БАНКОВСКИЙ ПРОЦЕССИНГОВЫЙ ЦЕНТР

ОТЧЕТ

о тенденциях и случаях мошенничества в сфере банковских платежных карточек за 1 полугодие 2020 года

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:

Уровень мошенничества на территории Республики Беларусь с использованием скимминговых устройств по-прежнему является стабильно низким.

Единственный случай установки скимминговых устройства за 1 полугодие 2020 года был зафиксирован в июне месяце на банкомате в городе Могилеве. По информации от правоохранительных органов мошенники были задержаны на месте преступления, утечки карточных данных не было, благодаря чему удалось избежать финансовых потерь, связанных со снятием денежных средств по поддельным карточкам.

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

В 1 полугодии 2020 года основная доля мошеннических операций приходится на мошенничество с использованием реквизитов карточек наряду со значительным снижением количественных показателей мошенничества с использованием поддельных карточек и отсутствием случаев мошенничества по утерянным/украденным карточкам.

Самой актуальной проблемой остается мошенничество с использованием методов социальной инженерии. В настоящее время подавляющая часть финансовых потерь от карточного мошенничества приходится на хищения с применением социальной инженерии. Мошенники пользуются доверчивостью и недостаточной финансовой грамотностью граждан, выманивают реквизиты карточек держателей, их персональные данные и совершают противоправные действия, направленные на хищение денежных средств. Следует отметить, что появились схемы социальной инженерии, основанные на манипуляциях угрозой распространения коронавирусной инфекции COVID-19. Держатели получают фишинговые письма или сообщения в социальных сетях, связанные с угрозой распространения коронавирусной инфекции COVID-19, целью которых является получение конфиденциальных данных держателей и последующее хищение их денежных средств. Также значительно увеличилось количество случаев мошенничества с использованием различных торговых платформ, когда злоумышленники под видом покупателя обращаются к частному продавцу, обещая перевести на его карточку оплату за товар. При этом направляют продавцу ссылку на поддельную страницу интернет-банкинга, где ничего не подозревающий держатель вводит данные от своего интернет-банкинга, а в это время злоумышленники перехватывают доступ к учетной записи пользователя и его личному кабинету, после чего переводят на подконтрольные мошенникам счета все доступные средства владельца; либо злоумышленник выманивает в мессенджерах или социальных сетях у держателя необходимые реквизиты карточки и присылает фишинговую ссылку для ввода пароля 3D Secure, после чего с карточки держателя происходит несанкционированное списание денежных средств.

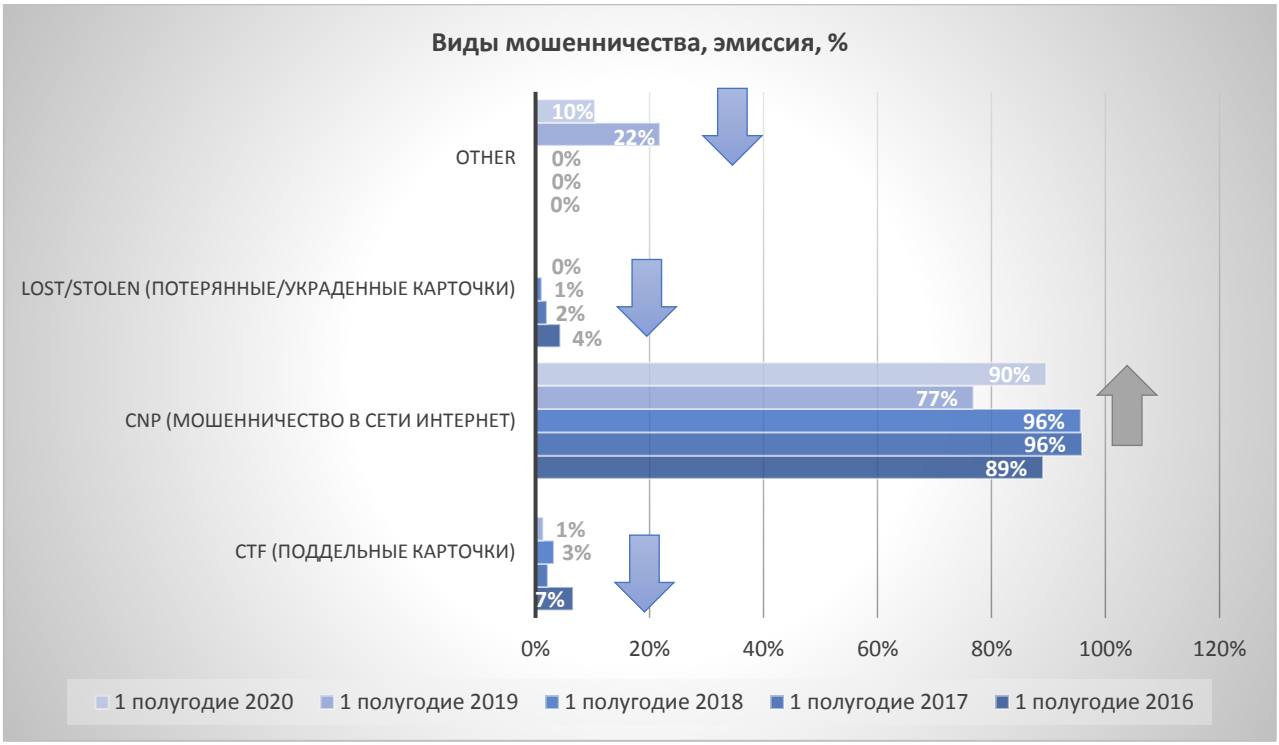
По итогам 1 полугодия 2020 года количество мошеннических операций по карточкам банков, которые обслуживаются в ОАО «Банковский процессинговый центр», по типу мошенничества распределилось следующим образом: **90%** мошеннических операций приходится на мошенничество **с использованием реквизитов карточек**, **10%** незаконных операций с банковскими платежными карточками приходится на **account takeover,** случаев мошеннических операций с использованием **утерянных/украденных карточек** не зарегистрировано.

в 1 полугодии 2020 года по **поддельным карточкам** не было зафиксировано ни одной успешной операции, все мошеннические попытки были выявлены работниками ОАО «Банковский процессинговый центр» в результате срабатывания правил мониторинга системы Fraud Management. Следует отметить общую тенденцию снижения случаев использования поддельных карточек, что соответствует общемировой миграции мошенничества в среду в сферу e-commerce и операций без присутствия карточки, что привлекает злоумышленников в первую очередь незначительными затратами для осуществления мошеннических действий. Также необходимо принять во внимание закрытие границ в связи с распространением коронавирусной инфекции COVID-19, что ограничивает географическое передвижение как злоумышленников, так и самих держателей, тем самым исключая возможность трансграничного мошенничества с использованием поддельных карточек.

В 1 полугодии 2020 года в 6,7 раза увеличилось количество мошеннических операций по сравнению с аналогичным периодом 2019 года, при этом общая сумма мошеннических операций увеличилась в 2 раза, а средняя сумма 1 мошеннической операции составила 11 долларов США (34 доллара США в 1 полугодии 2019 года). Небольшое значение средней суммы мошеннических операций обусловлено растущим интересом злоумышленников к осуществлению мошеннических операций в среде e-commerce и операций без присутствия карточки, а также значительным количеством несанкционированных операций на Google сервисах, где совершается большое количество попыток проведения оплат, но на небольшие суммы в рамках баланса счетов держателей.

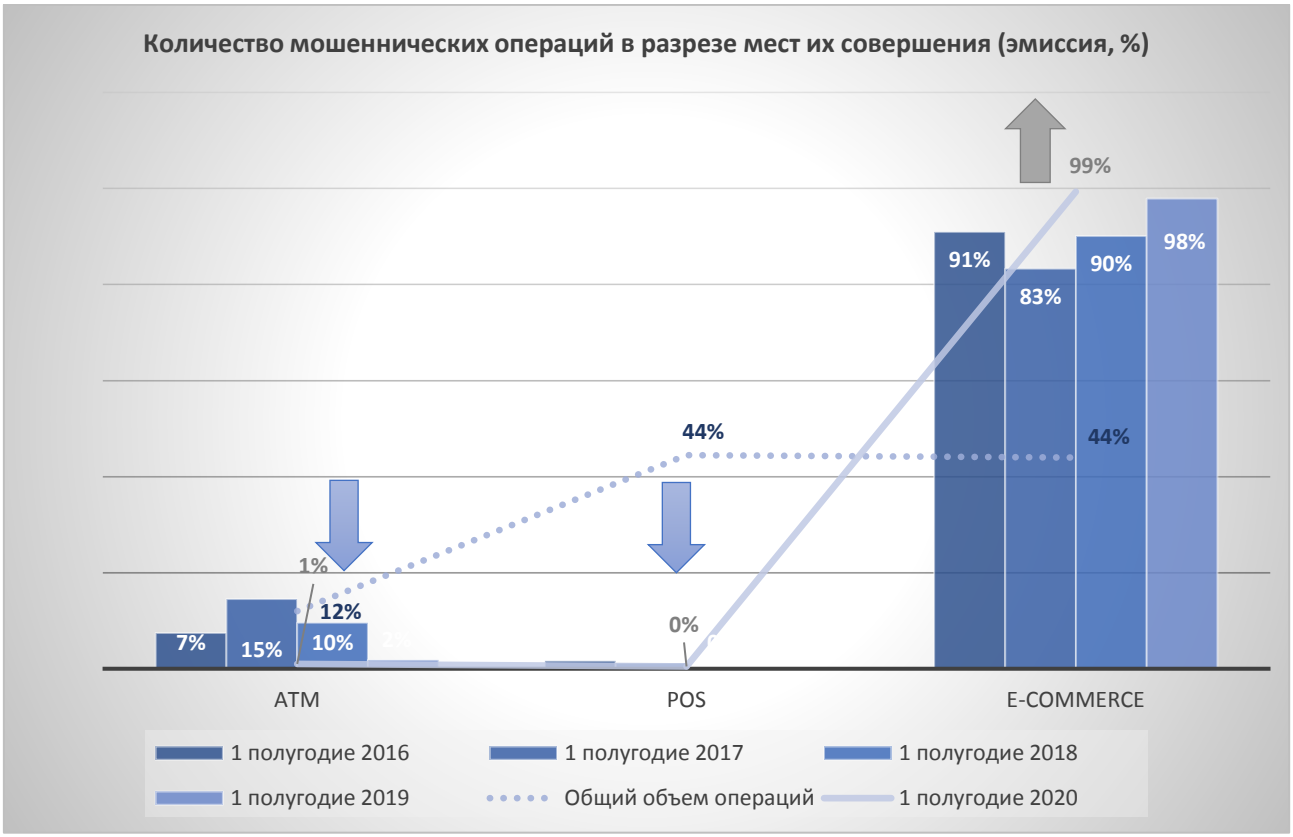
Также в 1 полугодии 2020 года можно отметить устойчивую тенденцию роста мошенничества с использованием технологии 3D Secure (в 3,5 раз больше по сравнению с 1 полугодием 2019 года). Данный показатель свидетельствует о значительной доле мошеннических операций, обусловленных использованием методов социальной инженерии, когда мошенникам становятся доступны все необходимые для осуществления платежей/переводов реквизиты, в том числе и пароли 3D Secure. Также участились случаи, когда злоумышленники получают доступ к системам дистанционного банковского обслуживания держателей, в результате чего получают возможность управлять счетами и карточками банковских клиентов.

Детальная информация о тенденциях мошенничества представлена на диаграммах ниже.



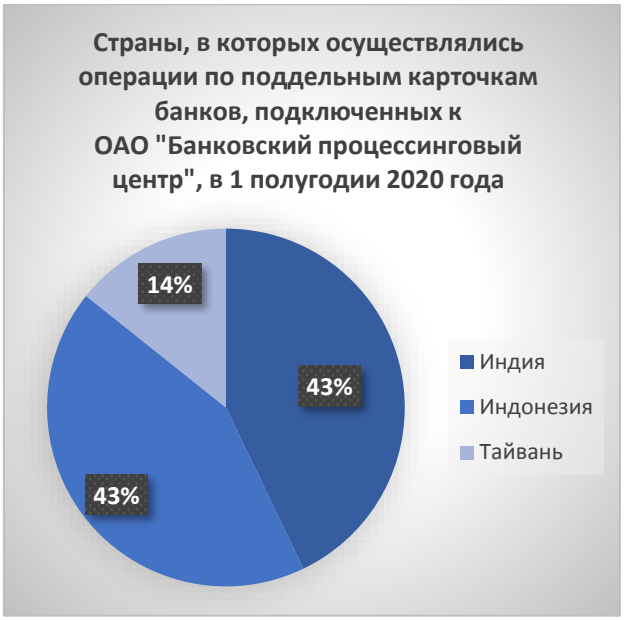

Количество мошеннических операций в разрезе видов
(эмиссия, условные единицы)
50
28
0
38
19
674
1247
1127
1076
8383
0
0
0
0
0
972
305
CTF
CNP
LOST/STOLEN
OTHER
1 полугодие 2016
1 полугодие 2017
1 полугодие 2018
1 полугодие 2019
1 полугодие 2020

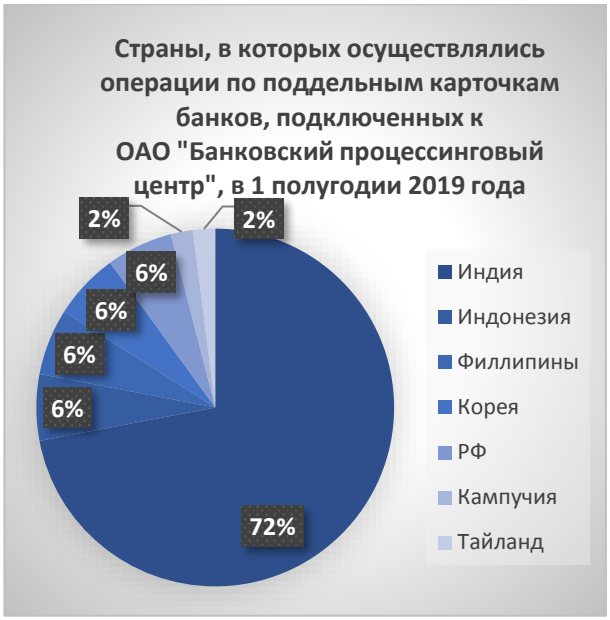

Количество мошеннических операций в разрезе мест их совершения
(эмиссия, условные единицы)
23
60
7
63
36
18
281
344
592
1900
3721
2026
0
4
29
578
ATM
POS
E-COMMERCE
3-D SECURE
1 полугодие 2016
1 полугодие 2017
1 полугодие 2018
1 полугодие 2019
1 полугодие 2020

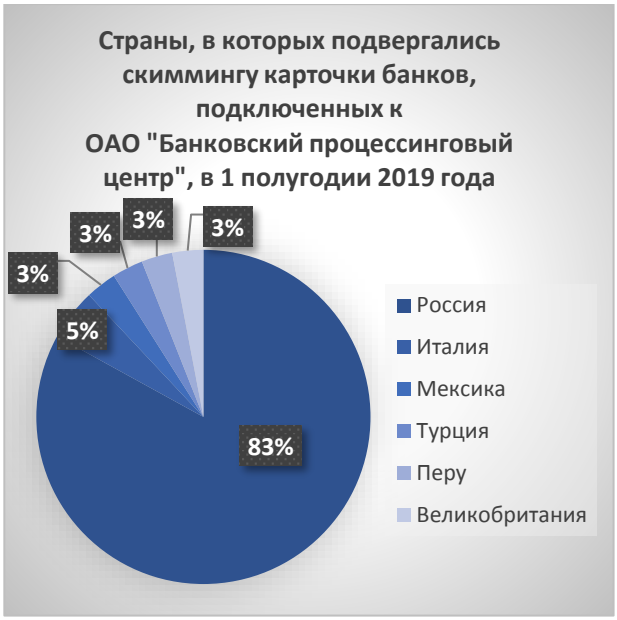


Операции с поддельными карточками:

Общей тенденцией 1 полугодия 2020 года является значительное уменьшение мошеннических операций с использованием поддельных карточек. Так по сравнению с аналогичным периодом 2019 года мошенничество по поддельным карточкам снизилось в 5 раз. Если еще в 1 квартале 2020 года были случаи использования поддельных карточек в таких странах, как Индия (43% случаев), Индонезия (43% случаев) и Тайвань (14% случаев) после компрометации в Великобритании (г. Лондон) – 29% случаев, Российской Федерации (29% случаев), в частности, в г. Санкт-Петербург, в Австрии, Турции и Индонезии – по 14% случаев, то в 2 квартале 2020 года не было выявлено ни одного реального случая использования поддельных карточек. Работниками ОАО «Банковский процессинговый центр» фиксировались сгенерированные попытки проведения мошеннических операций с имитацией использования магнитной полосы, чипа и бесконтактных операций по карточкам в ОТС Бразилии.







Мошеннические операции с использованием реквизитов карточек:

Основными тенденциями мошенничества с использованием реквизитов карточек в 1 полугодии 2020 года являются:

мошенничество с использованием методов социальной инженерии, обусловленное компрометацией карточных данных держателей посредством фишинга, вишинга, а также взлома учетных записей пользователей в социальных сетях. Наблюдался всплеск звонков мошенников от имени банков с целью получения реквизитов карточек держателей после утечки данных на маркетплейсе «Joom», создание поддельных сайтов, имитирующих СДБО банков, выманивание необходимых реквизитов от имени покупателя при размещении объявлений на общедоступных ресурсах по продаже товаров с дальнейшим выводом средств через различные финансовые и нефинансовые институты, зарегистрированные на территории Республики Беларусь, Российской Федерации, Украины и Казахстана;

присутствие фактов компрометации систем дистанционного банковского обслуживания клиентов в рамках социальной инженерии. Особую ценность для злоумышленников имеют такие данные, как логины/пароли и ключи доступа к СДБО, перехват которых способствует установлению полного контроля со стороны мошенников над финансами держателя;

мошенничество по токенам, когда злоумышленники с использованием методов социальной инженерии выманивают у держателей данные, необходимые для присвоения токена карточке, в результате чего мошенники привязывают токен карточки держателя на свое мобильное устройство и совершают несанкционированные платежи в сети интернет с использованием заведенного электронного кошелька. Данный способ мошенничества является относительно новым и свидетельствует о необходимости рассмотрения возможности внедрения дополнительных способов аутентификации в процессе привязки токена к мобильному устройству;

наличие значительного количества мошеннических операций на онлайн-сервисах, которые занимаются продажей цифровых товаров: компьютерных программ и игр. Актуальной тенденцией по-прежнему является взлом аккаунтов Google, после чего злоумышленники осуществляют большое количество операций оплаты Google сервисов на мелкие суммы в пределах баланса счета держателей. Указанные сервисы, как правило, зарегистрированы на территории США, что оказывает влияние на рост доли операций с использованием реквизитов карточек в ОТС, зарегистрированных на территории США;

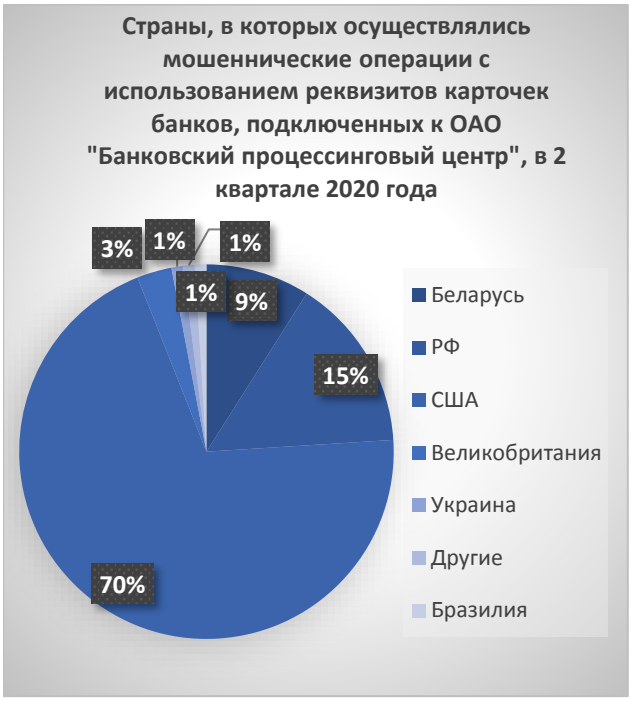
большое количество мошеннических тестовых операций и атак на БИНы банков (сгенерированные номера карточек) на сайтах, зарегистрированных на территории США, Канады, Бразилии, Египта, ОАЭ, Малайзии и др. стран с целью выявления реальных карточек для дальнейшего использования их реквизитов в мошеннических целях;

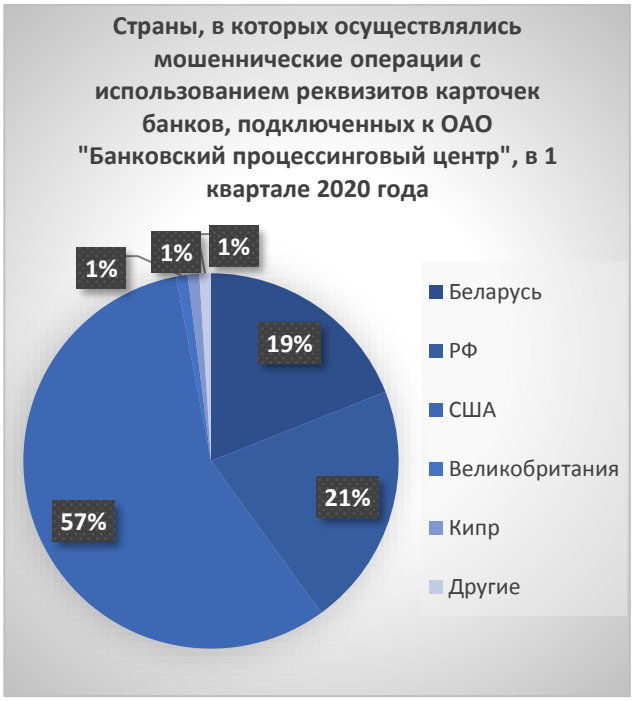
появление мошеннических китайских сайтов и сайтов с соцопросами, когда держателям предлагается пройти соцопрос и получить вознаграждение, но для этого необходимо оплатить соответствующую комиссию. В результате никакого вознаграждения держатель не получает, но теряет свои денежные средства после добросовестной оплаты комиссии;

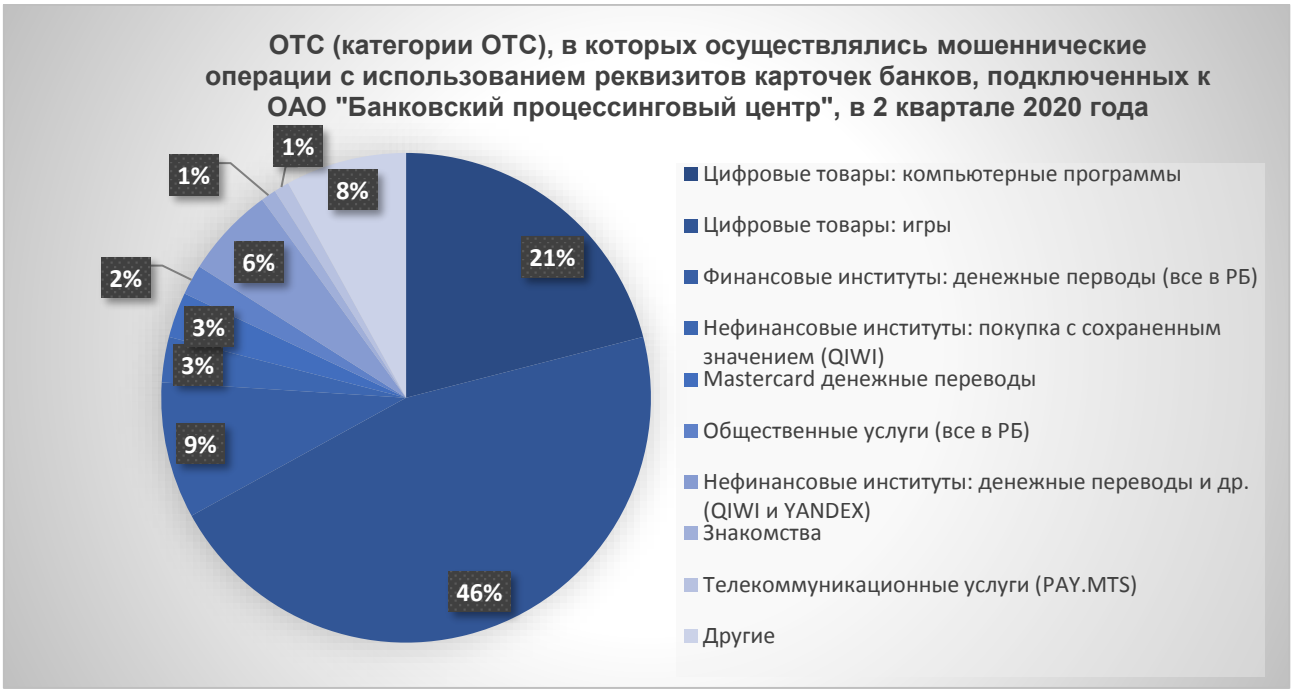
возобновление попыток мошеннических онлайн возвратов от ОТС, зарегистрированных на территории США. Вид мошенничества появился в 1 квартале 2019 года и основан на формировании авторизационного кредитового сообщения по операции возврат с последующим выводом денежных средств путем снятия кредитных денежных средств или переводом на другие карточки/счета «дропами», при этом выставления в клиринг операций возврат не происходит. Возобновление мошеннических попыток осуществления операций онлайн возврат свидетельствует о постоянном поиске злоумышленниками уязвимостей систем банков, отвечающих за блокировки по счетам, а также указывает на необходимость постоянной работы по информированию держателей карточек о правилах пользования банковскими платежными карточками, в том числе об ответственности за мошеннические действия;

наличие «friendly fraud» мошенничества. Держатели заказывают товары/услуги и оплачивают их с помощью карточки, после чего намеренно инициируют возврат платежа, утверждая, что данные их карточки были украдены. После возврата средств на карточку, купленный товар или предоставленная услуга остается. «Friendly fraud» также используется в сочетании с повторной пересылкой заказов (re-shipping). Преступники используют украденные платежные данные, чтобы оплатить свои покупки, но доставка товара осуществляется не на их личный адрес, а на адрес посредников, которые затем перенаправляют товары в другое место доставки.


Виды мошенничества CNP, %
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
2,4%
66,6%
31,0%
6,2%
52,8%
41,0%
5,5%
56,4%
38,1%
2,8%
36,6%
60,6%
3,0%
32,5%
64,5%
17,3%
65,4%
17,3%
ЯНВАРЬ 2020
ФЕВРАЛЬ 2020
МАРТ 2020
АПРЕЛЬ 2020
МАЙ 2020
ИЮНЬ 2020
E-commerce
Социальная инженерия
Компрометация СДБО


Страны, в которых осуществлялись мошеннические операции с использованием реквизитов карточек банков, подключенных к ОАО "Банковский процессинговый центр", в 2 квартале 2020 года
3%
1%
1%
1%
9%
15%
70%
Беларусь
РФ
США
Великобритания
Украина
Другие
Бразилия


Страны, в которых осуществлялись мошеннические операции с использованием реквизитов карточек банков, подключенных к ОАО "Банковский процессинговый центр", в 1 квартале 2020 года
1%
1%
1%
19%
21%
57%
Беларусь
РФ
США
Великобритания
Кипр
Другие



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

В 1 полугодии 2020 года зафиксировано 233 случая операций мошеннического характера в эквайринговой сети банков, которые обслуживаются в ОАО «Банковский процессинговый центр», что в 2,6 раза меньше аналогичного показателя 1 полугодия 2019 года. Из них **49%** составляют мошеннические операции **по утерянным/украденным карточкам; 43%** приходится на долю мошеннических операций **без присутствия карточки** (из них 56% это операции с использованием 3D Secure) и **5%** приходится на **другие виды мошенничества:** 91% из них составляет account takeover – мошенничество, при котором осуществляется перехват данных держателей и, получая контроль над

счетом, мошенники совершают безаутентификационные операции; 9% - incorrect processing – ситуация, при которой мошенническая транзакция стала возможной из-за отсутствия проверки безопасности, что позволило совершить операцию (вероятно ошибка возникла на стороне иностранного банка-эмитента, так как операции не были опротестованы); **3%** приходится на мошеннические операции с использованием **поддельных карточек** (из 7 заявленных операций 2 операции прошли без присутствия карточки, а 5 по бесконтактному интерфейсу). Уменьшение количества поддельных карточек в эквайринговой сети свидетельствует о фактическом смещении мошенничества в сферу e-commerce и операций без присутствия карточки, что в первую очередь обусловлено развитием информационных технологий и низкими затратами со стороны мошенников, а также влиянием закрытия границ в связи с угрозой распространения коронавирусной инфекции COVID-19, что значительно ограничивает возможность передвижения злоумышленников и влияет на общее снижение мошенничества с использованием поддельных карточек.

Вместе с развитием новых технологий меняются и методы хищения с банковских платежных карточек. В 1 полугодии 2020 года по сравнению с аналогичным периодом 2019 года практически в 3 раза увеличилось количество случаев мошенничества по утерянным/украденным карточкам. Подавляющее количество мошеннических операций по утерянным/украденным карточкам были осуществлены со считыванием бесконтактного интерфейса. Такой способ оплаты позволяет мошенникам совершать большое количество операций в рамках установленных лимитов без необходимости подтверждения совершения операции вводом ПИН-кода либо использования других методов аутентификации.

Общая сумма мошеннических операций в 1 полугодии 2020 года по сравнению с 1 полугодием 2019 года снизилась практически в 2 раза, при этом средняя сумма 1 мошеннической операции выросла на 23% и составила 90 долларов США (69 долларов США в 1 полугодии 2019 года). Увеличение средней суммы одной мошеннической операции также обусловлено ростом количества случаев мошенничества по утерянным/украденным карточкам (в связи с распространением коронавирусной инфекции COVID-19 международные платежные системы увеличили лимиты для бесконтактных операций).

В 1 полугодии 2020 года в 2 раза уменьшилась доля мошеннических операций без присутствия карточки по сравнению с 1 полугодием 2019 года. Снижение обусловлено небольшим количеством успешных мошеннических операций, совершенных в интернет-магазинах, так как в большинстве случаев формировались отмены авторизационных запросов с последующим возвратом средств держателям, в результате чего ни одна из сторон не понесла финансовых потерь.

Из общих тенденций мошенничества в среде e-commerce и операций без присутствия карточки следует отметить, что основная доля мошенничества приходится на операции в интернет-магазинах, которые занимаются продажей электронных игр и ключей. Также незначительная доля мошеннических попыток была зафиксирована в туристической сфере, а также в сфере телекоммуникационных услуг. 54% всех мошеннических операций в интернет-магазинах прошли с применением технологии 3D Secure.

Внимание мошенников к среде e-commerce свидетельствует о необходимости дополнительного контроля в отношении интернет-торговцев со стороны банков-эквайеров. Необходимо проводить более тщательные проверки при принятии на эквайринговое обслуживание, так как заключение договора с недобросовестным торговцем может повлечь резкое увеличение количества мошеннических операций и, как следствие, значительные финансовые потери со стороны банка. Также актуальной мерой безопасности является введение страховых депозитов в размере половины от предполагаемого оборота денежных средств по карточкам в терминалах торговца за месяц или увеличение сроков осуществления возмещения денежных средств для новых клиентов.

В целом уровень мошенничества в эквайринговой сети можно охарактеризовать как стабильно низкий.

Детальная информация представлена на диаграммах ниже.