УДК 336.717

АНАЛИЗ ВИДОВ МОШЕННИЧЕСТВА В СФЕРЕ ИНДУСТРИИ ПЛАТЕЖНЫХ КАРТ

М.Х. ТУРСУНОВА
(Представлено: И.А. СТРОГАНОВА)

В настоящей статье рассматриваются вопросы мошенничества посредством платёжных банковских карточек и связанных с этим рисков для эмитентов карточек. Автором предложены методы и возможные пути решения. Разрозненные решения по предотвращению преступлений, связанных с платежными карточками, препятствуют своевременному выявлению мошенничества, поскольку они не могут представить единое представление о потенциальных угрозах хищений.

Поскольку мир стремительно движется к цифровизации, а денежные операции становятся безналичными, использование банковских карт быстро растет. Связанная с этим преступная мошенническая деятельность также растет, что приводит к огромным финансовым и репутационным рискам. Актуальность вопроса безопасного использование держателями платежных карт обусловлена рядом внутренних и внешних факторов. Существует угроза несанкционированного доступа к остаткам на текущих счетах, которым привязана карточка. Безусловно, это стало серьезной проблемой в современную эпоху цифровизации, так как все транзакции можно легко завершить онлайн, введя только данные платежной карты. Даже в 2010-х годах многие пользователи розничных веб-сайтов стали жертвами мошенничества с онлайн-транзакциями непосредственно перед тем, как для покупок в Интернете была использована двухэтапная проверка [1]. Организации, потребители, банки и торговые организации подвергаются риску, когда нарушение данных – обеспечивающих доступ к средствам на счете, к которому привязана карточка (это такие реквизиты как логин и пароль) приводит к краже денежных средств и, в конечном счете, к потере лояльности клиентов вместе с репутацией обслуживающей компании.

Несмотря на внедрение более безопасных технологий, мошенничество с платежными картами по-прежнему остается одной из самых больших проблем для банков и компаний, выпускающих платежные карты. Несанкционированные операции с картами в 2017 году поразили 16,7 миллионов жертв [2]. Кроме того, как сообщила Федеральная торговля комиссия (независимое агентство правительства США, призванное защищать права потребителей и, в частности, следящее за соблюдением антимонопольного законодательства), количество заявлений о мошенничестве с банковскими картами в 2017 году было на 40% больше, чем в предыдущем году [3]. Общие потери от мошенничества с картами остаются высокими, поскольку мошенники используют значительный рост транзакций в сфере онлайн-карт. На основе данных отчета аналитического агентства, автором структурированы виды мошенничества 2018 года, их структура представлена на рисунке 1.

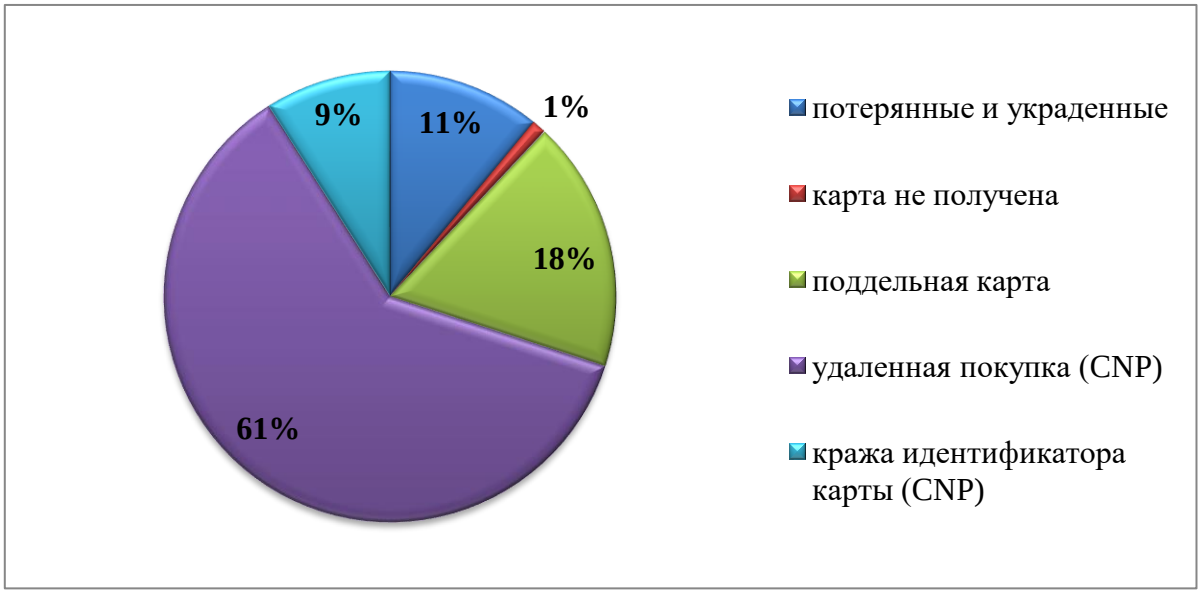

Рисунок 1. – Виды мошенничества с платежными карточками 2018 года (% от общих убытков)

Источник: собственная разработка на основе [4].

Таким образом из представленной на рисунке 1 информации наиболший общий весь мошенничество составляет удаленная покупка (транзакция без карты - Card not present, CNP) происходит, когда ни владелец карты, ни банковская карта физически не присутствуют во время транзакции. Чаще всего это происходит

при заказах, которые выполняются удаленно – по телефону или факсу, через Интернет или по почте). Мошенничество с удаленными покупками по-прежнему происходит в основном из-за того, что преступники используют данные карт, полученные в результате кражи данных, таких как утечка данных третьими лицами.

В отчете компании Nilson (Американская компания, крупнейшая независимая фирма, проводящая маркетинговые измерения в индустрии товаров повседневного спроса, медиа измерения и исследования потребителей) говорится, что к 2025 году общий объем сбор интеграций личных данных платежных карт во всем мире составит 56,182 трлн долларов, а общий объем мошенничества с картами во всем мире, как ожидается, составит 35,31 млрд долларов. Мошенничество на каждые 100 долларов в общем объеме снизится до 6,28 цента. Потери от мошенничества в США, по прогнозам, достигнут 12,51 миллиарда долларов в 2025 году [5].

Мошенничество с платежными карточками является идеальным вариантом использования машинного обучения и искусственного интеллекта (ИИ) и имеет большой опыт успешного использования. Когда потребители получают звонок, текстовое сообщение, электронное письмо или сообщения в приложении от эмитента своей карты с просьбой подтвердить транзакцию или сообщить им о мошенничестве с их картой, они могут даже не подозревать, что за этим отличным обслуживанием клиентов стоит блестящий набор алгоритмов. Следует отметить, обнаружение мошенничества с банковскими картами с помощью машинного обучения – это процесс исследования данных командой специалистов по анализу данных и разработка модели, которая обеспечит наилучшие результаты в выявлении и предотвращении мошеннических транзакций.

Машинное обучение помогает специалистам по обработке данных эффективно определять, какие транзакции с наибольшей вероятностью будут мошенническими, при этом значительно сокращая количество ложных срабатываний. Эти методы чрезвычайно эффективны в предотвращении и обнаружении мошенничества, поскольку они позволяют автоматически обнаруживать закономерности в больших объемах потоковых транзакций. Алгоритмы машинного обучения также могут изучать недавнюю онлайн-активность клиента, такую как поведение при оплате, социальные сети, социальное обеспечение, местоположение IP, активность устройства и адрес выставления счетов. Чем больше точек данных доступно для клиента, тем ниже оценка риска для этого клиента. Основываясь на этих входных данных системы, торговцы и банки могут повысить свою безопасность для аутентификации или оценки процесса риска.

Эти данные также могут быть использованы для обновления профиля клиента и определения надежности клиента. Это позволит продавцам быть в курсе мошеннических транзакций, таких как возврат платежей, поддельная учетная запись, спам, захват учетной записи и т.д.

Необходимо подчеркнуть, что отрасли финансовых услуг и технологий находят наибольшую ценность в искусственном интеллекте (далее – ИИ). ИИ позволяет использовать более совершенные алгоритмы, которые могут различать приемлемую и потенциально мошенническую информацию. Благодаря волне искусственного интеллекта, по мере того как мошенники становятся лучше, машины, обнаруживающие их, тоже становятся лучше. Мошенничество с банковскими картами составляет значительную долю этих расходов. Искусственный интеллект может обеспечить более быстрое, дешевое и точное обнаружение мошенничества. Финансовые учреждения, предлагающие услуги по платежным картам, сталкиваются с новой задачей – защитой данных своих потребителей и снижением риска попадания данных в руки киберпреступников. Фактически, по оценкам исследования, ожидается, что валовые убытки от мошеннических операций с картами достигнут 40 миллиардов долларов в 2027 году [6].

В заключение следует отметить, что мошенничество является серьезной проблемой для всей индустрии банковских карт, которая растет с ростом популярности электронных денежных переводов. Для эффективного предотвращения преступных действий, которые приводят к утечке информации о банковских счетах, подделке платежных карт, краже средств со счетов, к которым привязаны платежные карточки, потере репутации и лояльности клиентов, эмитентам банковские платежные карт следует рассмотреть возможность внедрения передовых методов предотвращения мошенничества с платежными картами и обнаружения мошенничества. В эпоху цифровицазии искусственный интеллект и машинное обучение, аналитические инструменты достигли нового повсеместного применения. Методы, основанные на машинном обучении, могут постоянно повышать точность предотвращения мошенничества на основе информации о поведении каждого держателя карты. Также аналитика может помочь в изучении неиспользованных рынков с высоким потенциалом роста и в диверсификации рисков.

ЛИТЕРАТУРА

1. Credit Card Fraud Detection: Top ML Solutions in 2021 [Электронный ресурс]. – Режим доступа: https://spd.group/machine-learning/credit-card-fraud-detection/. – Дата доступа: 20.09.2021.
2. 2018 Identity Fraud Study, Javelin Strategy & Research [Электронный ресурс]. – Режим доступа: https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin. – Дата доступа: 22.09.2021.
3. Future Technologies Company (FTC) [Электронный ресурс]. – Режим доступа: https://www.ftc. – Дата доступа: 23.09.2021.

4. Credit Card Fraud Statistics to Keep You Aware in 2021 [Электронный ресурс]. – Режим доступа: https://spendmenot.com/blog/credit-card-fraud-statistics/. – Дата доступа:24.09.2021.
5. Nilson Report [Электронный ресурс]. – Режим доступа: https://nilsonreport.com/mention/1313/1link/. – Дата доступа: 25.09.2021.
6. V. Filippov, L. Mukhanov, B. Shchukin, Credit Card Fraud Detection System [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/241158178_Credit_card_fraud_detection_system. – Дата доступа: 25.09.2021.