайн-сегменты. Основными целями для обналичивания через онлайн-платежи останутся: покупка цифровых активов, онлайн-гемблинг, благотворительные фонды-однодневки, а также оплата дорогих услуг (премиум-подписки, IT-сервисы).

- Локализация инфраструктуры. Мошенники будут активнее создавать локальную фишинговую инфраструктуру и использовать местные отделения торговли и сервиса в целевых регионах для снижения подозрительности операций.

- «Дружественное мошенничество» (Friendly Fraud) останется серьезной проблемой, особенно в секторе цифровых товаров и подписок, где граница между реальной компрометацией и умышленным чарджбэком размыта.

Главный вызов 2026 года — симбиоз технологической изощренности и психологической манипуляции. Основной фокус безопасности сместится с простого анализа транзакций на комплексную оценку цифрового поведения клиента, проверку устройств и активное противодействие социальной инженерии на всех каналах взаимодействия.