МРНТИ 10.21.01

Ш. Елубаева[1]
[1]Университета Сулеймана Демиреля, Каскелен, Казахстан

ПРОБЛЕМЫ ЗАЩИТЫ ПРАВ КЛИЕНТОВ БАНКОВ ПРИ РАССМОТРЕНИИ СУДАМИ ДЕЛ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТ-БАНКИНГА

Аннотация. Данная статья посвящена актуальным проблемам судебной защиты прав клиентов банков, связанных с использованием интернет-банкинга. Анализируется текущее состояние предпринимаемых государством мер по защите прав потребителей финансовых услуг в данной сфере с акцентом на результаты судебного рассмотрения дел по искам пострадавших клиентов. В частности, рассмотрена проблема возложения банками ответственности на клиента за безопасность операций в интернет-банкинге и сложность доказывания вины банка, в результате чего складывается негативная судебная практика, не способствующая защите пострадавших клиентов. В статье даны предложения по усилению защиты прав клиентов интернет-банкинга.

Ключевые слова: защита прав потребителей финансовых услуг, интернет-банкинг, банк, персональные данные, информационная безопасность, социальная инженерия.

****

Abstract. This article is devoted to the actual problems of judicial protection of the rights of bank customers related to the use of Internet banking. The current state of measures taken by the state to protect the rights of consumers of financial services in this area is analyzed, with an emphasis on the results of judicial review of cases on claims of affected customers. In particular, the problem of assigning responsibility by banks to the client for the security of transactions in Internet banking and the complexity of proving the bank's guilt is considered, resulting in negative judicial practice that does not contribute to the protection of affected customers. The article contains proposals to strengthen the protection of the rights of Internet banking customers.

Keywords: consumer protection of financial services, Internet banking, bank, personal data, information security, social engineering.

****

Аңдатпа. Бұл мақала интернет-банкингті пайдаланумен байланысты банк клиенттерінің құқықтарын сот арқылы қорғаудың өзекті мәселелеріне арналған. Зардап шеккен клиенттердің талаптары бойынша

істерді сотта қарау нәтижелеріне назар аудара отырып, осы саладағы қаржылық қызметтерді тұтынушылардың құқықтарын қорғау бойынша мемлекет қабылдап жатқан шаралардың ағымдағы жай-күйі талданады. Атап айтқанда, банктердің интернет-банкингтегі операциялардың қауіпсіздігі үшін клиентке жауапкершілік жүктеу проблемасы және банктің кінәсін дәлелдеудің қиындығы қаралды, соның нәтижесінде зардап шеккен клиенттерді қорғауға ықпал етпейтін теріс сот практикасы қалыптасуда. Мақалада интернет-банкинг клиенттерінің құқықтарын қорғауды күшейту бойынша ұсыныстар берілген.

Түйін сөздер: қаржылық қызметтерді тұтынушылардың құқықтарын қорғау, интернет-банкинг, банк, дербес деректер, ақпараттық қауіпсіздік, әлеуметтік инженерия.

Введение

Согласно Закону РК «О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций» обеспечение надлежащего уровня защиты интересов потребителей финансовых услуг является одной из задач государственного регулирования финансового рынка.

Как указывается на интернет-странице Агентства РК по регулированию и развитию финансового рынка (далее – Агентство/Регулятор) на единой платформе интернет-ресурсов государственных органов [1] в рамках выполнения указанной задачи выявляются практики и процессы финансового рынка, которые «могут навредить интересам потребителей финансовых услуг» и принимаются соответствующие системные и законодательные меры для их устранения.

Данная статья подготовлена с целью выяснения вопроса, насколько комплексно защищены права потребителей финансовых услуг, а именно, клиентов банка в случае использования ими интернет-банкинга.

Под комплексом мер по защите прав банковских клиентов понимаются мероприятия Регулятора как по принятию соответствующих нормативных правовых актов, так и по изучению правоприменительной практики, формировании обзоров такого изучения с целью совершенствования имеющейся нормативной базы, определения направлений взаимодействия с другими государственными органами, а также дачи рекомендаций банкам и их клиентам.

Так, в настоящее время Агентство (до 2020 года – Национальный Банк РК) издает нормативные правовые акты, подробно регламентирующие требования к банкам по информационной безопасности, защите персональных данных клиентов, и постоянно совершенствует методы идентификации/аутентификации клиентов в системах интернет-банкинга.

В рамках мероприятий по повышению финансовой грамотности населения Регулятор регулярно публикует рекомендации в адрес

потребителей по сохранению своих персональных данных, не разглашению реквизитов платежных карт, паролей, CVC-кодов и т.д.

Это важная часть работы, осуществляемая Агентством, направлена на совершенствование технических систем защиты банков и на информирование банковских клиентов о необходимости соблюдения ими мер «самозащиты», но проводится она без учета человеческого фактора, который будет рассмотрен ниже.

В части аналитической информации хотелось бы отметить, что ни Национальным Банком РК, который определяет правила оказания банками электронных банковских услуг, ни Агентством не формируются обзоры по несанкционированным операциям в интернет-банкинге, не определены признаки операций без согласия клиентов, которые могли бы использоваться банками для их приостановления подозрительных операций, не анализируются данные о возмещенных средствах пострадавшим клиентам.

Существующие обзоры Агентства сообщают лишь о количестве обращений потребителей на действия банков, их процентном соотношении в общем количестве обращений по всем финансовым организациям и о количестве принятых мер, без конкретизации нарушений со стороны банков.

Для сравнения: в России Центральный Банк, являющийся регулятором российского финансового рынка, публикует обзоры:

1) об операциях, совершенных без согласия клиентов финансовых организаций [2], в которых сообщает о динамике данных операций, о причинах их совершения (к примеру, в 2020 году методы социальной инженерии составили 68,6%), о предпринимаемых мерах;

2) об инцидентах информационной безопасности при переводе денежных средств [3], в которых приводятся доли возмещенных средств, атак с применением социальной инженерии, фишинговых атак, уязвимостей программного обеспечения;

3) компьютерных атак в кредитно-финасовой сфере [4], в котором приводятся сведения об основных типах атак в кредитно-финансовой сфере, в том числе с использованием социальной инженерии.

В Казахстане отсутствуют судебная статистика и обобщения практики рассмотрения судами данной категории дел, а также не проводятся исследования независимых организаций по вопросам текущего состояния защиты прав клиентов интернет-банкинга и анализа причин, способствующих росту кибермошенничеств.

Вместе с тем, нельзя не отметить проведенный в 2021 году крупнейшим поставщиком услуг кибербезопасности в Центральной Азии - Центром анализа и расследования кибератак анализ защищенности сайтов казахстанских банков, но его целью было выявление уязвимостей

информационных систем банков, которые потенциально могут быть использованы злоумышленниками [5], без изучения правовых проблем.

К примеру, в России судебная практика по делам, связанным с хищениями в интернет-банкинге, проанализирована аналитиками Центра судебных экспертиз компании RTM Group [6]. Это подробное исследование на основе опубликованных данных судов общей юрисдикции и арбитражных судов РФ, несмотря на то, что проведено в 2016 году, остается актуальным и на сегодняшний день, так как выявленные проблемы и причины, способствующие хищениям денежных средств клиентов, существуют и в настоящее время.

В этой связи, статьей в определенной степени восполняются данные пробелы в отношении казахстанской судебной практики. Изучены решения судов по искам клиентов по гражданским делам, связанным с использованием интернет-банкинга, проанализированы причины возникновения данных споров и выработаны определенные рекомендации для судов, регулирующих органов, банков, а также их клиентов.

Таким образом, тема статьи является достаточно актуальной, требует дальнейшего изучения и проведения исследований.

II. Анализ гражданских дел по искам клиентов интернет-банкинга к банкам

Для анализа гражданских дел найдены судебные решения из Банка судебных актов, а также из Судебной базы ИС «Параграф» по ключевым словам «интернет-банкинг», «несанкционированный платеж» и «несанкционированный доступ».

Проанализировано 12 дел по искам, предъявленным к банкам, среди которых 11 исков - с участием или в отношении физических лиц, по 1 иску истцом выступает юридическое лицо.

Изучение гражданских дел, связанных с интернет-банкингом, позволило выделить 2 группы данной категории дел:

1) судебные споры, непосредственно связанные с хищением злоумышленниками денежных средств со счетов клиентов.

Требованиями исков данной группы являются взыскание с банка сумм (ущерба, убытков) или обязывание банка возвратить утраченные суммы. В некоторых случаях истцы требуют также компенсации морального вреда;

2) судебные споры, в которых злоумышленники посредством своих несанкционированных действий возлагают на них исполнение обязательств перед банками и одновременно неосновательно обогащаются (оформление кредитов).

Исковым требованием данной группы, как правило, является признание недействительными кредитных договоров.

В 75% изученных дел суд отказал в удовлетворении требований клиентов.

Необходимо отметить следующие моменты, определяющие заранее проигрышное положение пострадавших клиентов в спорах с банками:

В первую очередь, это договоры, изначально составленные в пользу банка, позволяющие ему снять с себя ответственность в результате мошенничеств. Так, в решении по иску К.К. к ДБ АО «Сбербанк» о взыскании суммы приводятся договорные положения, в силу которых банк не несет ответственность в случае, если информация о счетах клиента, логинах, идентификаторах, паролях системы интернет-банкинга становится известной «третьим лицам в результате недобросовестного выполнения клиентом условий их хранения и использования» [7].

О виновности клиента в восприимчивости атакам социальной инженерии (методам психологического воздействия на человека с целью завладения его конфиденциальной информацией, необходимой для получения доступа к счетам) упоминают и зарубежные авторы, при этом отмечая, что «банки также должны разделить ответственность за то, чтобы их клиенты не становились жертвами таких атак» [8].

Во вторую очередь, это сложность доказывания вины банка в причинении вреда. В данном случае следует отметить, что клиент банка, являясь слабой стороной договора, не обладает необходимыми знаниями в области интернет-технологий и не располагает необходимыми инструментами для доказывания фактов непринятия банком достаточных мер информационной безопасности для защиты денежных средств клиента.

Судами не исследуются вопросы текущего состояния систем информационной безопасности банков, их уязвимостей или нарушений со стороны банков и не назначаются соответствующие судебные экспертизы для выяснения данных вопросов.

В то же время, необходимо отметить, что даже в случаях принятия банком требуемых мер информационной безопасности, внедрения и совершенствования антифрод-процедур, проведения информационной работы для предупреждения клиентов о мошенничествах, хищения денег клиента зачастую совершаются при содействии самого клиента под воздействием атак социальной инженерии.

Так, выяснение причин, повлекших денежные потери клиентов, позволило выделить 4 группы дел с определением процентного соотношения каждой из них в общем количестве:

Как видно из диаграммы, большая часть клиентов (41,66%) самостоятельно подключили номера телефонов мошенников к функции доставки СМС-паролей в интернет-банкинге, вследствие чего мошенники смогли получить полный доступ к счетам клиентам.

В финансовой среде дискутируются вопросы, может ли банк обеспечить защиту клиентов от социальных хакеров, и если может, то каким образом [10].

Некоторые данные позволяют сделать вывод, что банки могут посредством совершенствования антифрод-процедур значительно снизить количество транзакций, совершаемых с помощью социальной инженерии.

К примеру, казахстанский Альфа-Банк «с помощью системы «Антифрод» зафиксировал более 20 тыс. событий с подозрением на мошенничество, каждое из которых было обработано в режиме онлайн…В 2020 году банку удалось предотвратить потери клиентов на сумму более 780 млн тенге, распознав несанкционированное вмешательство третьих лиц в процесс проведения операций» [11].

В России с внесением изменений в Федеральный закон «О национальной платежной системе», обязывающих оператора возмещать клиенту суммы мошеннических операций (совершенных без согласия клиента), «практически все банки внедрили у себя антифрод-системы» [12].

О положительных результатах использования антифрод-процедур и информационной работы с клиентами при помощи рассылок, через радио и телевидение также сообщают российские Тинькофф Банк и Московский кредитный банк, которые отмечают отсутствие всплеска хищений [13].

Предложения по повышению уровня защиты прав клиентов интернет-банкинга

Судебная практика – лишь результат (следствие) правоприменения, в связи с чем, необходимо устранять причины, способствующие мошенничествам: нормативная база, не поспевающая за постоянно совершенствующими методами мошенников, договорные положения банков, возлагающие всю ответственность на клиента за необеспечение сохранности конфиденциальных сведений, а также низкая цифровая, финансовая и правовая грамотность населения.

В этой связи, необходимо внедрение системного подхода, включающего следующие меры по усилению защиты прав клиентов интернет-банкинга:

1) судам:

регулярно обобщать практику споров, связанных с использованием услуг интернет-банкинга, на республиканском уровне, с выработкой рекомендаций, предложений и памяток для всех лиц, использующих интернет-банкинг;

разработать нормативное постановление в целях формирования единообразной судебной практики при рассмотрении данной категории дел с рекомендациями по изучению/оценке состояния систем информационной безопасности банка, наличия антифрод-процедур, в том числе посредством назначения судебных экспертиз;

2) Национальному Банку и Агентству для формирования эффективных подходов решения проблем клиентов интернет-банкинга:

формировать статистику и обзоры операций, совершенных без согласия клиентов, а также обзоры инцидентов информационной безопасности для выработки необходимых мер, в том числе издания соответствующих нормативных правовых актов и рекомендаций для банков;

изучать международный опыт предотвращения мошенничеств в интернет-банкинге, усиливать требования информационной безопасности к банкам и внедрять правовые способы борьбы с социальной инженерией;

на постоянной основе проводить работу по повышению финансовой киберграмотности населения;

3) банкам второго уровня внедрять и совершенствовать антифрод-процедуры, которые позволят приостанавливать не специфичные для клиента операции (по размерам сумм, регулярности, частоте переводов и т.д.), вводить дополнительные проверки при проведении таких операций;

4) клиентам банков повышать свою финансовую киберграмотность, более внимательно и осторожно относиться к своим персональным данным: логинам, паролям и кодам для безопасного использования услуг интернет-банкинга.

Заключение

Подводя итог, следует отметить, что в вопросах защиты прав клиентов интернет-банкинга необходимо совершенствование законодательства не только в части ужесточения технических требований по информационной безопасности банков и защиты персональных данных их клиентов. В связи с постоянно совершенствующими мошенническими схемами необходимо учитывать психологию человека и работать над внедрением правовых способов борьбы с методами социальной инженерии.

Список использованной литературы

1 Сайт АРРФР [Электронный ресурс] / Защита прав потребителей финансовых услуг - Режим доступа: GOV.KZ (www.gov.kz) - свободный. - Загл. с экрана.

2 Банк России [Электронный ресурс] / Обзор операций, совершенных без согласия клиентов финансовых организаций за 2020 год - Режим доступа: review_of_transactions_2020.pdf (cbr.ru) – свободный. – Загл. с экрана.

3 Банк России [Электронный ресурс] / Обзор отчетности об инцидентах нформационной безопасности при переводе денежных средств II квартал 2021 года – Режим доступа: Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств | Банк России (cbr.ru) – свободный. – Загл. с экрана.

4 Банк России [Электронный ресурс] / Основные типы компьютерных атак в кредитно-финансовой сфере в 2019–2020 годах – Режим доступа: attack_2019-2020.pdf (cbr.ru) – свободный. – Загл. с экрана.

5 Центр анализа и расследования кибер атак [Электронный ресурс] / Результаты анализа защищенности веб-ресурсов банков второго уровня Республики Казахстан 2021 - Режим доступа: https://cert.kz/files/reports/kz-banks-security-report-webtotem-2021.pdf – свободный. – Загл. с экрана.

6 RTM Group [Электронный ресурс] / Анализ судебной практики за 2016 год по спорам в результате хищений через каналы ДБО - Режим доступа: https://www.securitylab.ru/analytics/485706.php – свободный. – Загл. с экрана.

7 Банк судебных актов [Электронный ресурс] / Режим доступа: Судебный кабинет (sud.kz) / Аналогичное дело рассматривалось

также российским судом: Поиск решений судов общей юрисдикции (xn--90afdbaav0bd1afy6eub5d.xn--p1ai)

8 Ivaturi, K., & Janczewski, L. (2013). Social engineering preparedness of online banks: An Asia-Pacific perspective. Journal of Global Information Technology Management, 16(4), 21–46. - Режим доступа: https://doi.org/10.1080/1097198X.2013.10845647

9 Кузнецов М. В. Социальная инженерия и социальные хакеры. – БХВ-Петербург, 2007.- 430 с.

10 Журнал «ПЛАС» [Электронный ресурс] / Социальная инженерия против банковских клиентов. Причины «успеха» и способы защиты – Режим доступа: Социальная инженерия против банковских клиентов. Причины «успеха» и способы защиты » Журнал ПЛАС №6 (plusworld.ru) - свободный. – Загл. с экрана.

11 Сайт Kursiv.kz [Электронный ресурс] – Режим доступа: Альфа-Банк — №1 по защищенности в Казахстане | Курсив - бизнес новости Казахстана (kursiv.kz) - свободный. – Загл. с экрана.

12 Доктор Веб [Электронный ресурс] / Выпуск 20 ноября 2017.– Режим доступа: Антифрод: эффективен, но не всемогущ (drweb.ru) - свободный. – Загл. с экрана.

13 Мартыненко Н.Н., Овчаренко А.В. МОШЕННИЧЕСТВО В СФЕРЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ И МЕТОДЫ БОРЬБЫ С НИМ В УСЛОВИЯХ ПАНДЕМИИ // Инновации и инвестиции. 2020. №12. URL: https://cyberleninka.ru/article/n/moshennichestvo-v-sfere-distantsionnogo-bankovskogo-obsluzhivaniya-i-metody-borby-s-nim-v-usloviyah-pandemii (дата обращения: 20.11.2021)