ЦЕНТРАЛЬНЫЙ БАНК
РОССИЙСКОЙ ФЕДЕРАЦИИ
(Банк России)

107016, Москва, ул. Неглинная, 12
www.cbr.ru
тел. (499) 300-30-00

Кредитным организациям,
некредитным финансовым
организациям

От 12.02.2020 № ИН-014-56/6

на от

Информационное письмо о проверке кредитными организациями и некредитными финансовыми организациями принадлежности клиенту адреса электронной почты

В целях противодействия осуществлению переводов денежных средств без согласия клиента, незаконных финансовых операций Банк России рекомендует кредитным организациям и некредитным финансовым организациям в случае направления посредством электронной почты уведомлений, предусмотренных абзацем четырнадцатым пункта 5.2.1 Положения Банка России от 17 апреля 2019 года № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента», абзацем четвертым пункта 11.4 Положения Банка России от 17 апреля 2019 года № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций», реализовывать механизм подтверждения принадлежности клиенту адреса электронной почты, на который кредитной организацией (некредитной финансовой организацией) осуществляется направление указанных уведомлений (далее – механизм подтверждения адреса электронной почты).

В качестве меры, создающей условия для реализации механизма подтверждения адреса электронной почты, кредитным организациям

(некредитным финансовым организациям) рекомендуется осуществлять проверку принадлежности клиенту абонентского номера подвижной радиотелефонной связи, сообщенного кредитной организации (некредитной финансовой организации) клиентом (далее – подтвержденный номер телефона).

Механизм подтверждения адреса электронной почты кредитным организациям (некредитным финансовым организациям) рекомендуется реализовывать следующим образом:

при сообщении кредитной организации (некредитной финансовой организации) клиентом адреса электронной почты (в случае изменения адреса электронной почты клиента – нового адреса электронной почты клиента) способом, позволяющим идентифицировать получателя сообщения, информационная система кредитной организации (некредитной финансовой организации) проводит поиск сообщенного клиентом адреса электронной почты среди адресов электронной почты других клиентов кредитной организации (некредитной финансовой организации) и в случае выявления совпадения адресов электронной почты фиксирует информацию о том, что сообщенный клиентом адрес электронной почты не подтвержден;

в случае неподтверждения сообщенного клиентом адреса электронной почты кредитная организация (некредитная финансовая организация) уведомляет об этом клиента способом, позволяющим идентифицировать получателя уведомления;

в случае несовпадения сообщенного клиентом адреса электронной почты с адресами электронной почты других клиентов кредитной организации (некредитной финансовой организации) информационная система кредитной организации (некредитной финансовой организации) формирует уникальную ссылку для подтверждения принадлежности клиенту адреса электронной почты совместно с графическим кодом подтверждения (далее – ссылка верификации адреса электронной почты) и направляет ее по сообщенному клиентом адресу электронной почты, а также формирует код короткого текстового сообщения (далее – код СМС) и направляет его на подтвержденный номер телефона клиента;

в случае перехода клиента по ссылке верификации адреса электронной почты на сайт кредитной организации (некредитной финансовой организации) и ввода на сайте кредитной организации (некредитной финансовой организации) кода СМС, соответствующего коду СМС, направленному кредитной организацией (некредитной финансовой

организацией) на подтвержденный номер телефона клиента, а также корректного графического кода подтверждения принадлежность адреса электронной почты клиенту кредитной организации (некредитной финансовой организации) считается подтвержденной.

При реализации механизма подтверждения адреса электронной почты кредитным организациям (некредитным финансовым организациям) рекомендуется:

1. Использовать ссылки верификации адреса электронной почты, имеющие:

уникальную последовательность символов для защиты от перебора и угадывания,

срок действия, определенный во внутренних документах кредитной организации (некредитной финансовой организации), разработанными в рамках системы управления рисками кредитной организации (некредитной финансовой организации) (далее – срок действия),

соответствие только подтверждаемому адресу электронной почты клиента в течение всего срока действия.

2. Использовать коды СМС, имеющие случайную последовательность цифр для защиты от перебора и угадывания, срок действия, а также обеспечивать ограниченное количество попыток ввода кода СМС.

3. Использовать формы ввода данных, обеспечивающие ограничение доступа автоматизированных (роботизированных) систем к вводу кода СМС и графического кода подтверждения.

4. Обеспечивать удаление не подтвержденных адресов электронной почты клиента из информационной системы кредитной организации (некредитной финансовой организации) по истечении срока действия ссылки верификации адреса электронной почты или в случае превышения количества попыток ввода кода СМС.

Настоящее информационное письмо подлежит размещению на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет».

Заместитель Председателя Д.Г. Скобелкин