Секция «Обеспечение финансовой безопасности России: финансовые расследования в цифровой экономике»

Выявление мошенничества с кредитными картами в условиях цифровизации

Научный руководитель – Анищенко Евгений Владимирович

Королева Екатерина Константиновна
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра экономических и финансовых расследований, Москва, Россия
E-mail: koroleva.kate@list.ru

Актуальность темы исследования заключается в том, что мошенничество с кредитными картами представляет собой серьезную проблему, затрагивающую отдельных лиц и финансовые организации. Поскольку использование кредитных карт продолжает расти как в онлайн-, так и в офлайн-транзакциях, злоумышленники научились выявлять и использовать слабые места, что приводит к росту мошеннических действий.

Целью исследования является рассмотрение видов мошенничества с кредитными картами и подходов к выявлению мошенничества с кредитными картами в условиях цифровизации.

Большинство случаев мошенничества с кредитными картами (примерно 71% случаев по данным ЦБ РФ [2]) происходит в онлайн-среде путем проведения транзакций с получением личных данных держателя карты, включая учетные записи и профили пользователей, имена, адреса электронной почты, IP-адреса и т.д. Одним из распространенных видов преступлений с кредитными картами является «чистое» мошенничество, которое осуществляется с использованием законной и достоверной информации. При «чистом» мошенничестве злоумышленники используют украденные или фальсифицированные личные данные, выдавая себя за подлинных держателей кредитных карт, что позволяет им совершать мошеннические действия без распознания. Целью «чистого» мошенничества с кредитными картами является завладение кредитными средствами держателя карты путем обхода мер безопасности (например, процедур проверки личности) [4].

С целью предотвращения данного вида мошенничества реализуют такие меры безопасности как метод многофакторной аутентификации для усиления проверки личности держателя карты и шифрования конфиденциальных данных. Основной задачей предотвращения данного вида мошенничества является обесценение конфиденциальной информации о кредитной карте. В данном случае одним из действенных методов выступает токенизация – процесс замены номеров кредитных карт случайно сгенерированными номерами, которые невозможно отследить. Таким образом, финансовая транзакция не содержит никакой исходной информации и по-прежнему позволяет платежным системам обрабатывать платежи по кредитной карте, не раскрывая номер расчетного счета. Токенизация позволяет расширить возможности бесконтактных платежей и снижает риск похищения персональных данных при транзакциях при помощи кредитных карт [1].

Одним из распространенных видов мошенничества с кредитными картами является совершение мошенничества с фальсификацией данных с целью получения лимита по кредитной карте. В данном случае злоумышленник использует украденные данные личности для подачи заявки на кредитную карту без намерения вернуть долг кредитору.

Для предотвращения и выявления данного вида мошенничества в практике финансовых организаций используют инструменты базы данных «Знай своего клиента» (KYC). Данный инструмент предназначен для проверки личности на различных уровнях – подача

заявки на кредитную карту, пользование кредитной картой и т.д. Инструмент KYC включает проверку удостоверения личности и других документов, биометрическую проверку – лицо, голос. Например, в банках Индии успешно применяется электронная система проверки e-KYC – метод проверки, аккредитованный UIDAI (Агентство Индии по уникальной идентификации). Помимо заполнения заявления на проверку на основе уникального ID, информация проверяется в базе данных UIDAI за несколько минут [3]. Этот инструмент эффективен в обнаружении мошенничества, поскольку предоставляет информацию о любом настоящем или будущем клиенте банка в режиме реального времени. Данный инструмент также используются для выявления проблемных держателей карт.

Еще один распространенный вид мошенничества с кредитными картами – «дружественное» мошенничество – потребитель совершает покупку в интернет-магазине с помощью своей собственной кредитной карты, а затем запрашивает возвратный платеж у банка-эмитента после получения приобретенных товаров или услуг. После одобрения возвратный платеж отменяет финансовую транзакцию, и держатель кредитной карты получает возмещение потраченных им денег [5].

Для обнаружения и предотвращения данного вида мошенничества финансовые организации применяют модели машинного обучения (контролируемые и неконтролируемые), которые позволяют проводить анализ большого массива данных о проводимых транзакциях, включая истории транзакций держателей карт, их покупательское поведение и другие параметры для выявления потенциально подозрительных транзакций по кредитной карте [6]. Поведенческая аналитика при помощи искусственного интеллекта позволяет изучать поведение клиентов и обнаруживать аномалии, которые могут сигнализировать о «дружественном» мошенничестве, например необычные покупки или история возвратных платежей.

По проведенному исследованию можно заключить, что мошенничество с кредитными картами классифицируется как одна из форм кредитных правонарушений и включает «чистое» мошенничество путем использования украденных достоверных данных с целью завладения кредитными средствами держателя карты, мошенничество с фальсификацией данных с целью получения кредитной карты, «дружественное» мошенничество с целью возврата платежа по совершенной транзакции. При этом основными методами выявления и предотвращения мошенничества с кредитными картами в условиях цифровизации являются токенизация, формирование базы данных «Знай своего клиента» (KYC), модели искусственного интеллекта и машинного обучения, которые доказали свою эффективность в деятельности финансовых организаций за рубежом и могут успешно внедряться в российской банковской сфере.

Источники и литература

1) Миклухо Д. Защита от мошенников: как работает токенизация банковских карт, 18 декабря 2023 https://rg.ru/2023/12/08/zashchita-ot-moshennikov-kak-rabotaet-tokenizaciia-bankovskih-kart.html
2) Обзор операций, совершенных без согласия клиентов финансовых организаций. Банк России, 14.02.2023 https://cbr.ru/analytics/ib/operations_survey_2022/
3) Alamri M., Ykhlef, M. Survey of Credit card anomaly and Fraud Detection using sampling techniques // Electronics, 2022, Vol. 11(23)
4) Anderson R. Why Information Security is Hard-An Economic Perspective, 2022. P. 358 - 365
5) Borgne Y. L. Machine Learning for Credit card fraud Detection - towards data science. Medium, 2022, January 6 https://towardsdatascience.com/machinelearning-for-credit-ca

rd-fraud-detection-a-jupyter-book-for-reproducible-research-8ca5edad7b5d

6) Carcillo F. Combining unsupervised and supervised learning in credit card fraud detection, 2019 https://www.semanticscholar.org/paper/Combining-unsupervised-and-supervised-learning-in-Carcillo-Borgne/70f612edc09538f147ec58710db41e06de65427a