ХИЩЕНИЯ, СОВЕРШАЕМЫЕ С ПОМОЩЬЮ ИСПОЛЬЗОВАНИЯ БАНКОВСКИХ ТЕХНОЛОГИЙ

Прыгунова Диана Сергеевна

магистрант, Российский государственный социальный университет, РФ, г. Москва

Никодимов Игорь Юрьевич

д-р юрид. наук, доцент, доцент кафедры уголовного права Российского Государственного Социального Университета, РФ, г. Москва

EMBEZZLEMENT OF FUNDS COMMITTED THROUGH USAGE OF BANKING TECHNOLOGIES

Diana Prygunova

Candidate for a master's degree, Russian State Social University, Russia, Moscow

Igor Nikodimov

Doctor of Juridical Sciences, assistant professor in Russian State Social University, Russia, Moscow

Аннотация. С развитием банковских технологий и внедрением их в сферу банковских услуг, появляются как позитивные аспекты в лице совершенствования системы обслуживания клиентов банка, ускорения процессов обработки платежей, так и негативные, находящие отражение в новых видах, способах и методах хищения денежных средств. В частности, в статье рассматриваются выделенные за последнее время способы хищения денежных средств, совершаемые посредствам использования банковских технологий, неправомерного использования банковских карт и персональных данных клиентов банков.

Abstract. Development of banking technologies and their implementation in the sphere of banking services provoke some positive aspects like improving Bank customer service system, accelerating processing of payments and negative one like reflection of new types and methods of embezzlement of funds. Particularly article deals with recently identified methods of embezzlement of funds committed through usage of banking technologies, illegal usage of Bank cards and personal data of Bank customers.

Ключевые слова: уголовное право, банковская сфера, банковские технологии, банковские карты, хищение денежных средств.

Keywords: criminal law, banking, banking technology, Bank cards, embezzlement of funds.

Имплементация инновационных банковских технологий, к сожалению, неизбежно протекает

наряду с появлением новых способов хищения денежных средств с расчетных счетов клиентов банков злоумышленниками. Так, за 2018 год Центральным Банком зафиксирована общая статистическая цифра хищения с банковских карт физических лиц в размере 1,4 миллиарда рублей, что касается счетов юридических лиц, то преступными действиями были совершены попытки хищения денежных средств свыше 1,47 миллиарда рублей.

Следственная и судебная практика показывает, что преступления данной категории чаще всего могут быть квалифицированы по таким статьям Уголовного кодекса Российской Федерации, как статья 159 «Мошенничество», статья 159.3 «Мошенничество с использованием электронных средств платежа».

За последнее время выделилась целая группа видов хищения денежных средств с использованием банковских технологий, к ним следует отнести следующие:

Скимминг, представляет собой вид хищения денежных средств с использованием специального устройства — скиммера, способного считывать данные банковской карты. Своей целью скиммеры ставят получение таких важных данных карты, как номер карты, срок ее действия, Ф.И.О. владельца платежной карты и ПИН-код для последующего восстановления украденных данных на поддельной карте.

Шимминг, по своей сути являющийся некой усовершенствованной разновидностью скимминга, использует такой инструмент, как шиммер — устройство толщиной в несколько миллиметров, способное считывать данные банковской карты. Данный инструмент злоумышленников с легкостью может поместиться в разъем картридера банкомата. Защитой от данного вида хищения может служить использование карт с чипами.

Фишинг – распространённый вид кибермошенничества, базирующийся на методах социальной инженерии, с помощью фишинга преступники пытаются завладеть конфиденциальными данными клиента банка. Фишинг может быть представлен в виде массовых рассылок писем в сети интернет, а также смс-сообщений, в которых мошенники с помощью психологических приемов побуждают клиентов банка добровольно предоставить свои конфиденциальные данные, а также платежные реквизиты банковской карты. Как правило, к сообщению прикреплена ссылка, предлагающая прямой переход на сайт банка, внешне мало отличающийся от настоящего.

Вишинг – в данном виде злоумышленники также пытаются завладеть данными держателя карты, однако делают это посредствам телефонной связи. Здесь также есть различные способы завладения необходимой преступникам информации, к примеру, жертве поступает звонок от автоинформатора с сообщением о попытке совершения мошеннических действий с банковской картой. Со слов злоумышленников, для предотвращения таких действий, держателю карты необходимо перезвонить на определенный номер, если клиент банка произведет звонок по названному номеру, с его карты спишутся денежные средства.

Таким образом, в статье приведены основные виды хищения денежных средств с банковских карт с помощью банковских технологий, незаконного завладения персональными данными держателей карт и конфиденциальных данных платежной карты. К основным видам следует отнестии скимминг, шимминг, фишинг и вишинг, каждый вид имеет свои способы завладения необходимой злоумышленникам информации. Однако такое общее правило, как сохранение внимательности, финансовая и правовая грамотность, помогут избежать или вовремя предотвратить хищение денежных средств с банковской платежной карты.

Список литературы:

1. Лысенко В.В. Особенности расследования хищений денежных средств с использованием банковских карт в условиях противодействия и его преодоления // Пробелы в российском законодательстве. 2015. №2. URL:https://cyberleninka.ru/article/n/osobennosti-rassledovaniya-hischeniy-denezhnyh-sredstv-s-ispolzovaniem-bankovskih-kart-v-usloviyah-protivodeystviya-i-ego-preodoleniya (дата обращения: 09.12.2019).

2. Черных В.В. Проблемы расследования мошенничества, совершенного с использованием банковских карт, и пути их решения // Вестник ТИУиЭ. 2018. №1 (27). URL: https://cyberleninka.ru/article/n/problemy-rassledovaniya-moshennichestva-sovershennogo-s-ispolzovaniem-bankovskih-kart-i-puti-ih-resheniya (дата обращения: 10.12.2019).

3. Статистика и аналитика. Состояние преступности. [Электронный ресурс]. – URL: https://мвд.рф/Deljatelnost/statistics