Мошенничество в сфере платежных инструментов и сервисов в 1 полугодии 2026 года: общая статистика и тенденции



Банковский Процессинговый Центр

Содержание:

ОБЩАЯ ИНФОРМАЦИЯ 3

ЭМИССИЯ 3

Мошеннические операции по поддельным карточкам 6

Мошеннические операции с использованием реквизитов карточек 7

РЕКЛАМАЦИИ ЭМИССИЯ 11

ЭКВАЙРИНГ 12

РЕКЛАМАЦИИ ЭКВАЙРИНГ 15

Перепечатка отчета и/или отдельной информации возможна только с письменного разрешения ОАО «Банковский процессинговый центр».

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 1 полугодии 2026 года основная доля мошенничества с банковскими платежными карточками в Республике Беларусь приходилась на операции без физического присутствия держателя карточки. Случаев установки скимминговых устройств и массовой компрометации данных держателей карточек на территории Республики Беларусь за данный период не зафиксировано.

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

По итогам 1 полугодия 2026 года зафиксировано изменение структуры мошеннических угроз, обусловленное значительным ростом количества BIN-атак (генерация номеров карточек и тестовые операции). При этом социальная инженерия продолжает оставаться одним из наиболее широко используемых способов мошенничества – 94% от суммы совершенных мошеннических операций в 1 полугодии 2026 года были украдены непосредственно с использованием ее методов.

В отчетном периоде генерация номеров карточек и тестовые операции стали самыми распространенными в сегменте e-commerce. Злоумышленники активно используют специализированное программное обеспечение для подбора номеров карточек и инициируют 1–2 транзакции (тестовые списания на небольшие суммы) с целью проверки валидности карточных данных перед крупным хищением. Атаки осуществляются преимущественно через торговые точки электронной коммерции, обладающие слабыми механизмами антифрод-защиты.

Социальная инженерия. Несмотря на снижение относительной доли в текущем периоде, метод остается одним из самых серьезных по сумме ущерба. Мошенники связываются с жертвами через телефонную связь и мессенджеры, представляясь сотрудниками банков, Ассоциации банков, процессингового центра, правоохранительных органов, сотовых операторов, поликлиники. Цель звонков – получить конфиденциальную информацию (номера карточек, персональные данные, логины, пароли, SMS-коды) и в дальнейшем ее использовать в мошеннических целях.

Особую проблему составляют мошеннические схемы, направленные на полное финансовое разорение граждан, – когда злоумышленники убеждают оформить кредит, продать недвижимость или снять все сбережения и передать их курьеру либо перевести через инфокиоск под предлогом «сохранения» или «декларирования» средств. После выполнения всех инструкций мошенники прекращают выходить на связь, а клиент остается без денег и с кредитными обязательствами.

Схема с принудительной токенизацией карточек клиентов банков в мобильных устройствах злоумышленников по-прежнему остается актуальной. При данном виде мошенничества используются как классические схемы социальной инженерии, так и уязвимости в процедурах удаленной идентификации, позволяющие добавить карточку в Apple Pay/Google Pay без физического подтверждения держателем. После токенизации карточки мошенники беспрепятственно совершают оплаты в торгово-сервисных предприятиях и снимают наличные в банкоматах как на территории Республики Беларусь, так и за ее пределами, обходя классические ограничения по карточкам.

Фишинговые ссылки не теряют свою актуальность в рамках мошеннических схем. Злоумышленники создают высококачественные копии сайтов банков, маркетплейсов, почтовых и транспортных компаний. Жертва, попадая на поддельный ресурс, вводит реквизиты для входа или оплаты, тем самым передавая мошенникам доступ к личному кабинету и карточным данным, что ведет к полной потере средств. В 1 полугодии 2026 года участились случаи использования фишинга для обхода двухфакторной аутентификации (запрос сессионных cookie).

Финансовое мошенничество под видом инвестиций остается самым дорогостоящим видом обмана. Так называемые «лжеброкеры» предлагают гражданам открыть инвестиционные счета в интернете и заработать сверхприбыль за короткий промежуток времени. Данные схемы активно маскируются под легальные криптобиржи и P2P-обменники. Все инвестиции, сделанные через подобные платформы, полностью теряются инвестирующими, а вернуть средства становится практически невозможно.

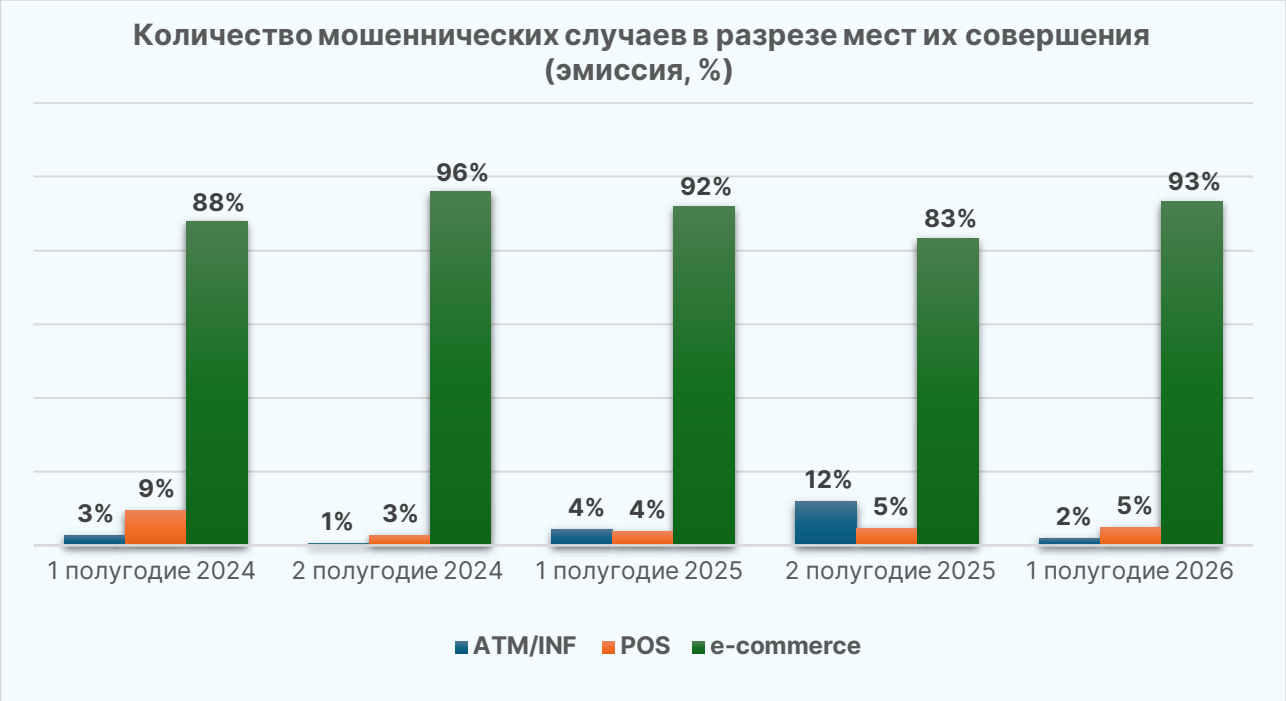
Дружественное мошенничество (Friendly Fraud). Клиенты оспаривают операции под предлогом «услуга не оказана» или «несанкционированное списание», хотя товар или услуга были получены. Данный вид мошенничества создает дополнительные финансовые риски для эквайринговых проектов и требует усиления работы с доказательной базой (включая сбор IP-адресов, геолокацию и подтверждение факта доставки).

По итогам 1 полугодия 2026 года количество успешных мошеннических операций по карточкам банков, которые обслуживаются в ОАО «Банковский процессинговый центр», по типу мошенничества распределилось следующим образом: **57,9%** мошеннических операций приходится на мошенничество **с использованием реквизитов карточек**, **41,7%** незаконных операций с банковскими платежными карточками приходится на **account takeover (перехват счета/манипулирование держателем)**, **0,4%** успешных мошеннических операций пришлось на мошенничество с использованием **утерянных/украденных карточек**, успешных мошеннических операций с использованием **поддельных карточек** зарегистрировано не было.

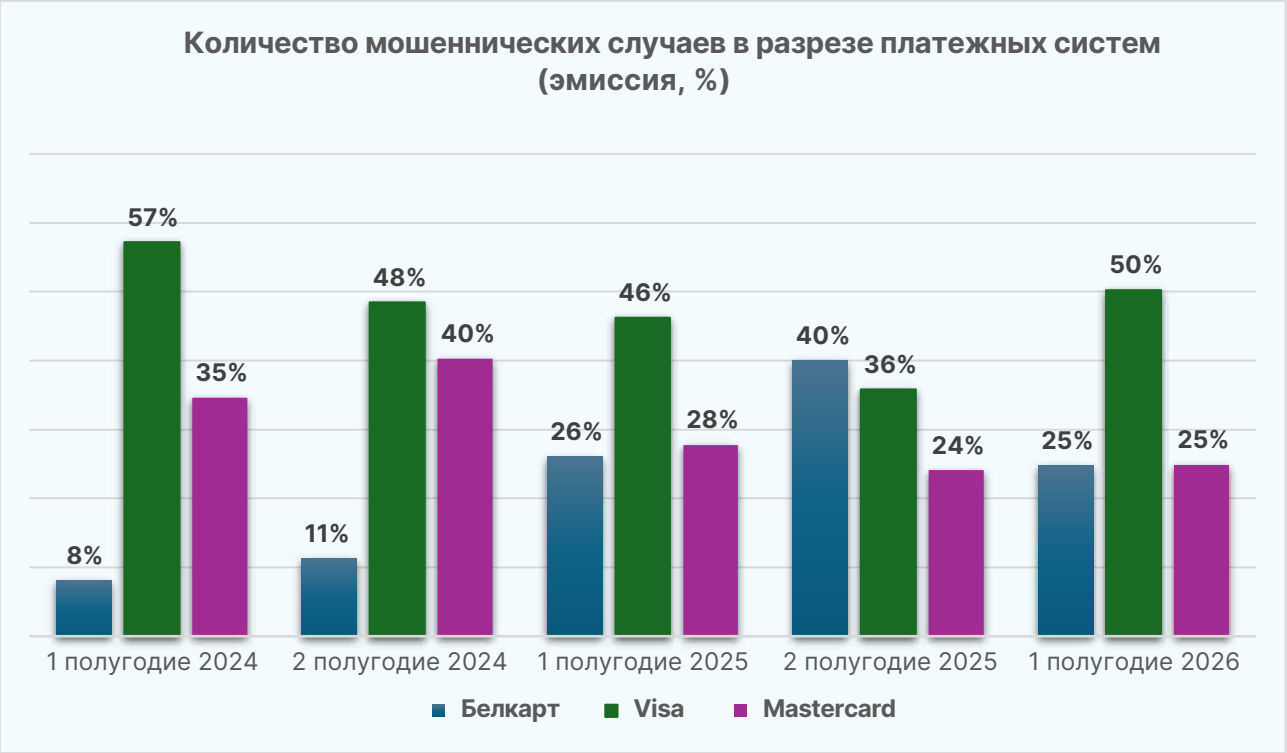
В 1 полугодии 2026 года на 4% уменьшилось количество успешных мошеннических операций, заявленных в международные платежные системы, по сравнению с 2 полугодием 2025 года, при этом 94% от суммы составляет именно социальная инженерия. Средняя сумма 1 мошеннической операции составила 179 долларов США (432 доллара США в 2 полугодии 2025 года). Уменьшение количества и суммы успешных мошеннических операций в отчетном периоде связано со снижением уровня мошенничества в рамках социальной инженерии.



В 1 полугодии 2026 года по количеству мошеннических случаев в разрезе мест их совершения 93% приходится на среду без присутствия карточки. В POS-терминалах прошло 5% случаев, в том числе токенизированные мошеннические операции, 2% - банкоматы и инфокиоски. Мошенничество в POS-терминалах и банкоматах обусловлено схемой мошенничества в рамках социальной инженерии, когда злоумышленники токенизируют карточки держателей на свои мобильные устройства, после чего осуществляют снятие наличных денежных средств в банкомате или оплачивают покупки в отделениях торговли и сервиса. В отличие от отчетного периода в 2 полугодии 2025 года активно использовалась схема мошенничества с использованием технологии NFC Gate, что обусловило увеличение доли мошеннических случаев в банкоматах и инфокиосках.



Банковский Процессинговый Центр



Мошеннические операции по поддельным карточкам:

В 1 полугодии 2026 года количество мошеннических случаев с использованием поддельных карточек уменьшилось в 2,2 раза относительно 2 полугодия 2025 года. В 1 полугодии 2026 года был выявлен случай использования поддельной карточки в клубах видеоигр на территории Соединенных Штатов Америки, случаи проведения операций в различных ОТС на территории Южно-Африканской Республики, Бразилии и Кореи, а также один неуспешный случай снятия наличных денежных средств в банкомате на территории Бразилии.

В 2 полугодии 2025 года поддельные карточки использовались в розничном магазине и на паркинге на территории США, в ресторане в Германии и в магазине на территории Бразилии, а также в организациях торговли и сервиса в таких странах, как ЮАР, Арабские Эмираты, США и Таиланд. Был выявлен неуспешный случай использования поддельной карточки в АТМ на территории Индии.

В целом, уровень мошенничества по поддельным карточкам остается низким. Невысокая популярность у злоумышленников скимминга обусловлена переориентацией на более доступные способы хищения денежных средств, в том числе на методы социальной инженерии, при использовании которых доход мошенников значительно выше при минимальных затратах.





Мошеннические операции с использованием реквизитов карточек:

Основными тенденциями мошенничества с использованием реквизитов карточек в 1 полугодии 2026 года являются:

- Мошенничество с применением методов социальной инженерии. Основной причиной неправомерных списаний с использованием социальной инженерии является компрометация платежных данных держателей карточек. Данный процесс преимущественно реализуется посредством телефонных звонков держателям, фишинговых рассылок, а также взаимодействием на торговых интернет-площадках. В 1 полугодии 2026 года доля данного вида мошенничества сократилась на 22% по сравнению с 2 полугодием 2025 года. Указанная динамика обусловлена ужесточением банковских лимитов и установлением ограничений на P2P-операции и на снятие наличных в банкоматах по бесконтактной технологии, что привело к переориентации злоумышленников в среду e-commerce. Для вывода похищенных средств в отчетном периоде злоумышленники задействовали платежные сервисы, зарегистрированные на территории Республики Беларусь.

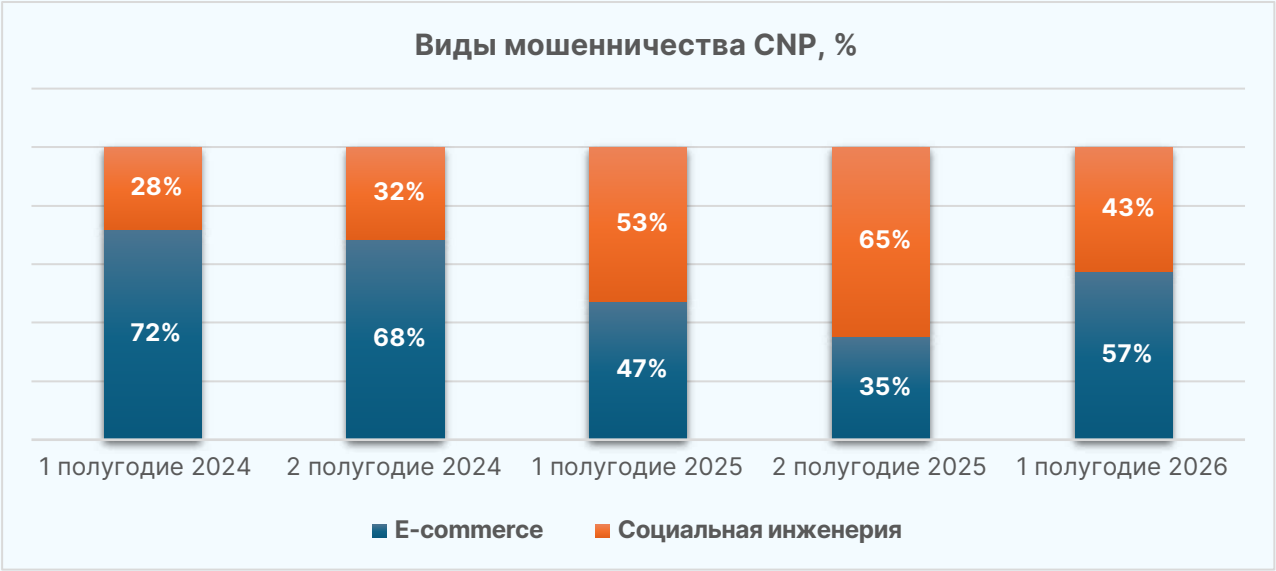
- Операции с использованием токенов. Количество мошеннических транзакций с применением токенов в 1 полугодии 2026 года снизилось на 58% по сравнению с 2 полугодием 2025 года. Типовая схема мошенничества предполагает привязку токена карточки держателя к мобильному устройству злоумышленника с последующим осуществлением несанкционированных платежей посредством заведенного электронного кошелька. Структура распределения данных операций по каналам выглядит следующим образом: 52% приходится на ОТС, 36% – интернет-сервисы, 12% – банкоматы.

- Компрометация систем ДБО. Неправомерный доступ к системам дистанционного банковского обслуживания клиентов также достигается методами социальной инженерии. Наибольший интерес для злоумышленников представляют логины, пароли и иные учетные данные, перехват которых позволяет получить полный контроль над финансовыми активами держателя. Получение доступа к системам ДБО преимущественно осуществлялось посредством инсталляции на мобильные устройства держателей программ удаленного доступа. Отмечено сокращение данной схемы мошенничества на 60% относительно 2 полугодия 2025 года.

- Атаки на BIN-номера банков и тестовые операции. В 1 полугодии 2026 года зафиксирован рост числа тестовых транзакций и атак на BIN-номера банков (генерация номеров карточек),

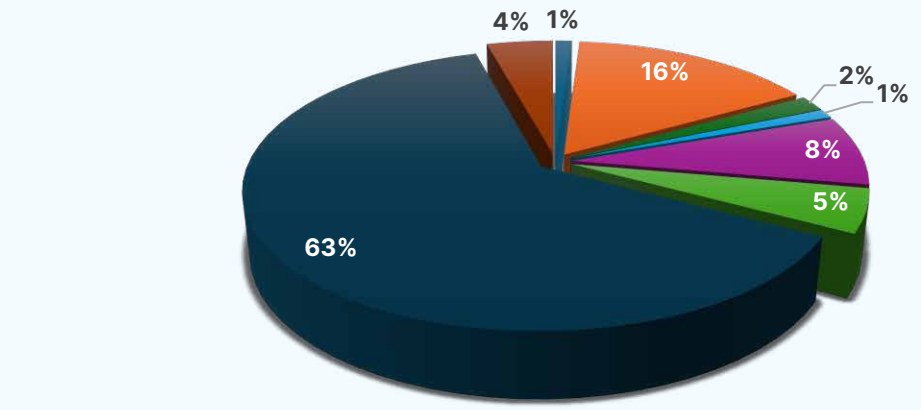
нацеленных на идентификацию действующих карточных счетов с последующим противоправным использованием их реквизитов. Инструментами для проведения BIN-атак выступали предприятия торговли и сервиса, инкорпорированные на территории США, Канады и Великобритании. Операции по генерации номеров карточек и тестовые платежи (исключая транзакции с протоколом 3-D Secure) составили 29% от общего объема мошеннических действий в секторе электронной коммерции за указанный период.

- Мошенничество в сфере электронной коммерции. Противоправные действия в сегменте e-commerce обусловлены компрометацией персональных данных держателей (включая инциденты утечек информации — data breach), а также совершением несанкционированных операций через онлайн-площадки по реализации цифровых товаров (программное обеспечение, игровой контент). Сохраняется тенденция взлома учетных записей Google, Apple, Facebook: после получения несанкционированного доступа к аккаунту злоумышленники инициируют платежи в сервисах на суммы, не превышающие остаток доступных средств на карточке держателя. Преимущественная регистрация вышеуказанных сервисов на территории США обуславливает высокий удельный вес операций с использованием карточных реквизитов в организациях торговли и сервиса в данном регионе.



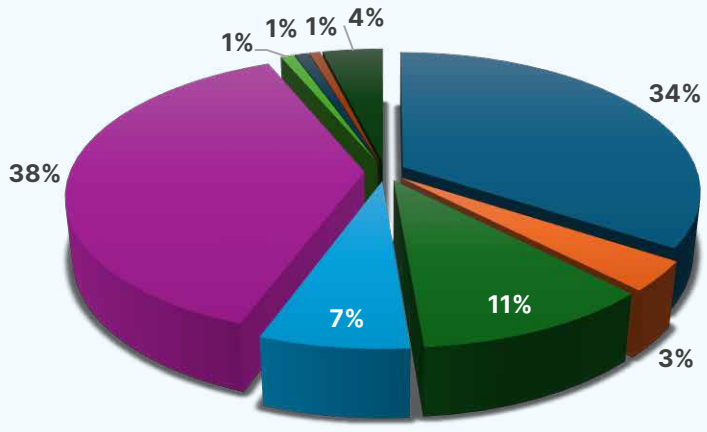


Страны, в которых осуществлялись мошеннические операции в 1 полугодии 2026 года



- Арабские Эмираты
- Республика Беларусь
- Китайская Народная Республика
- Великобритания
- Ирландия
- Российская Федерация
- Соединённые Штаты Америки
- Другие

Страны, в которых осуществлялись мошеннические операции в 2 полугодии 2025 года



- Республика Беларусь
- Великобритания
- Ирландия
- Российская Федерация
- Соединённые Штаты Америки
- Словакия
- Польша
- Казахстан
- Другие

Категории MCC, в которых осуществлялись мошеннические операции в 1 полугодии 2026 года



Категории MCC, в которых осуществлялись мошеннические операции в 2 полугодии 2025 года



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

В 1 полугодии 2026 года общее количество рекламаций в части эмиссии снизилось в 1,3 раза по сравнению с 2 полугодием 2025 года. В части эмиссии в рамках процесса оспаривания сохраняется тенденция поступления большого количества заявлений держателей карточек на опротестование мошеннических операций без присутствия карточки. Несанкционированные держателями карточек операции оспаривались преимущественно на интернет-ресурсах APPLE.COM, GOOGLE, SP HOLAFLY.COM, XAI LLC.

В 1 полугодии 2026 года рекламации по причинам оспаривания распределились следующим образом:

78,2% от общего количества рекламаций были инициированы по причине мошенничества по операциям, совершенным с использованием реквизитов карточек в сети Интернет (в 2 полугодии 2025 года – 87,8%);

7,3% приходится на рекламации, оспоренные по причине неполучения возврата денежных средств (в 2 полугодии 2025 года – 6%);

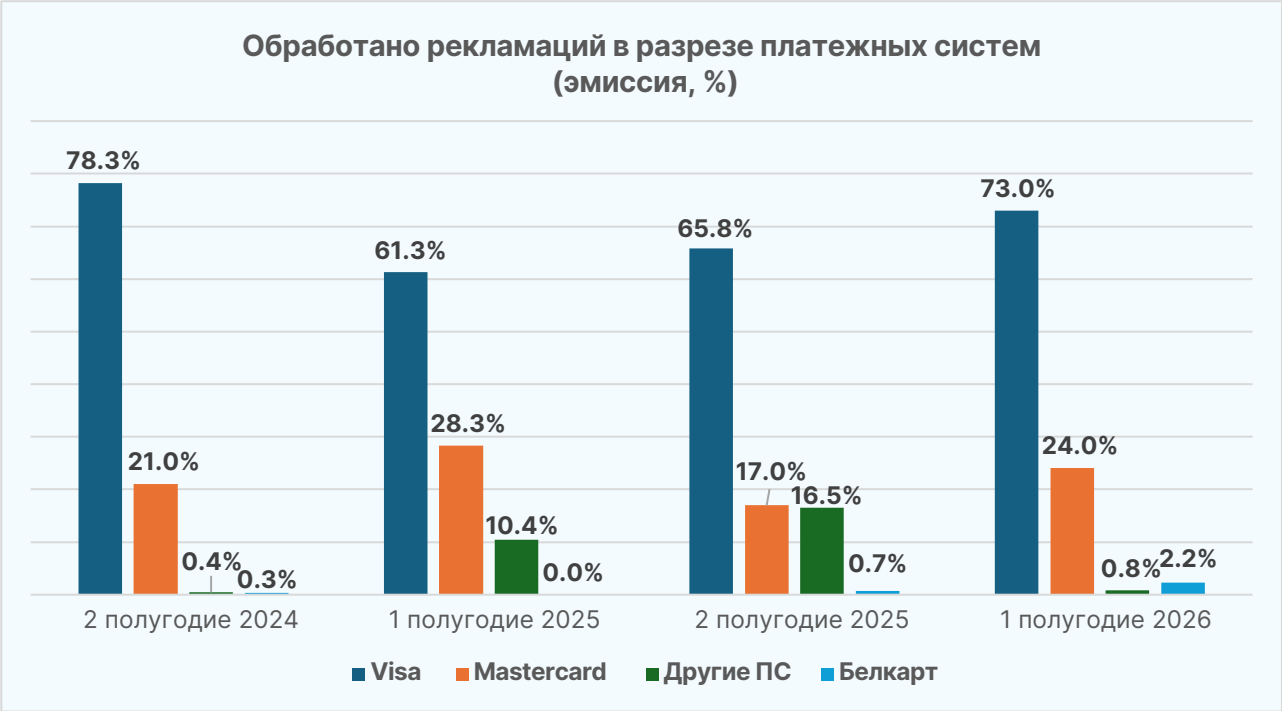
6,1% от общего количества рекламаций – это операции, оспоренные по причине неполучения держателем карточки товаров и услуг (в 2 полугодии 2025 года – 4,63%);

3,1% приходится на долю рекламаций по операциям неполучения денежных средств в банкоматах (в 2 полугодии 2025 года – 1,1%);

5,3% от общего количества оспоренных операций составили другие виды рекламаций (в 2 полугодии 2025 года – 23,1%).



Распределение рекламаций по платежным системам: МПС Visa – 73%, МПС Mastercard – 24%, ПС Белкарт – 2,2%, другие ПС – 0,8%.



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

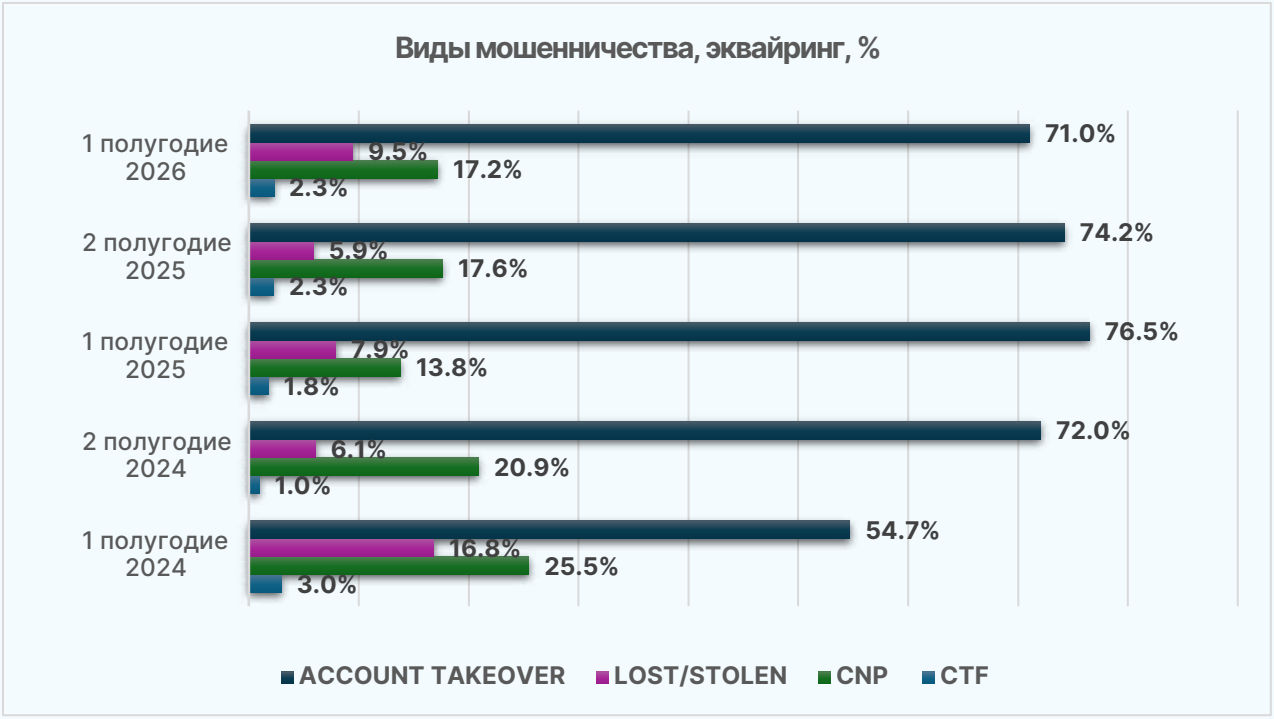
В 1 полугодии 2026 года количество операций мошеннического характера в эквайринговой сети банков, которые обслуживаются в ОАО «Банковский процессинговый центр», снизилось на 30% относительно 2 полугодия 2025 года. Из них **17,2%** приходится на долю мошенничества по операциям без присутствия карточки, 9,5% составляют мошеннические операции **по утерянным/украденным карточкам**, **2,3% - поддельные карточки** и **71%** приходится на **перехват счёта/манипулирование держателем**: 79% из которых прошли как e-commerce операции, 16% - 3-D Secure операции, 5% операций были осуществлены с признаком бесконтактных операций или по чипу.

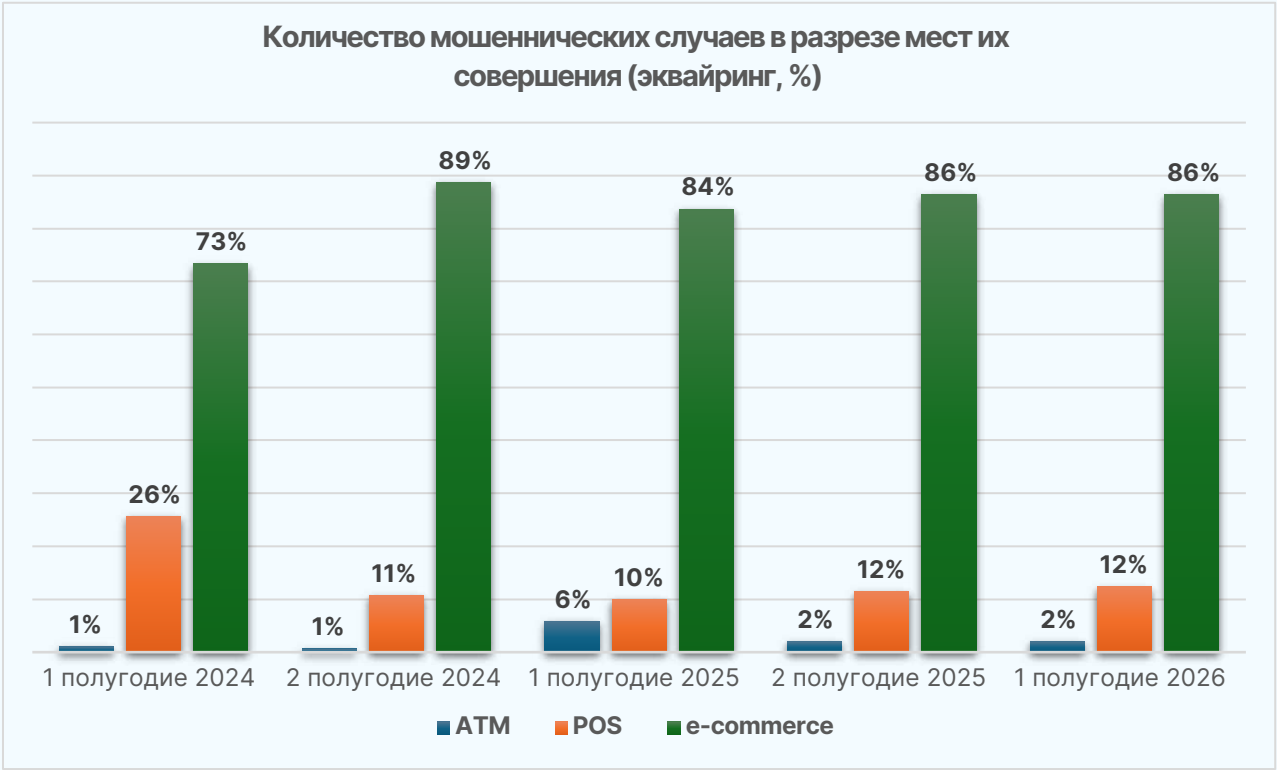
Мошеннические операции **без присутствия карточки** в 42% случаев прошли как операции с применением технологии 3-D Secure; 52% - e-commerce операции; 6% операций были осуществлены с признаком бесконтактных операций или по чипу.

В случае с **утерянными/украденными карточками** 82% операций были осуществлены с признаком бесконтактных операций или операций по чипу, 6% - 3-D Secure операции, 12% - e-commerce операции.

Мошенничество **по поддельным карточкам** - 47% заявленных операций прошли с признаком бесконтактной операции, 40% – с использованием реквизитов карточки, 13% - 3-D Secure операции.

Действительных случаев использования поддельных карточек в эквайринговой сети банков, подключенных к ОАО «Банковский процессинговый центр», не зафиксировано. Общая сумма мошеннических операций в 1 полугодии 2026 года снизилась на 38% по сравнению с 2 полугодием 2025 года, средняя сумма 1 мошеннической операции составила 291 доллар США (330 долларов США в 2 полугодии 2025 года). Снижение показателей связано с уменьшением доли социальной инженерии в связи с вводом банками ограничительных мер по операциям снятия наличных денежных средств по бесконтактной технологии и по токенам.





Банковский Процессинговый Центр

Мошеннические операции преимущественно проходили в эквайринге банков, на обслуживании у которых находятся сервисы денежных переводов, их доля составила 36%; 34% - жилищно-коммунальные услуги и инфокиоски; по 6% пришлось на продовольственные магазины/ супермаркеты и услуги платного телевидения; 3% - образовательные услуги; 2% - места общественного питания; 13% - другие ОТС.

Категории МСС, в которых осуществлялись мошеннические операции в эквайринговой сети в 1 полугодии 2026 года

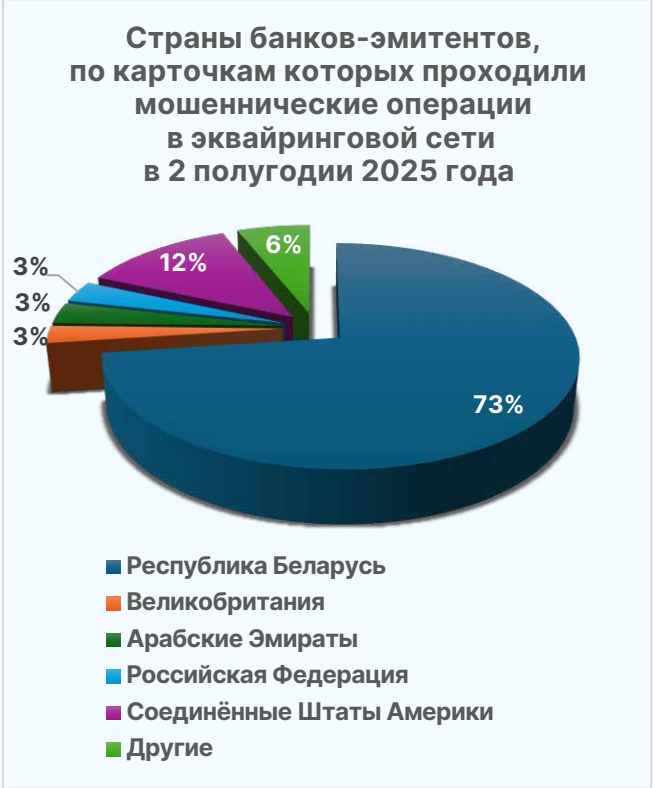


Категории МСС, в которых осуществлялись мошеннические операции в эквайринговой сети в 2 полугодии 2025 года



Наиболее часто в 1 полугодии 2026 года в эквайринговой сети в мошеннических целях использовались карточки, эмитированные банками Беларуси, США, России и Кыргызстана.





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

В 1 полугодии 2026 года общее количество эквайерских рекламаций увеличилось в 1,1 раза по сравнению с 2 полугодием 2025 года. В эквайерской части большинство операций, оспоренных по причинам неполучения товаров/услуг и неполучения возврата средств – это рекламации, инициированные по операциям оплаты билетов на различные мероприятия, а также услуг по доставке цветов.

В 1 полугодии 2026 года рекламации по причинам оспаривания распределились следующим образом:

24,4% оспоренных операций относятся к операциям неполучения товаров и услуг (во 2 полугодии 2025 года – 31,4%);

18,5% составили оспаривания по причине мошенничества с использованием реквизитов карточек (в 2 полугодии 2025 года – 12,5%);

14,1% – не получен возврат денежных средств (в 2 полугодии 2025 года – 17,2%);

11,9% составляют запросы копий документов, подтверждающих совершение операций. Все рекламации были завершены на этапе Fulfillment, банками-эквайерами были предоставлены документы, подтверждающие правомочность выставления операций к оплате (в 2 полугодии 2025 года – 5,7%);

10,4% составляют опротестования по операциям P2P – держатели иностранных карточек отказываются от зачисленных денежных средств (в 2 полугодии 2025 года – 1,9%);

5,4% от общего числа рекламаций составили операции, оспоренные по причине неполучения денежных средств в банкомате (в 2 полугодии 2025 года – 7,4%);

15,3% от общего количества оспоренных операций приходится на другие виды рекламаций (в 2 полугодии 2025 года – 24%).



Распределение рекламаций по платежным системам: Mastercard – 34,7%, Visa – 37,9%, другие ПС – 23,3%, МПС UPI – 2,6%, ПС Белкарт – 1,5%.

