Исследование трендов мошенничества по картам и ДБО физических лиц

***Афанасьев Сергей**, КБ «Ренессанс Кредит», март 2019 г.*

Введение

В феврале 2019 года ФинЦЕРТ Банка России опубликовал обновленную статистику по мошенническим хищениям с карт и счетов физических лиц[1]. В отчете ФинЦЕРТа содержится общая статистика по банковскому сектору РФ с трендами мошенничества по картам и ДБО физлиц за период с 2015 по 2018 гг.
К сожалению, в обзоре ФинЦЕРТа не отражена детализация в долях по каналам и типам мошеннических платежей, что не позволяет установить истинные причины и основные источники мошеннических транзакций, что, в свою очередь, затрудняет выработку мероприятий, направленных на минимизацию рисков мошенничества.
В нашем исследовании мы дополняем результаты обзора ФинЦЕРТа Банка России и показываем детализацию трендов мошенничества по картам и ДБО в разрезе каналов и типов мошеннических схем.

Анализ проводился на данных КБ «Ренессанс Кредит».
Горизонт анализа: 01.01.2016 – 31.12.2018

Примечание 1
В данном исследовании учитывались все мошеннические операции, включая заблокированные банком. Из приведенной статистики КБ «Ренессанс Кредит» блокирует ~90% мошеннических платежей в режиме онлайн. Включение в статистику заблокированных мошеннических платежей позволяет экстраполировать полученные результаты на весь банковский сектор РФ, поскольку при данном подходе исключается специфика внутрибанковских фрод-правил и моделей (например, лимиты на определенные типы операций, каналы и т.п.)

Примечание 2
Показатели уровня мошенничества рассчитывались как отношение объема мошеннических платежей, проведенных в определенном канале (Интернет, Банкоматы, или POS-терминалы), к общему объему платежей в данном канале. Данная методика позволяет исключить влияние роста объемов платежей в определенном канале (например, скимминг характерен для транзакций в Банкоматах или POS-терминалах, т.е. интернет-платежи необходимо исключать из расчета).

[1] ОБЗОР НЕСАНКЦИОНИРОВАННЫХ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ ЗА 2018 ГОД: http://www.cbr.ru/Content/Document/File/62930/gubzi_18.pdf

Часть 1. Проверка репрезентативности

1.1. Доля мошеннических платежей от всего объема платежей (в рублях)

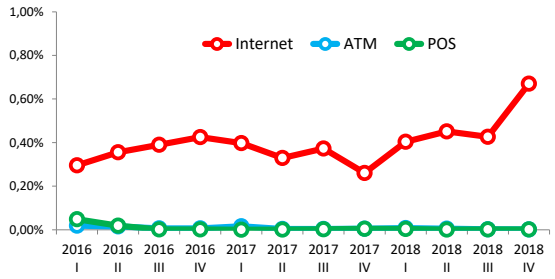
Сопоставление динамики доли мошеннических платежей по банковскому сектору с нормированной динамикой доли мошенничества в КБ «Ренессанс Кредит» показывает, что общие формы кривых сохраняются. Это значит, что данные КБ «Ренессанс Кредит» можно экстраполировать на весь банковский сектор с точностью до формы кривой/тренда (абсолютные показатели при этом будут отличаться).

Во II квартале 2018 года, согласно отчету ФинЦЕРТа, наблюдается резкий рост объема и доли мошеннических транзакций. Данная аномалия наблюдается во всех трех каналах (интернет, банкоматы, POS-терминалы). При этом в Банкоматах и POS-терминалах объем мошенничества вырос в 2-2,5 раза, а потом вернулся на прежний уровень. Такое поведение одновременно в трех каналах не характерно для внешней мошеннической атаки. Кроме того, на данных КБ «Ренессанс Кредит» мы не наблюдаем таких резких изменений, из чего можно сделать вывод, что скачок носит технический характер.

***Источник:** ФинЦЕРТ Банка России*

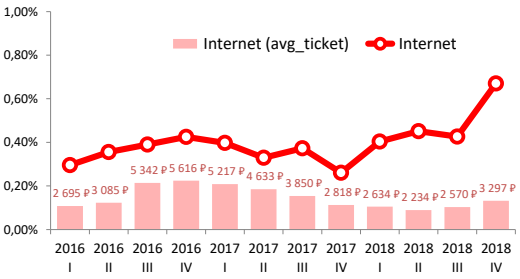
Часть 2. Общие тренды в разбивке по каналам

2.1. Доля мошеннических платежей по каналам от всего объема платежей в соответствующем канале (в рублях)



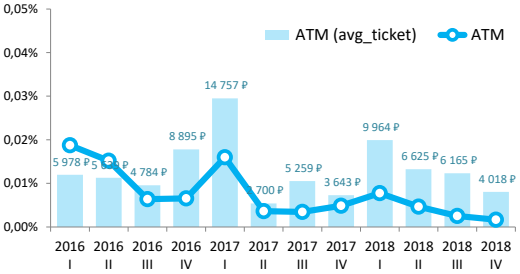
Динамика доли мошеннических платежей по каналам показывает, что самым рисковым каналом является Internet, куда относятся интернет-переводы (c2c, p2p, ДБО, веб-кошельки и т.д.), а также интернет-покупки (e-commerce). При этом доля интернет-мошенничества стабильно растет – в IV квартале 2018 года доля выросла в 2,6 раза по сравнению с IV кварталом 2017 года.
Уровень мошенничества в банкоматах (ATM) и в организациях торговли и услуг (POS) остается низким.

2.2. Internet: доля мошенничества в интернете от всего объема платежей в интернете (в рублях)



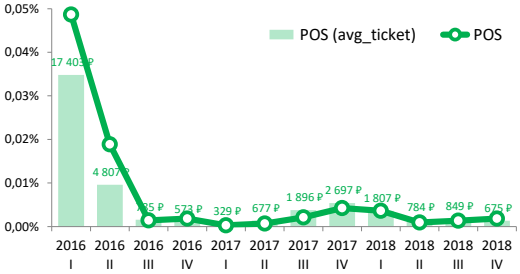
Если посмотреть на средний чек по мошенническим операциям в интернете, то видно, что с начала 2017 года и до середины 2018 года средний чек падал, но начиная с III квартала 2018 начал расти вместе с долей мошенничества. Это говорит о том, что мошенники помимо масштабирования своих схем (растет доля), повышают и свою эффективность (растет средний чек).

2.3. Банкоматы (ATM): доля мошенничества в банкоматах от всего объема платежей в банкоматах (в рублях)



В банкоматах уровень мошенничества в 2018 году стабильно снижался и является традиционно низким в последние годы. Этот тренд можно объяснить как положительный результат от перехода российских банков на EMV-технологию (карты с чипами), который массово начался в 2013 году. В картах с чипами используется технология токенизации, которая не подвержена старому способу карточного мошенничества – скимминг (считывание данных с магнитной полосы карты). Это позволило банкам снизить уровень скимминга практически до нуля.

2.4. POS: доля мошенничества в организациях торговли и услуг (POS) от всего объема платежей в POS-канале (в рублях)



Тренд уровня мошенничества в POS-канале также демонстрирует преимущества перехода банков на карты с чипами. С середины 2016 года уровень мошенничества снизился практически до нуля, а по среднему чеку видно, что фрод-транзакции в POS проводятся по беспиновой технологии (до 1000 руб.).

Часть 3. Основные виды мошенничества в разбивке по каналам

Для анализа трендов мошенничества по типам использовалась внутрибанковская типизация, включающая 5 основных типов мошенничества. Доля мошенничества по каждому типу в канале рассчитывалась как отношение мошеннических платежей, совершенных в данном канале, ко всему объему платежей этого канала.

Социальная инженерия (SMiShing) – операции в результате СМС-мошенничества;

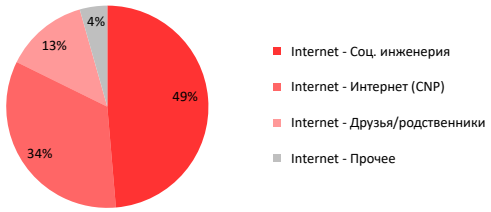
Интернет (Card-Not-Present) – операция без физического предъявления карты (интернет-платежи, заказ по почте/телефону, p2p/c2c, социальная инженерия, фишинг и т.д.);

Друзья/родственники (Friendly Fraud) – операции с использованием подлинной карты/реквизитов подлинной карты без разрешения клиента (знакомые, родственники);

Украденные/утерянные (Lost/Stolen) – операции по утерянным/украденным картам;

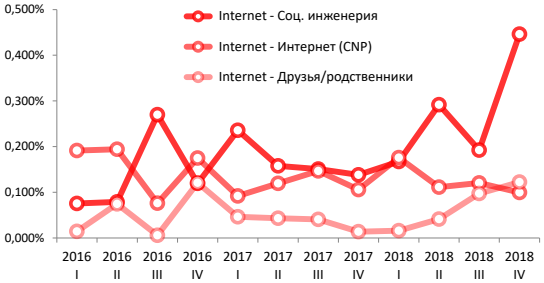
Скимминг (Card-Present-Fraud) – операции с физическим предъявлением поддельной карты;

3.1. Соотношения объемов мошеннических платежей в канале Internet по типам мошеннических схем



Для анализа трендов уровня мошенничества по типам, были отобраны топ-3 самых распространенных вида мошенничества, на которые приходится 96% всего мошенничества в канале Internet.
Почти половина всего фрода в интернете совершается методами социальной инженерии – 49%. На втором месте идет CNP-мошенничество (поддельные сайты и т.п.) – 34%. И на третьем месте – Friendly Fraud (использование карты знакомыми или родственниками) – 13%.

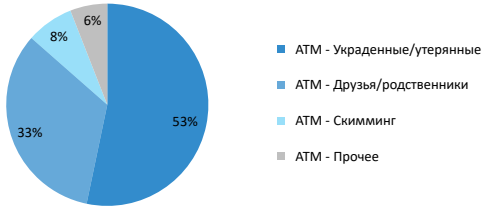
3.2. Динамика уровня мошенничества в канале Internet по типам мошеннических схем



По трендам видно, что в канале Internet растет доля социальной инженерии – рост в 3,2 раза в IV квартале 2018 года по сравнению с IV кварталом 2017 года.

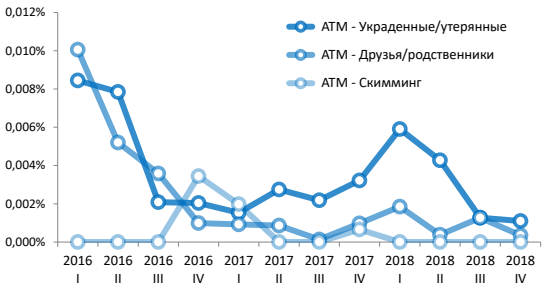
Доля CNP-мошенничества остается стабильно высокой и не меняется. К этому виду мошенничества относится «фишинг» (поддельные сайты), а также другие виды бесконтактных мошеннических платежей, с неустановленным типом мошенничества (социальная инженерия, friendly fraud и др.).

3.3. Соотношения объемов мошеннических платежей в канале ATM (банкоматы) по типам мошеннических схем

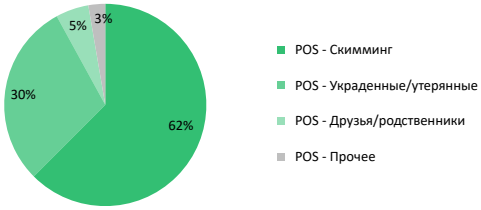


Для анализа трендов мошенничества по банкоматам (ATM), были отобраны топ-3 самых распространенных вида мошенничества, на которые приходится 94% всего мошенничества в канале ATM. Более половины всего фрода со снятием наличных в банкоматах совершается по украденным/утерянным картам – 53%. Под данный вид мошенничества чаще всего попадают пожилые люди, которые либо теряют карту с записанным на ней ПИН-кодом, либо становятся жертвами воров в отделениях банков и ATM-зонах[2]. На втором месте идет Friendly Fraud – 33%. На третьем с 8% расположился скимминг (копирование данных с магнитной полосы карты), который практикуется в основном за рубежом – в странах, не сумевших полностью перейти на EMV.

3.4. Динамика уровня мошенничества в канале ATM по типам мошеннических схем



3.5. Соотношения объемов мошеннических платежей в канале POS по типам мошеннических схем



Для анализа трендов мошенничества в организациях торговли и услуг (POS), были отобраны топ-3 самых распространенных вида мошенничества, на которые приходится 97% всего мошенничества в канале POS.

3.6. Динамика уровня мошенничества в канале ATM по типам мошеннических схем

По трендам видно, что уровень мошенничества в канале POS снизился практически до нуля.

[2] См. исследование портрета жертвы карточного мошенника: https://www.vedomosti.ru/finance/articles/2017/12/27/746691-kogo-chasche-vsego-obmanivayut-kartochnie-moshenniki

Резюме

Анализ динамики уровня мошенничества по картам и ДБО физических лиц показал, что основной риск сосредоточен в канале Internet. Вероятность (доля) мошенничества в этом канале в 2018 году в 117 раз выше, чем в канале ATM и в 252 раза выше, чем в канале POS.

ATM (банкоматы)
Уровень мошенничества в канале ATM остается низким и сконцентрирован в основном на выводе средств с украденных/утерянных карт, с подтверждением операций ПИН-кодом.

POS (организации торговли и услуг)
В POS-канале уровень мошенничества является самым низким и сосредоточен в основном на чеках менее 1000 рублей, проводимых по беспиновой технологии (NFC). Снижение уровня мошенничества в POS-канале практически до нулевых показателей стало возможным благодаря переводу российских карт на EMV-стандарт (чипы), который дает надежную защиту от скимминга.

Internet
Основным драйвером роста уровня мошеннических платежей по картам и ДБО физлиц является социальная инженерия в канале Internet, т.е. с использованием интернет-инструментов для вывода похищенных средств (веб-кошельки, c2c-сервисы, быстрые платежи и т.д.). Уровень социальной инженерии в интернет-канале в 2018 году вырос в 1,6 раза по сравнению с 2017 годом. А в IV квартале 2018 года уровень вырос в 3,2 раза по сравнению с IV кварталом 2017 года.
Социальная инженерия сейчас является главной проблемой для банков, о чем также свидетельствует значительный рост числа публикаций в СМИ и жалоб клиентов в социальных сетях и на публичных ресурсах[3] [4] [5] [6] [7] [8] [9].

Стабильно растущий уровень социальный инженерии показывает, что на данный момент у банков нет эффективных инструментов для борьбы с этим видом мошенничества. Обучение клиентов «никому не говорить смс-пароли» не позволяет сдерживать уровень социальной инженерии.

Разработанная ФинЦЕРТом межбанковская система «Фид-Антифрод» в будущем позволит в режиме онлайн блокировать средства клиента, выведенные мошенническим путем. Однако, учитывая незрелость системы и сложность интеграционных процессов в банках, реальных положительных результатов стоит ожидать не ранее, чем через 1-2 года.
Стоит также отметить, что данная система позволяет блокировать средства *только* при условии быстрого контакта с клиентом – пока мошенники не обналичили выведенные средства. Т.е. большая часть клиентов, до которых банку не удалось дозвониться, потеряют свои средства.

Учитывая вышесказанное, банкам придется *на своей стороне* разрабатывать и внедрять инструменты для защиты от социальной инженерии:

- Разрабатывать модели и правила для детектирования социальной инженерии в режиме онлайн;
- Ограничивать лимиты интернет-операций;
- Блокировать высокорисковые каналы вывода средств;
- Использовать внешние сервисы и дополнительные источники данных для анализа транзакций;
- Усиливать защиту на дистанционных каналах вывода;
- и т.д.

[3] https://www.kommersant.ru/doc/3894264
[4] https://rg.ru/2019/02/19/cb-obem-hishchenij-s-bankovskih-kart-vyros-pochti-v-poltora-raza.html
[5] https://www.banki.ru/news/daytheme/?id=10861180
[6] https://www.banki.ru/news/lenta/?id=10859701
[7] https://ria.ru/20190218/1550998849.html
[8] https://www.banki.ru/forum/?PAGE_NAME=read&FID=61&TID=355160
[9] https://www.kommersant.ru/doc/3867733?utm_source=yxnews&utm_medium=desktop