Мошенничество в сфере платежных инструментов и сервисов в 2023 году:

общая статистика и тенденции

Отчет на основе данных
Банковского процессингового центра

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:

Основная доля мошенничества в Республике Беларусь в 2023 году, как и в прошлом году, приходится на мошенничество с банковскими платежными карточками в среде без физического присутствия держателя при проведении операции. Случаев установки скимминговых устройств и массовой компрометации данных держателей карточек на территории Республики Беларусь в 2023 году зафиксировано не было.

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

Характерной тенденцией 2023 года является мошенничество с использованием реквизитов карточек наряду с единичными случаями мошенничества по поддельным и утерянным/украденным карточкам. В среде мошенничества с использованием реквизитов карточек основная доля мошенничества приходится на социальную инженерию – около 60%. Значительная доля мошенничества с применением социальной инженерии свидетельствует о том, что данный вид мошенничества быстро адаптируется к любым изменениям, а использование методов социальной инженерии приносит быстрый доход злоумышленникам при минимальных финансовых затратах. Мошенники стремятся получить личные данные держателей карточек, доступы к их счетам, системам дистанционного банковского обслуживания, МСИ и мобильным устройствам. В целях хищения денежных средств и персональных данных в 2023 году злоумышленники в рамках социальной инженерии связывались с потенциальными жертвами посредством торговых площадок, осуществляли звонки от имени работников банков, правоохранительных органов и других различных организаций, направляли сообщения в социальных сетях и осуществляли рассылки в мобильных мессенджерах.

Активно эксплуатировалась схема мошенничества, связанная с установкой приложений удаленного доступа (AnyDesk, TeamViewer, RustDesk) на мобильные устройства держателей, в результате реализации которой злоумышленники получали полный контроль над счетами и денежными средствами. Участились случаи, когда держатели переходили по фишинговым ссылкам, считая, что это официальные ресурсы банков, почтовых служб и служб доставки, где вводили логин и пароль от интернет-банкинга или реквизиты своей карточки для оплаты услуг, в результате чего конфиденциальные данные становились доступны злоумышленникам и/или держатели лишались своих денежных средств.

По-прежнему использовалась схема мошенничества, связанная с сайтами знакомств, когда злоумышленники для якобы организации встречи присылали держателям фишинговые ссылки на покупку билетов в театр, кино или в другие места для развлечений. В случае, если клиент переходит по данной ссылке и соглашается с проведением оплаты, с его счета списывается денежная сумма.

В 2023 году появилась новая схема мошенничества с кредитами, которые держатели самостоятельно оформляют, а затем переводят кредитные денежные средства в адрес мошенников посредством инфокиосков. В данном случае злоумышленникам удается внушить держателям, что они участвуют в проведении служебного расследования по поимке недобросовестного сотрудника банка. Также имели место случаи, когда держатели даже продавали своё имущество (квартиры, автомобили, технику) и осуществляли переводы денежных средств на счета злоумышленников.

В конце 4 квартала 2023 года стала активно использоваться схема мошенничества, связанная с токенизацией скомпрометированных карточек. После получения необходимых данных карточки с использованием методов социальной инженерии или фишинговых рассылок, мошенники привязывают карточку на свое мобильное устройство и пытаются совершить оплаты в сети интернет либо в организациях торговли и сервиса, которые находятся в различных странах.

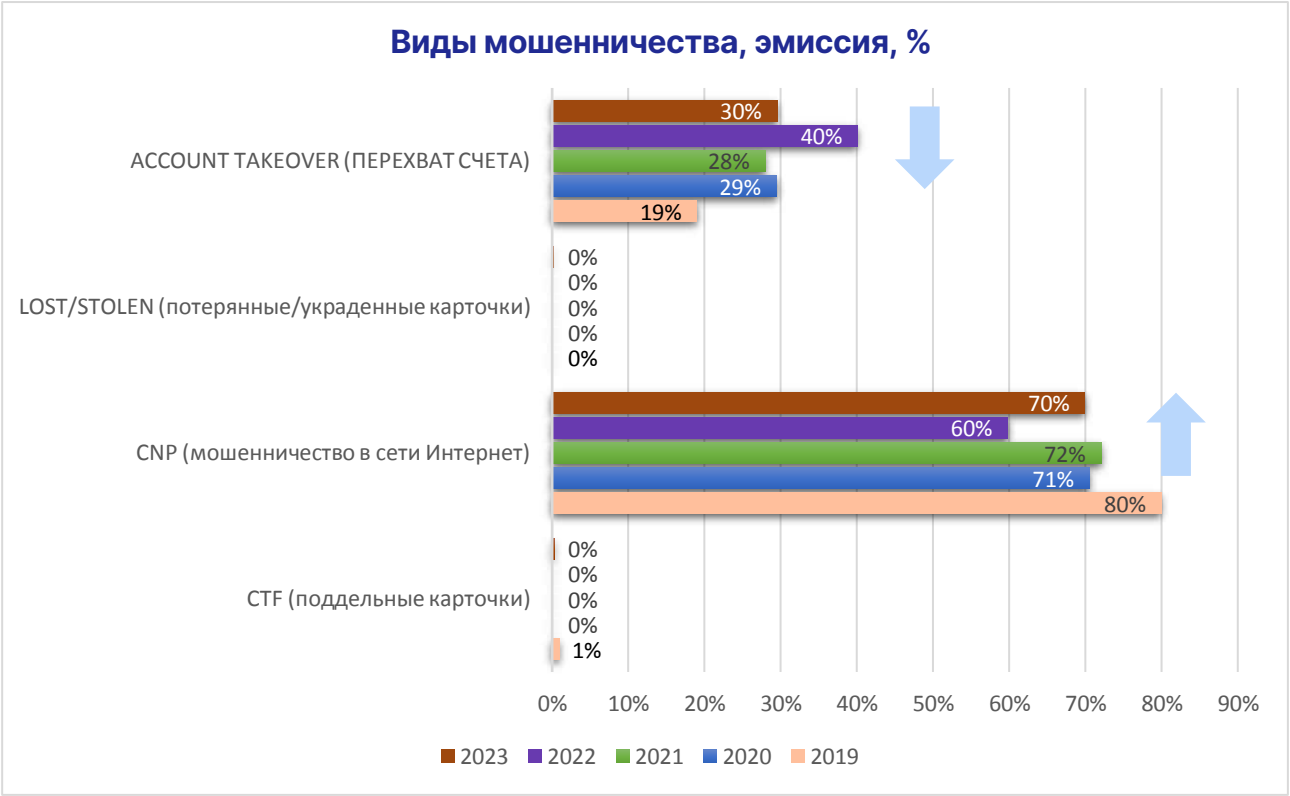
Участилось мошенничество, связанное с генерацией номеров карточек и атаками на БИНы банков - процесс инициирования 1-2 тестовых транзакций для проверки карточки с целью ее дальнейшего использования в мошеннических целях. При этом используются программные средства для генерации номеров карточек, а атаки осуществляются в торговых точках электронной коммерции, которые имеют слабые механизмы контроля и защиты от мошенничества.

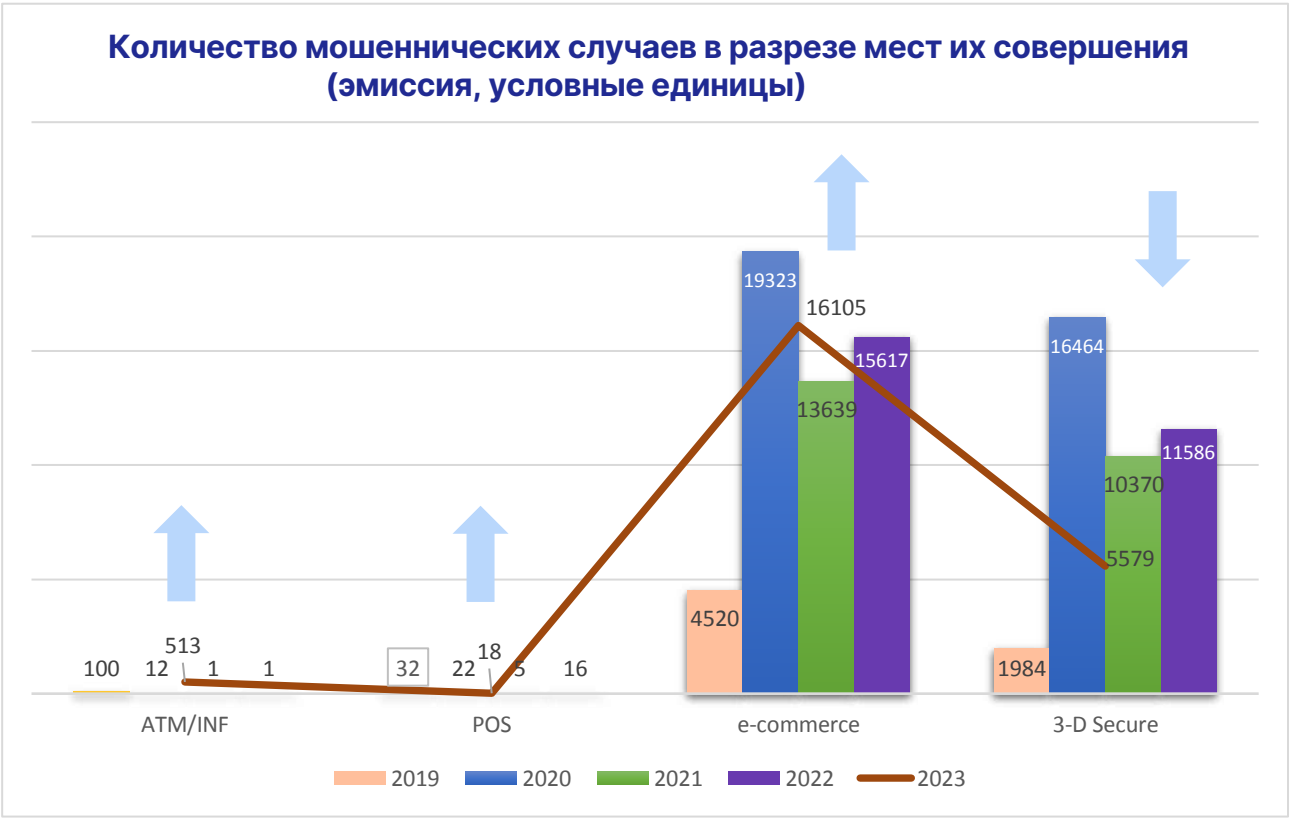
По итогам 2023 года количество успешных мошеннических операций по карточкам банков, которые обслуживаются в ОАО «Банковский процессинговый центр», по типу мошенничества распределилось следующим образом: **70%** мошеннических операций приходится на мошенничество **с использованием реквизитов карточек, 30%** незаконных операций с банковскими платежными карточками приходится на **account takeover (перехват счета).**

В 2023 году были зафиксированы мошеннические операции **по поддельным карточкам.** Открытие границ и, в целом, ослабление ограничений после периода коронавирусной инфекции COVID-19 способствовали активизации мошенничества, связанного со скиммингом.

В 2023 году количество выявленных мошеннических случаев (карточек) увеличилось на 8% относительно 2022 года, при этом на 57% сократилось общее количество успешных мошеннических операций, заявленных в международные платежные системы, общая сумма успешных мошеннических операций уменьшилась на 64%, а средняя сумма 1 мошеннической операции составила 35 долларов США (42 доллара США в 2022 году), что на 15% меньше алогичного показателя прошлого года. Уменьшение общей суммы успешных мошеннических операций, заявленных в международные платежные системы, обусловлено переориентацией злоумышленников на использование платежных сервисов, зарегистрированных на территории Республики Беларусь, использование систем дистанционного банковского обслуживания для вывода денежных средств, а также с увеличением количества мошеннических попыток по сгенерированным карточкам.

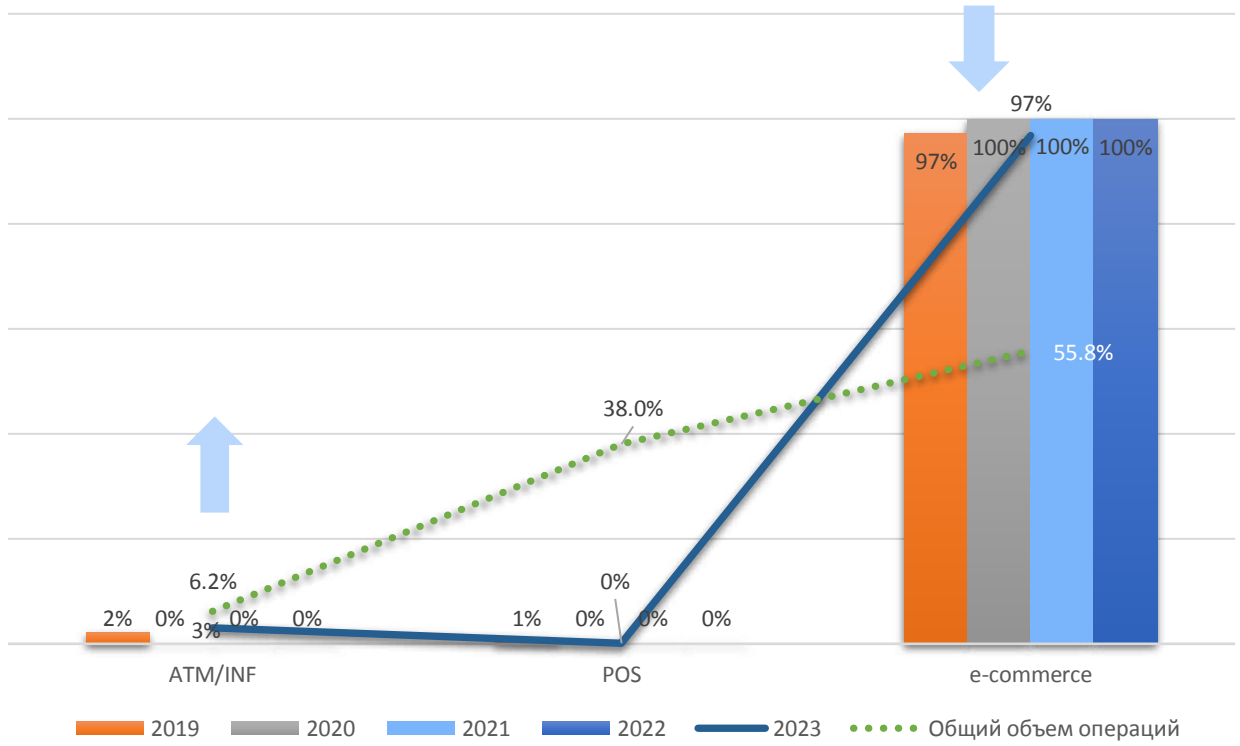
В 2023 году количество мошеннических случаев по операциям с использованием технологии 3-D Secure составило 34% (в 2 раза меньше по сравнению с 2022 годом). Снижение показателя связано с тем, что схемы мошенничества становятся все более разнообразными и подстраиваются под новые технологии и платежные решения.



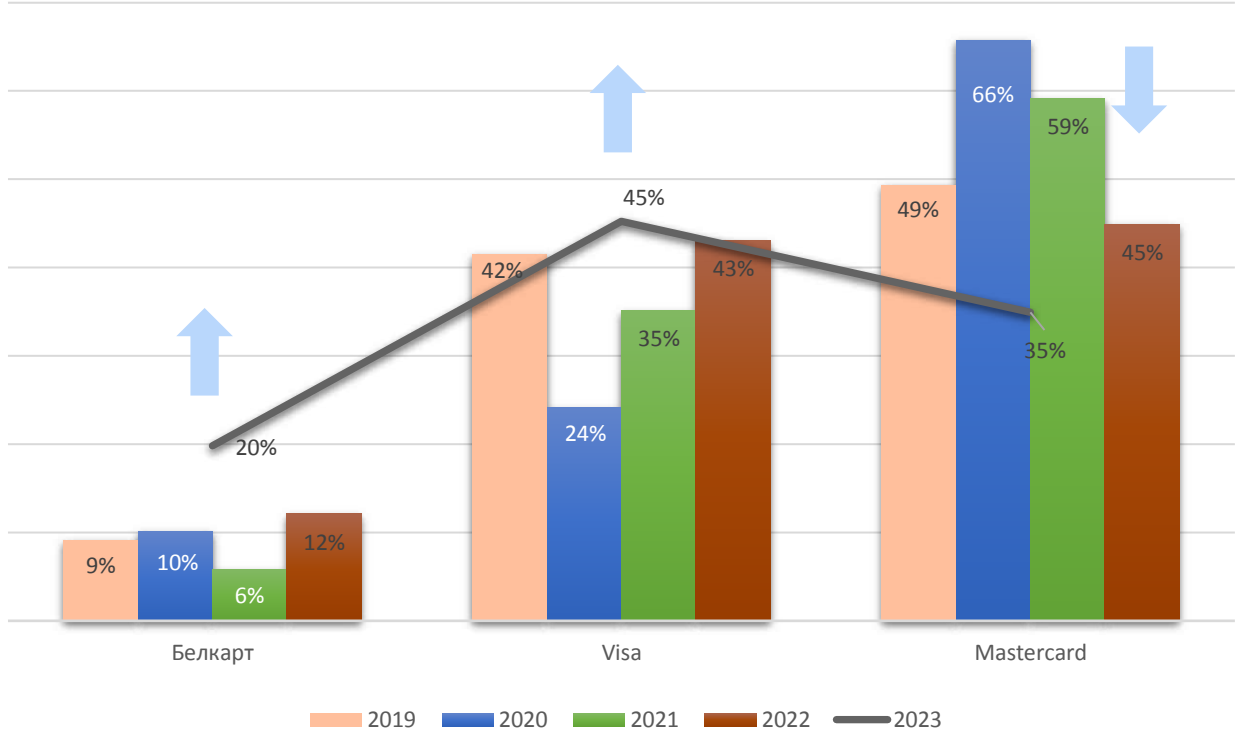


Банковский Процессинговый Центр

Количество мошеннических случаев в разрезе мест их совершения (эмиссия, %)



Количество мошеннических случаев в разрезе платежных систем (эмиссия, %)



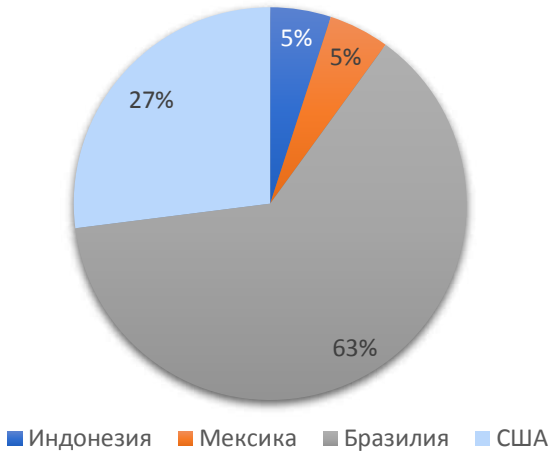
Банковский Процессинговый Центр

Мошеннические операции по поддельным карточкам:

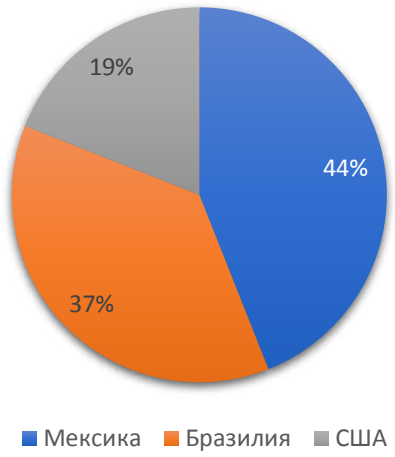
В 2023 году количество попыток мошеннических операций с использованием поддельных карточек увеличилось на 19% относительно 2022 года за счет проведения операций по сгенерированным карточкам с использованием магнитной полосы. Были зафиксированы случаи мошенничества по поддельным карточкам в АТМ в США, Бразилии и Индонезии (вероятно, компрометация произошла на территории Италии, Великобритании и Перу). В 2022 году был выявлен всего один неуспешный случай использования поддельной карточки в АТМ в США.

С использованием поддельных карточек в ОТС в 2023 году были выявлены случаи неуспешных попыток проведения мошенниками сгенерированных операций с использованием магнитной полосы в ОТС Бразилии, Мексики, случай неуспешной попытки оплаты с помощью бесконтактной технологии по поддельной карточке на территории Бразилии, а также случаи неуспешных попыток по поддельным карточкам в магазине спортивных товаров и медицинских услуг на территории США. В 2022 году мошенники преимущественно использовали генерацию магнитной полосы ОТС, зарегистрированных на территории Бразилии, Мексики, а также были выявлены случаи использования поддельной карточки в ресторане быстрого питания и в супермаркете на территории США.

Страны, в которых осуществлялись операции по поддельным карточкам банков в 2023 году



Страны, в которых осуществлялись операции по поддельным карточкам банков в 2022 году



Мошеннические операции с использованием реквизитов карточек:

Основными тенденциями мошенничества с использованием реквизитов карточек в 2023 году являются:

- мошенничество с применением методов социальной инженерии, обусловленное компрометацией реквизитов карточек клиентов преимущественно посредством взаимодействия мошенников с держателями на торговых площадках, фишинговых рассылок, а также scam звонков. Действия мошенников направлены на выманивание необходимых реквизитов карточек и персональных данных держателей с целью дальнейшего вывода средств, оформления кредитов. В 2023 году злоумышленники для вывода денежных средств по-прежнему преимущественно использовали платежные сервисы, которые зарегистрированы на территории Республики Беларусь, стали использовать инфокиоски в схемах с кредитами. В целом, в 2023 году наблюдалось общее снижение случаев мошенничества с использованием социальной инженерии в 1,3 раза относительно 2022 года;

- компрометация систем дистанционного банковского обслуживания клиентов посредством социальной инженерии. Особую ценность для злоумышленников имеют такие данные, как логины/пароли и доступы к системам ДБО, перехват которых способствует получению полного доступа к финансам держателя. Получение доступа к системам ДБО преимущественно осуществлялось путем установки злоумышленниками на мобильное устройство держателя программ удаленного доступа. Данный показатель вырос в 3,5 раза по сравнению с аналогичным показателем 2022 года;

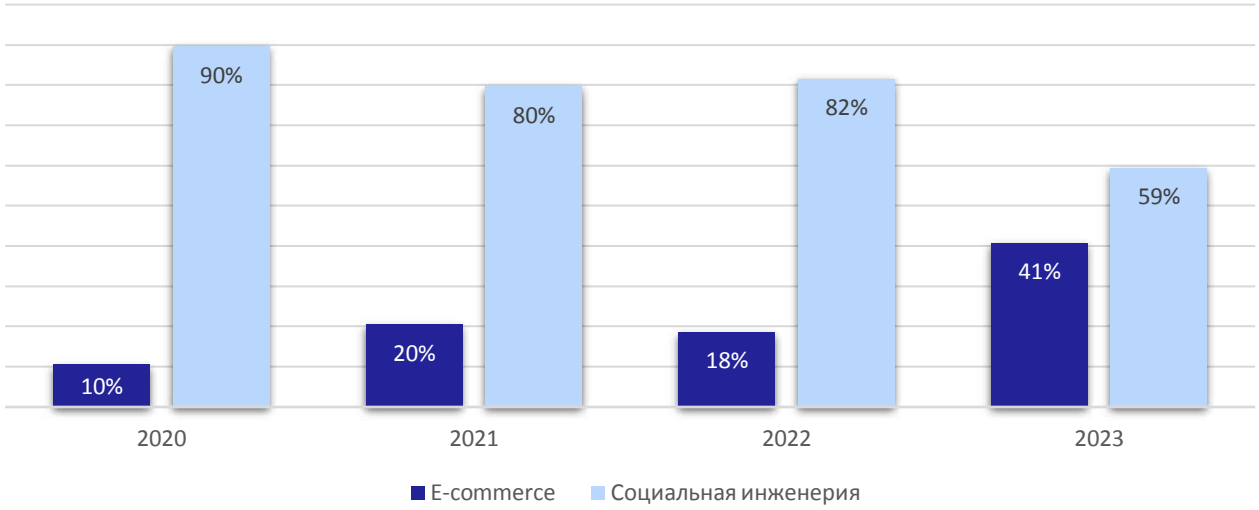
- мошенничество с использованием токенов. Количество случаев в отчетном периоде увеличилось в 29 раз по сравнению с 2022 годом. Злоумышленники посредством использования методов социальной инженерии, фишинговых рассылок выманивают у держателей необходимые данные и токенизируют карточку держателя на свое мобильное устройство, после чего совершают несанкционированные платежи с использованием заведенного электронного кошелька в интернет-магазинах, а также для оплаты в физических ОТС, расположенных на территории Таиланда, Японии, Италии, Мексики и т.д.;

- мошенничество, обусловленное компрометацией реквизитов карточек, взломами аккаунтов и учетных записей Google-сервисов реальных пользователей. Сервисы и интернет-ресурсы, на которых осуществлялись мошеннические операции, преимущественно зарегистрированы на территории США, что объясняет в 2023 году высокую долю операций с использованием реквизитов карточек в ОТС, зарегистрированных на территории США;

- тестовые операции и атаки на БИНы банков (сгенерированные номера карточек) с целью выявления реальных карточек для дальнейшего использования их реквизитов в мошеннических целях. Для тестовых операций в 2023 году чаще использовались ОТС, зарегистрированные на территории США и Великобритании;

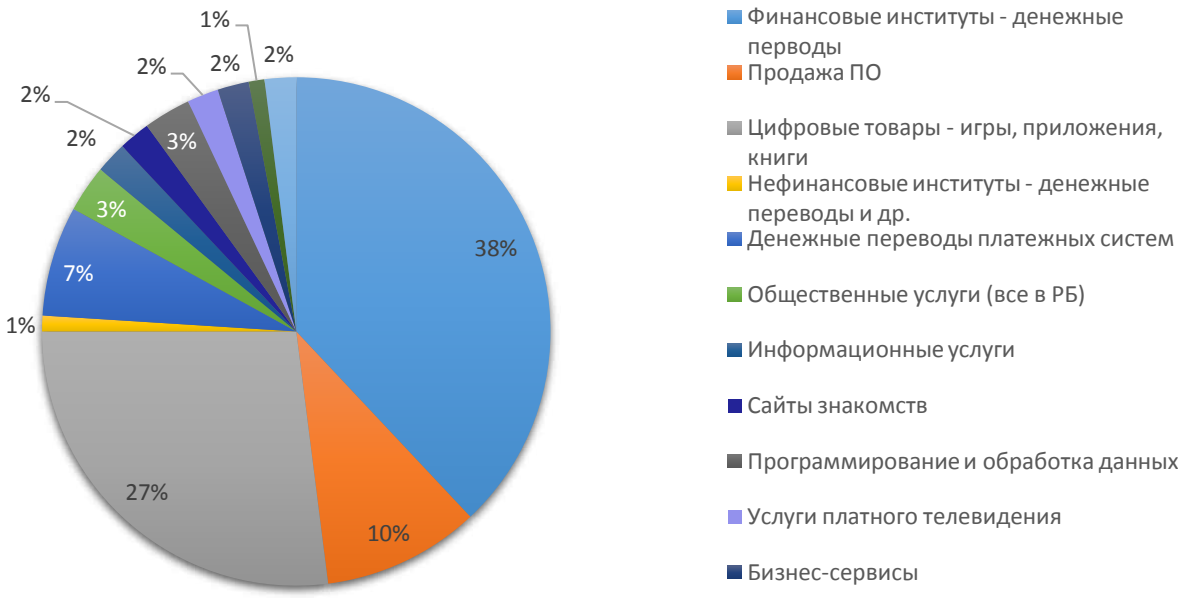
- присутствие фактов «friendly fraud» мошенничества, при котором владелец карточки либо его родственники/знакомые оплачивают товар или услугу, получают его/ее, пользуются, а затем намеренно инициируют возврат платежа, утверждая, что данные их карточки были скомпрометированы.

Виды мошенничества CNP, %

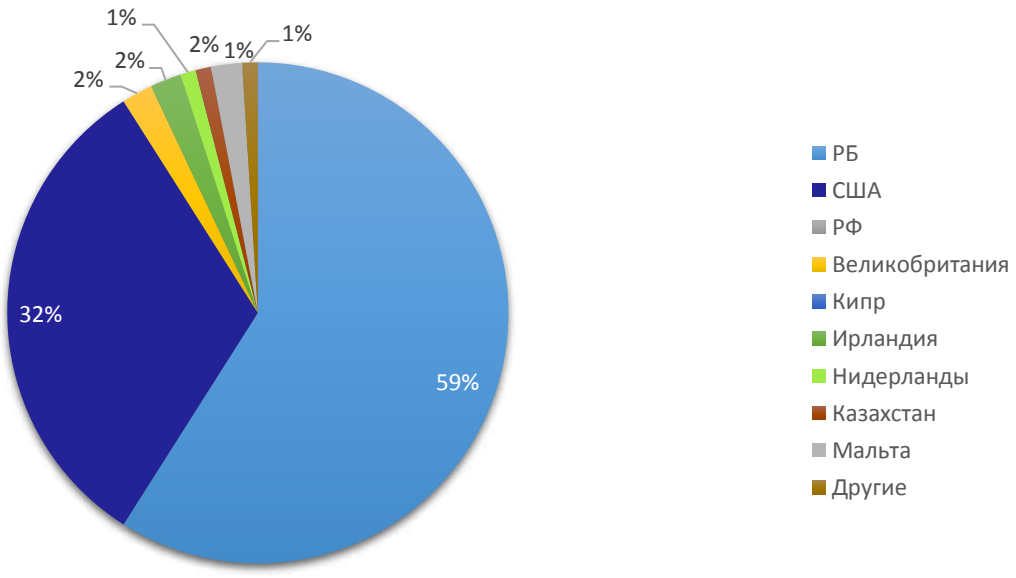


В каких ОТС (категориях ОТС) осуществлялись мошеннические операции с использованием реквизитов карточек в 2023 году

В каких ОТС (категориях ОТС) осуществлялись мошеннические операции с использованием реквизитов карточек в 2022 году

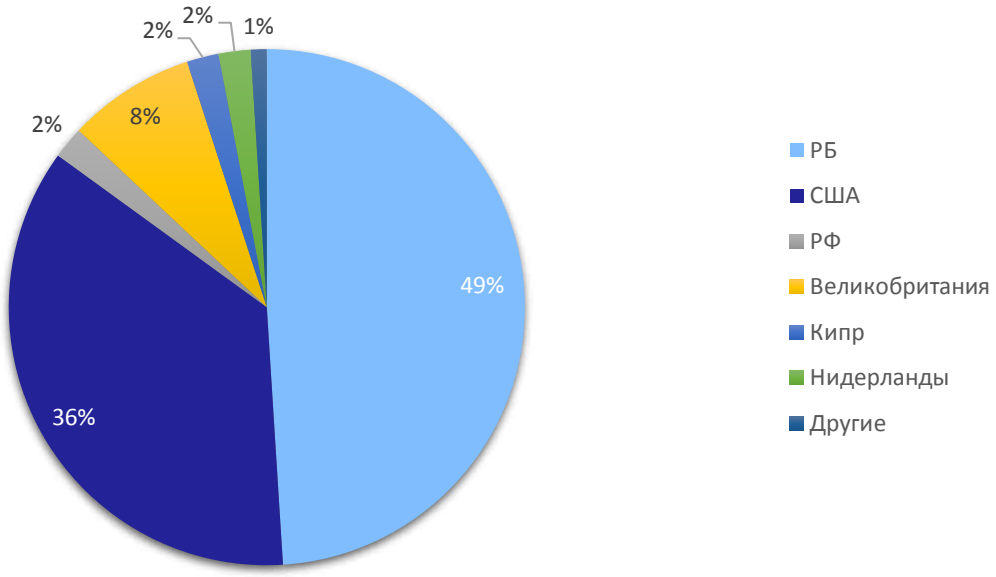


Страны, в которых осуществлялись мошеннические операции с использованием реквизитов карточек в 2023 году



Банковский Процессинговый Центр

Страны, в которых осуществлялись мошеннические операции с использованием реквизитов карточек в 2022 году



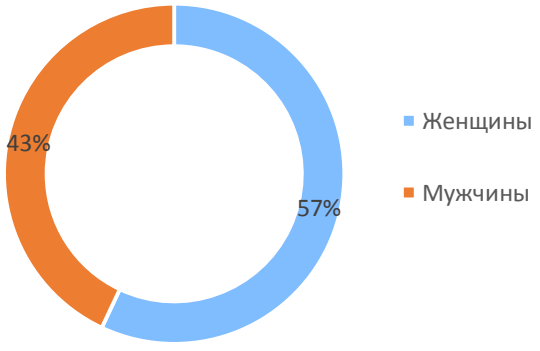
Статистика держателей, подвергшихся мошенничеству:

Согласно аналитическим данным ОАО «Банковский процессинговый центр» в 2023 году более доверчивыми оказались женщины - 57% случаев. В 16% случаев жертвами злоумышленников стали держатели, проживающие в городе Минске, а 84% случаев мошенничества приходится на проживающих в других регионах Беларуси.

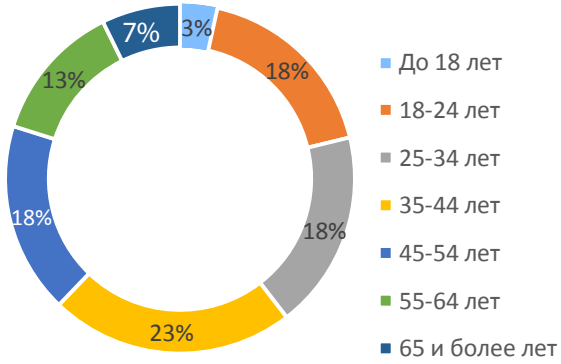
В 89% случаев мошенничество направлено на экономически активных граждан в возрасте от 18 до 64 лет, 7% – на держателей старше 65 лет, 3% атак пришлось на держателей младше 18 лет.

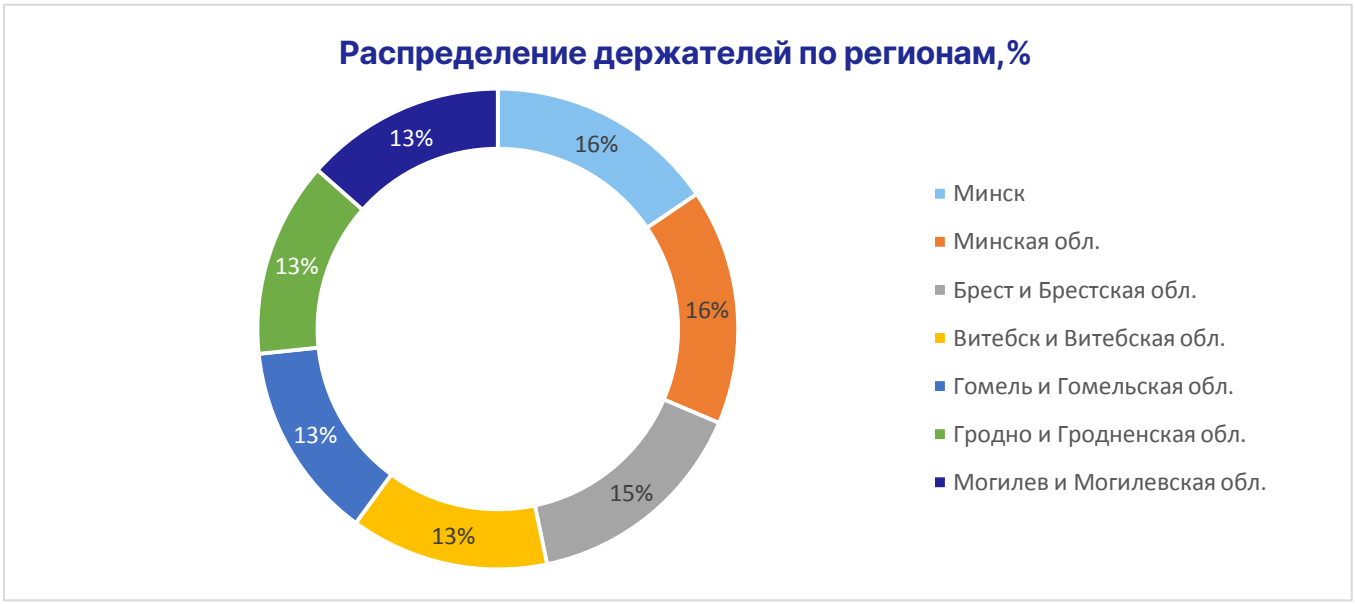
Детальная информация представлена на диаграммах.

Распределение держателей по половому признаку, %



Распределение держателей по возрасту, %





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

В 2023 году общее количество рекламаций эмиссии увеличилось в 1,5 раза относительно 2022 года, что обусловлено скачком мошеннических операций в иностранных ОТС, осуществляющих деятельность по продаже цифровых товаров и услуг, онлайн-казино, а также в специализированных розничных магазинах широкой направленности.

В 2023 году рекламации по причинам оспаривания распределились следующим образом:

85,8% от общего количества рекламаций были инициированы по причине мошенничества (74,4% в 2022 году);

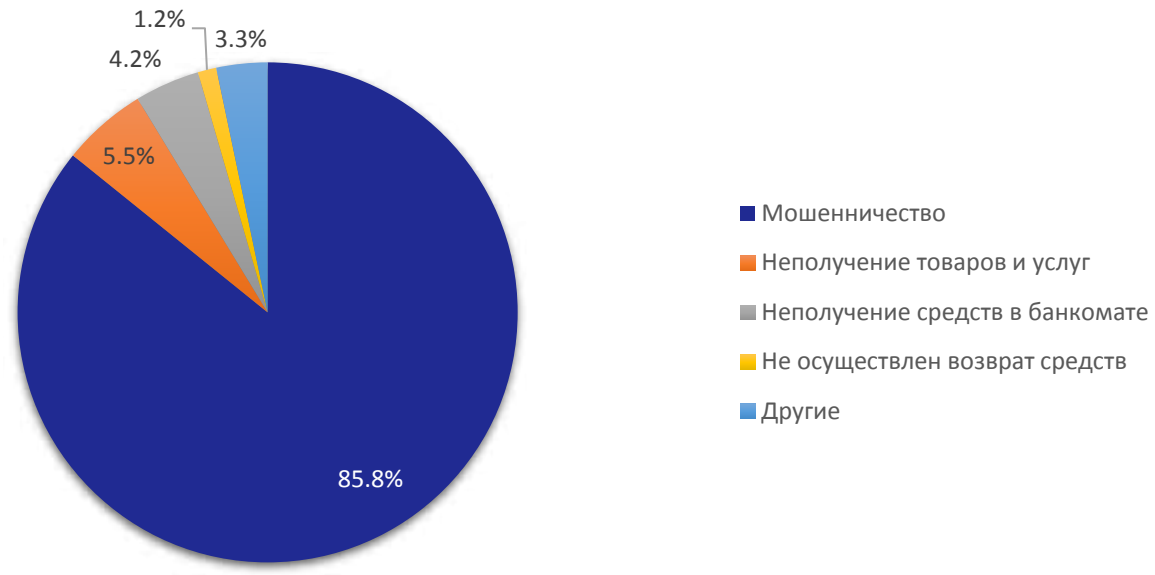
5,5% составляют операции, оспоренные по причине неполучения держателем карточки товаров/услуг (10,5% в 2022 году);

4,2% приходится на долю рекламаций по операциям неполучения денежных средств в банкоматах (6,4% в 2022 году). В основном это операции, проводившиеся в банкоматах Египта, Грузии, Испании и ОАЭ;

1,2% - операции, оспоренные по причине неполучения возврата денежных средств (2,3% в 2022 году);

3,3% от общего количества оспоренных операций составили остальные виды рекламаций (4,1% в 2022 году).

Распределение рекламаций по причинам оспаривания в 2023 году (эмиссия, %)



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

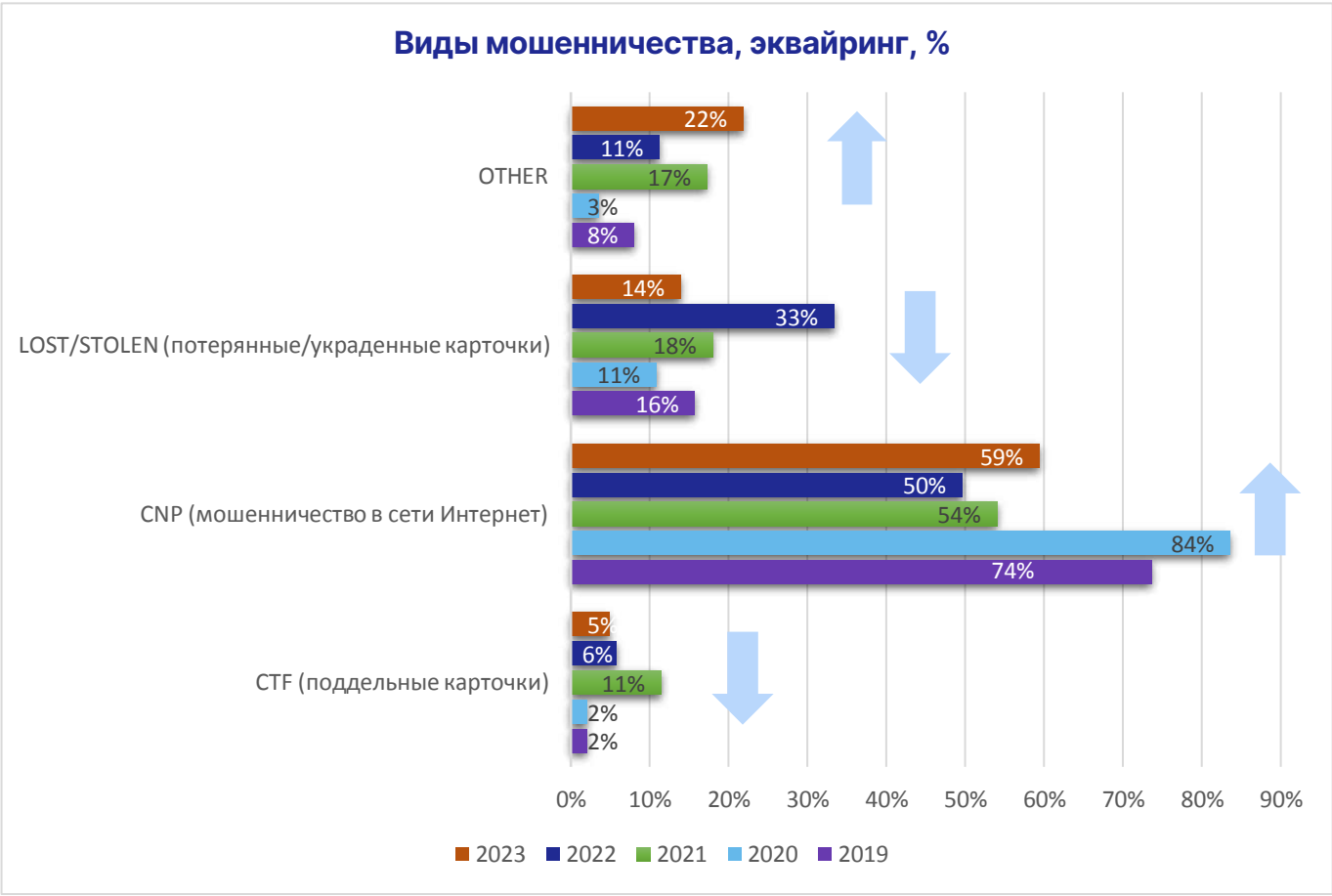
В 2023 году в 2,3 раза увеличилось количество операций мошеннического характера в эквайринговой сети банков, которые обслуживаются в ОАО «Банковский процессинговый центр». Из них 59% составляют мошеннические операции **без присутствия карточки, 22% - другие виды мошенничества:** 93% составляет мошенничество с перехватом данных держателей и мошенничество, связанное с манипуляцией владельцем счёта; 6% - мошенничество, связанное с выпуском карточки по поддельным данным; 1% - incorrect processing – на стороне эмитента были спроцессированы некорректные параметры (заявленные операции прошли по признаку бесконтактных операций), 14% приходится на долю мошеннических операций **по утерянным/украденным карточкам** и **5%** приходится на мошеннические операции с использованием **поддельных карточек.**

Мошеннические операции **без присутствия карточки** в 54% случаев прошли с использованием реквизитов карточки в среде e-commerce, 30% - это операции с использованием 3-D Secure, 9% - COF-транзакции и 7% в ОТС с физическим использованием карточки.

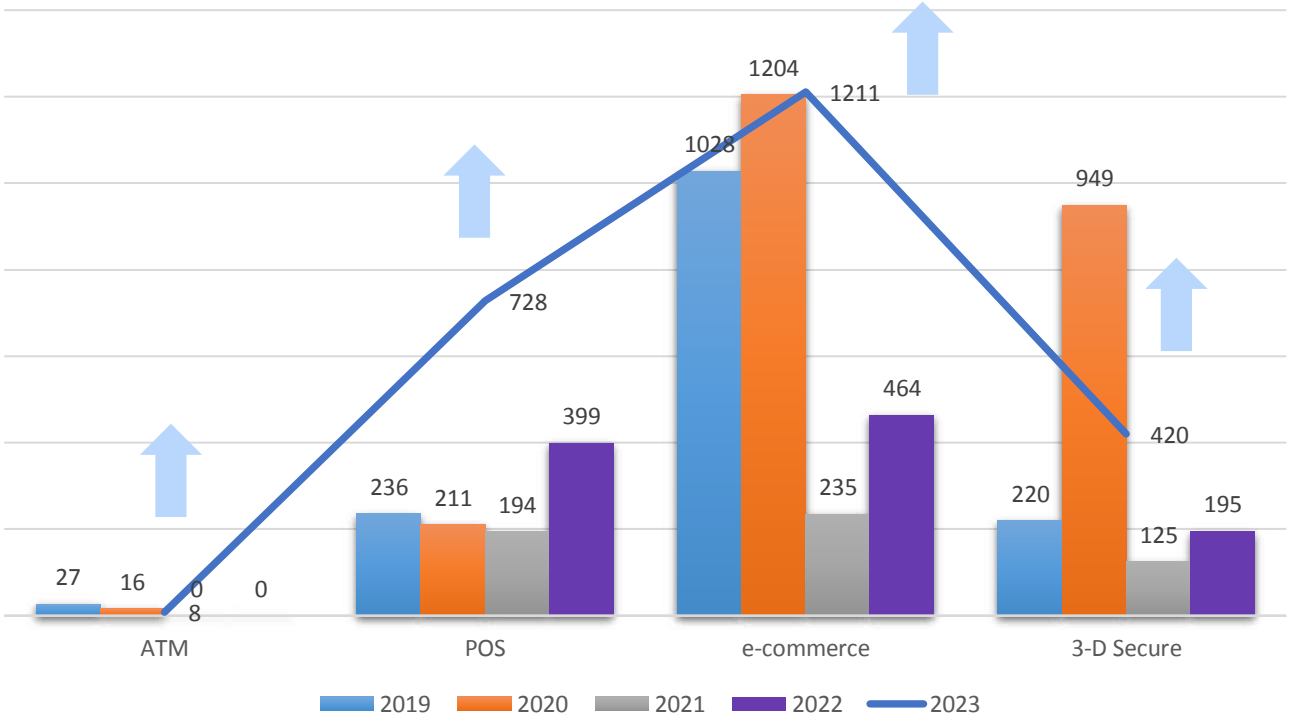
Мошеннические операции **по утерянным/украденным карточкам** в 85% случаев были осуществлены с признаком проведения бесконтактных операций, 13% пришлось на операции с использованием реквизитов карточек, в 2% случаев осуществлялись с использованием EMV технологии. Бесконтактные операции позволяют мошенникам совершать большое количество операций в рамках установленных лимитов без необходимости подтверждения совершения операции ПИН-кодом либо использования других методов подтверждения операции.

Мошенничество **по поддельным карточкам** в 82% случаев проходило по бесконтактному признаку, 18% из заявленных операций прошли с использованием реквизитов карточек. В 2023 году в эквайринговой сети банков не было зафиксировано ни одного реального случая использования поддельных карточек.

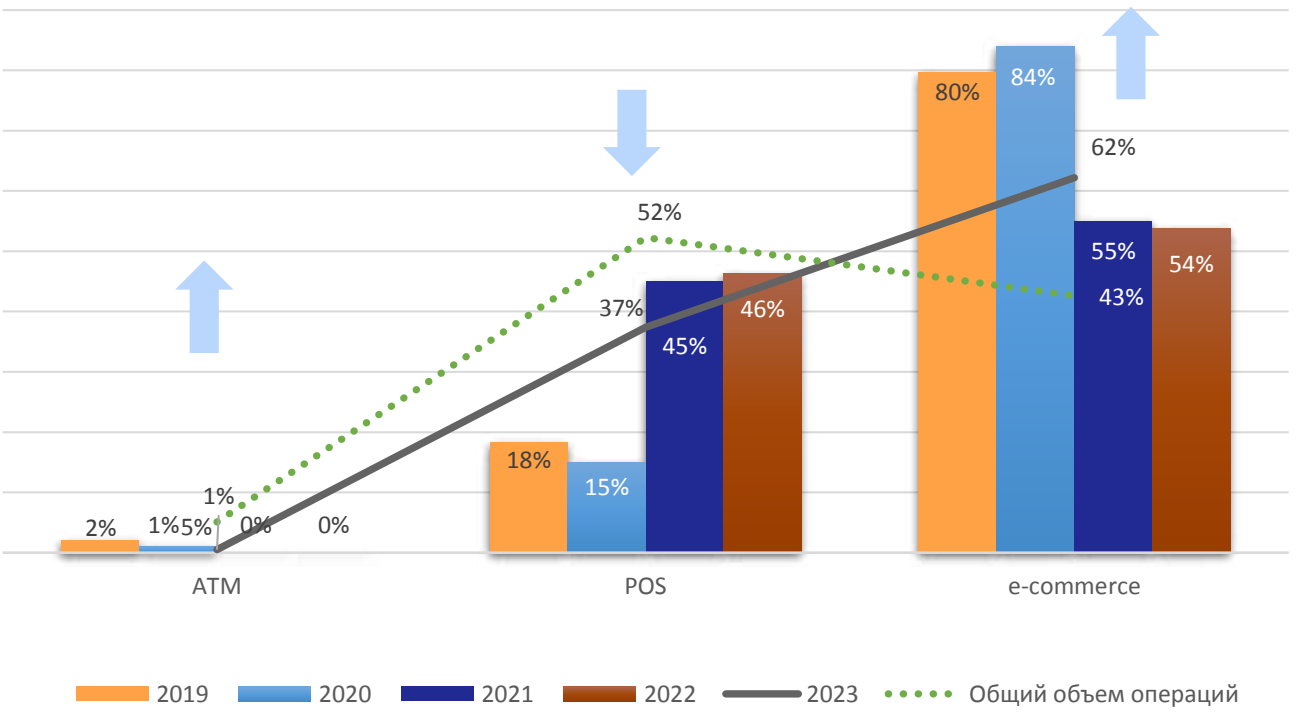
Общая сумма успешных мошеннических операций по сравнению с 2022 годом увеличилась на 134%, средняя сумма 1 мошеннической операции составила 87 долларов США (84 доллара США в 2022 году). Увеличение количества и суммы успешных мошеннических операций обусловлено ростом мошеннических операций в среде без присутствия карточки (на 170% в 2023 году относительно 2022 года). В целом, развитие информационных технологий, совершенствование систем защиты банкоматов, постепенный выход из оборота карточек только с магнитной полосой, а также незначительные затраты злоумышленников при мошенничестве в среде без присутствия карточки значительно снижают привлекательность мошенничества с использованием поддельных карточек.



Количество мошеннических операций в разрезе мест их совершения (эквайринг, условные едицы)



Количество мошеннических операций в разрезе мест их совершения (эквайринг, %)



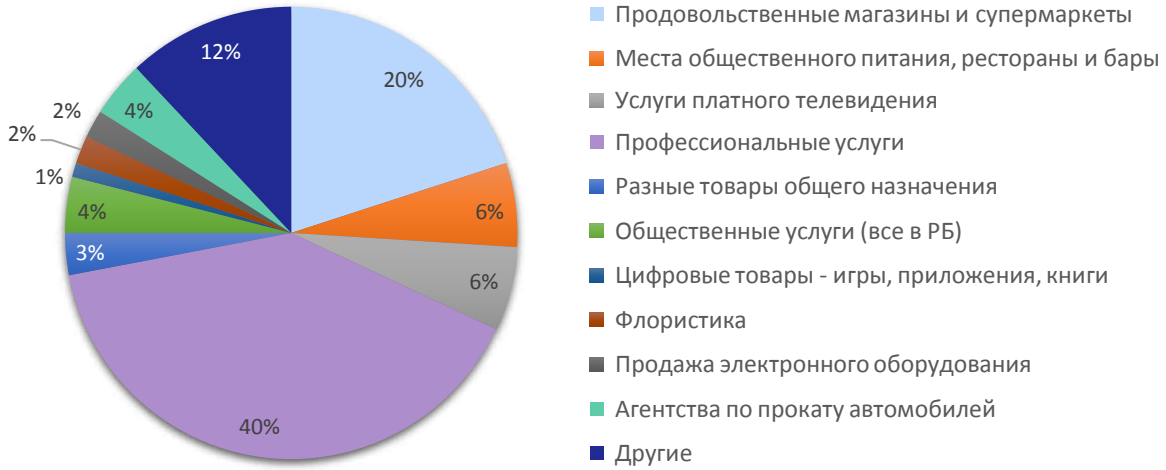
Банковский Процессинговый Центр

Рейтинг MCC, в которых осуществлялись мошеннические операции в эквайринге по количеству, распределился следующим образом: 40% на профессиональные услуги; 20% мошеннических операций прошли в продовольственных магазинах и супермаркетах; по 6% в сфере общественного питания, барах и ресторанах и услуги платного телевидения; по 4% пришлось на общественные услуги и агентства по прокату автомобилей; 3% - разные товары общего назначения; по 2% в сфере флористики и ОТС, занимающихся продажей электронного оборудования; 1% - ОТС, осуществляющие реализацию цифровых товаров - игр, приложений, книг и 12% - другие ОТС.

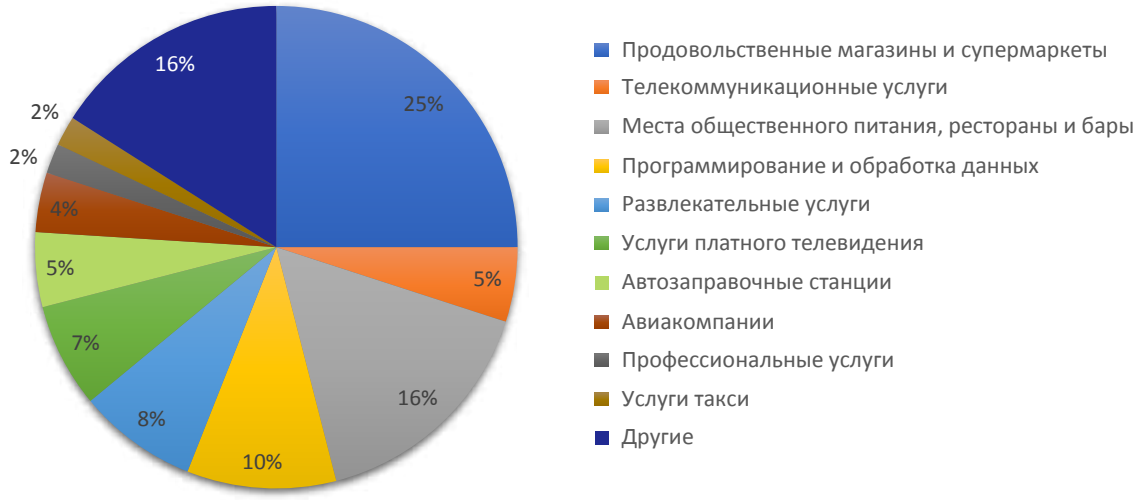
Наиболее часто в 2023 году в эквайринговой сети в мошеннических целях использовались карточки банков, эмитированных банками России, США и Канады.

В 2023 году по карточкам платежной системы UnionPay International в эквайринговой сети не было зафиксировано ни одной мошеннической операции.

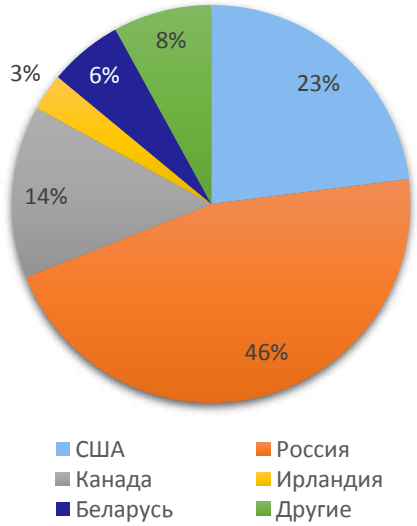
В каких ОТС (категориях ОТС) осуществлялись мошеннические операции в эквайерской сети по карточкам банков-нерезидентов в 2023 году



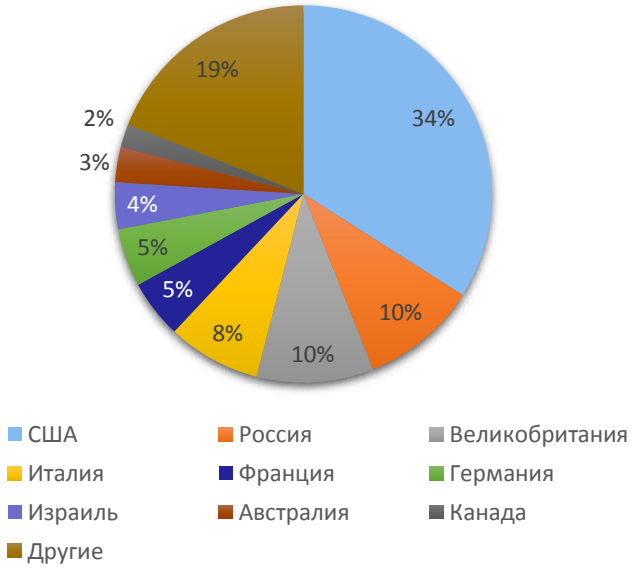
В каких ОТС (категориях ОТС) осуществлялись мошеннические операции в эквайерской сети по карточкам банков-нерезидентов в 2022 году



Страны банков-эмитентов, по карточкам которых проходили мошеннические операции в эквайринговой сети в 2023 году



Страны банков-эмитентов, по карточкам которых проходили мошеннические операции в эквайринговой сети в 2022 году



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

В 2023 году в 11,5 раз возросло количество эквайерских рекламаций относительно 2022 года. Увеличение количества обработанных рекламаций между отчетным периодом и показателем 2022 года обусловлено большим количеством входящих операций опротестования по причине нарушения технологии проведения операций.

В 2023 году рекламации по причинам оспаривания распределились следующим образом:

47,1% - нарушение технологии проведения операций (0,9% в 2022).

35,8% оспоренных операций относятся к операциям неполучения товаров и услуг (28,5% в 2022 году). Рекламации поступали по операциям, совершенным в таких торговых точках, как авиакомпании, гостиницы, магазины доставки цветов.

12% от общего количества рекламаций были оспорены по причине мошенничества (25,8% в 2022 году).

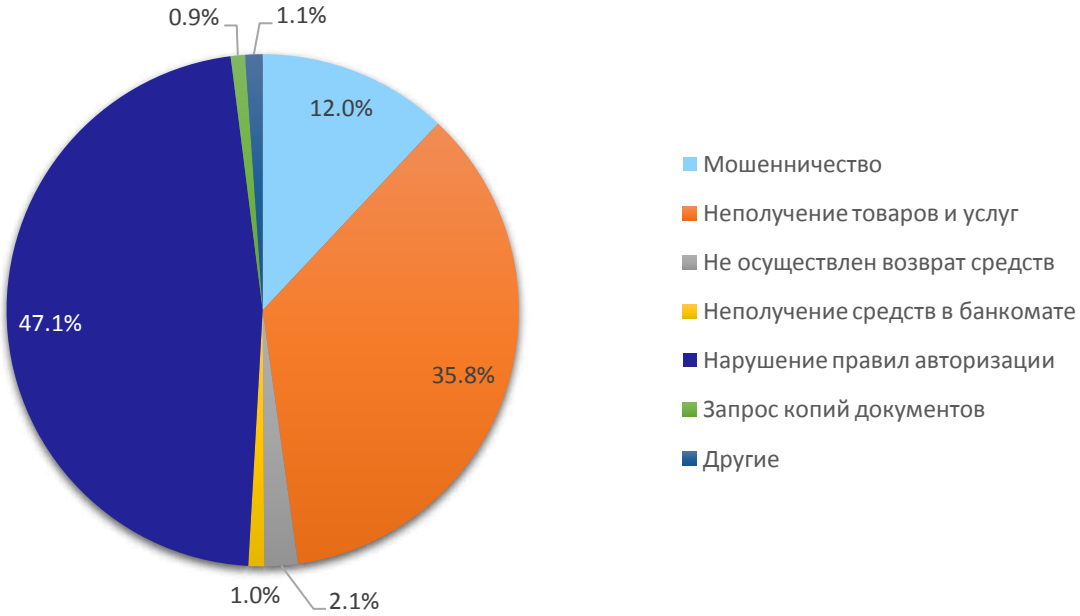
2,1% – не получен возврат денежных средств (10,6% в 2022 году).

1% от общего числа рекламаций составили операции, оспоренные по причине неполучения денежных средств в банкомате (18,1% в 2022 году).

0,9% – запросы копий документов, подтверждающих совершение операций (1,8% в 2022 году).

1,1% от общего количества оспоренных операций приходится на остальные виды рекламаций единичного характера (14,3% в 2022 году).

Распределение рекламаций по причине оспаривания в 2023 году (эквайринг, %)



ПРОГНОЗ:

Принимая во внимание получившие распространение схемы мошенничества в 2023 году, характерными для 2024 года будут:

• **Социальная инженерия.** Мошенничество с использованием методов социальной инженерии, как и в предыдущие годы, останется доминирующей угрозой. Многообразие форм данного вида мошенничества всегда дает быстрый и эффективный результат. Злоумышленники используют различные каналы связи: телефонные звонки, мессенджеры, социальные сети, просят пользователя установить на мобильный телефон средство удаленного управления. Популярная форма социальной инженерии 2023 года - убеждение жертв взять кредит, продать недвижимость и перевести все денежные средства на счета злоумышленников будет актуальной и в 2024 году. Мошенники очень изобретательны, подстраиваются под любые изменения и используют новостные повестки в своих целях. Подобные способы мошенничества будет использоваться пока держатели не начнут действовать более осознанно и с разумной осторожностью относиться к любым сообщениям и входящим звонкам.

• **Перехват доступа к СДБО и МСИ.** Мошенничество, которое позволяет злоумышленникам получить полный доступ ко всем платёжным инструментам и счетам держателя. Возможность открытия виртуальных, дебетовых и кредитных карточек с доставкой почтой, кредитных продуктов онлайн делает данный вид мошенничества очень привлекательным. Серьезной угрозой останутся программы удаленного доступа, которые мошенники все чаще устанавливают на мобильные устройства держателей и посредством их получают доступ к любым приложениям и особенно к СДБО.

• **Мошенничество с использованием токенов.** Тема токенизации и использование токенов в рамках социальной инженерии также будут актуальными в 2024 году. Ухищренные схемы злоумышленников позволяют манипулировать держателями, получать необходимые реквизиты и данные, чтобы использовать токены на своих мобильных устройствах для совершения несанкционированных операций. Развитие NFC технологии является дополнительным фактором, позволяющим мошенникам не только оплачивать товары в сети интернет и ОТС, но и снимать наличные в банкоматах.

• **БИН-атаки и генерация номеров карточек.** Это серьезная проблема, которая затрагивает эмитентов, продавцов и эквайеров по всему миру. При данных видах мошенничества злоумышленник проверяет активность карточки с целью ее использования в незаконных целях или продажи. Обычно эти атаки фокусируются на одном диапазоне BIN. Киберпреступники используют программные средства для генерации номеров карточек, а атаки осуществляют в торговых точках электронной коммерции, которые имеют слабые механизмы контроля за мошенничеством.

• **Использование искусственного интеллекта.** Злоумышленники всегда для достижения своих целей используют новейшие цифровые разработки. Использование искусственного интеллекта повышает эффективность вредоносного программного обеспечения, позволяет обходить механизмы защиты, подбирать пароли, анализировать большие массивы данных с целью извлечения номеров телефонов и банковских платежных карточек в мошенничестве, связанном с социальной инженерией. Мошенники будут использовать искусственный интеллект для создания более качественных поддельных изображений, дипфейков, которые смогут обмануть кого угодно, для создания мощных ботов в целях атак.

• **Фишинговые атаки.** Фишинговые рассылки и сайты всё сложнее отличить от легитимных. Поддельные сайты часто бывает сложно внешне отличить от оригинальных, что усложняет задачу для держателей по их выявлению. Количество фишинговых сайтов белорусских крупных банков и платёжных ресурсов увеличилось кратно. Злоумышленники стараются приурочить фишинговые кампании к громким событиям и инфоповодам, это означает, что объемы их атак будут лишь нарастать в 2024 году.

• **Использование JavaScript-снифферов в e-commerce.** Для онлайн-торговли по-прежнему угрозу представляют JavaScript-снифферы. Пользователи онлайн-магазинов зачастую являются самым слабым звеном системы безопасности. Вводя свои платежные данные, они подвергаются риску их компрометации. JS-сниффер - это онлайн-аналог скиммера. Но если скиммер - миниатюрное устройство, которое перехватывает данные карточки пользователя в банкомате, то JS-сниффер - это несколько строк кода, который внедряется злоумышленниками на сайт для перехвата вводимых пользователем данных.

• **Мошенничество с подписками на игры и хищение аккаунтов.** В большинстве современных игр есть тот или иной способ монетизации: от продажи внутри игровых предметов и бустеров до внутри игровой валюты. Разумеется, все это привлекает киберпреступников, ведь игровые ценности можно продать за реальные деньги. Именно поэтому злоумышленники так активно охотятся за аккаунтами геймеров, поэтому велика вероятность появление новых схем, связанных с перепродажей виртуальных валют и имущества через хищение аккаунтов реальных пользователей.

• **Система мгновенных платежей (СМП) и QR-платежи.** Развитие любых новых сервисов всегда привлекает интерес у злоумышленников, не станут исключением и сервисы СМП и QR-платежи. Привязка номера телефона к счетам злоумышленников, подмена QR-кода и т.д. будут использоваться мошенникам для хищения денежных средств.

Многие схемы мошенничества 2023 года не оказались новыми, при этом они видоизменились и подстроились под текущую ситуацию в мире, а новые технологии повлекли за собой и новые идеи мошенников, направленные на хищение денежных средств. Принимая во внимание сложившиеся тенденции, всем участникам финансового рынка не стоит ожидать значительного снижения уровня мошенничества в безналичной среде в 2024 году.