**Страхование банковской карты от мошенников: а стоит ли ее оформлять?**

Несмотря на то, что банковские счета и средства платежа (банковские карты) обеспечены достаточным уровнем защиты, случаи хищений средств продолжают пополнять криминальную статистику. Преобладающее большинство таких инцидентов происходит с использованием социальной инженерии, когда владелец счета/карты вводится в заблуждение и сообщает мошенникам необходимую для доступа к счету информацию, либо самостоятельно отправляет свои деньги злоумышленнику. Может ли клиент банка вернуть похищенные деньги? Об этом в интервью [АиФ](https://aif.ru/money/mymoney/bank_predlagaet_strahovku_karty_ot_moshennikov_stoit_li_ee_pokupat) рассказала эксперт центра финансовой грамотности НИФИ Минфина России Ольга Дайнеко.

Может, но только при условии, что он не передавал злоумышленнику данные карты, пин-коды и CVV|CVC, не вводился (самим владельцем или мошенником-не важно) код из СМС/push и не совершались иные действия по предоставлению доступа к счету. Либо возврат средств возможен в случае вины банка (не заблокировали карту/счет после сообщения об утере, не уведомил о совершении операции по счету, перечислил средства после сообщения клиента о хищении/утери карты, допустил уменьшение средств клиента по остатку на счете с признаками совершения операции без согласия клиента/зачислил на счет из базы ФинЦЕРТ).

Нередко банки предлагают обезопасить себя от непредвиденных ситуаций и приобрести страховку банковских карт. Чаще всего страхование оформляется в виде подписки: застрахован, пока платишь ежемесячный платеж по выбранному страховому пакету, прекращение выплат позволяет прекратить и страхование. Есть страховые полисы с оплатой страхового вознаграждения сразу за обозначенный период (например, на год). Подписка часто обходится дороже годового полиса (при равном страховом покрытии), но позволяет самостоятельно выбирать срок страхования и при необходимости-прекращать его. Перечень рисков по данным страховым продуктам примерно одинаков. Традиционно это:

- кража/потеря банковской карты (когда карта физически у злоумышленника, и он ей воспользовался);

- похищение средств при помощи технических устройств (например, скиммера- накладки на клавиатуру банкомата, считывающей пин-код во время снятия наличных).

- потеря денег в результате оплаты на фишинговом сайте, а также в случае деятельности вредоносного/вирусного программного обеспечения, взлома и в случае несанкционированного доступа к средствам по незащищенному Wi-Fi;

-в случае грабежа или разбойного нападения (когда отобрали деньги после получения их в банкомате в течение 12 (иногда-48) часов после снятия со счета).

Выбирая страховку, важно внимательно читать условия страхования, изучить договор/условия пакета страхования: изучить перечень рисков и способы подтверждения страхового события для выплаты страхового возмещения, а также размер выплаты по разным обстоятельствам страхового события (например, может оказаться, что снятие денег в банкомате в ночное (а не дневное) время уменьшит размер страховой выплаты).

Сам факт наличия страхования не должен расслаблять застрахованного: безответственное хранение пин-кодов карты, передача ее в чужие руки, несвоевременное сообщение о страховом событии, самостоятельное перечисление денег мошенникам часто находятся в перечне, относящемся к нарушению договора страхования и будет причиной отказа в страховом возмещении. Поэтому наличие страховки-не повод терять здравомыслие и пренебрегать базовыми правилами финансовой безопасности

Нужно ли приобретать такую страховую защиту-вопрос спорный: при хищении средств с помощью социальной инженерии (когда владелец карты сознательно проводит операцию и подтверждает ее необходимыми действиями) получить страховое возмещение не всегда возможно (нередко сложно документально подтвердить факт мошенничества). Кроме того, если часть страховых рисков/покрытий по ним пересекаются с обязанностью возмещения ущерба самим банком-стоит ли оплачивать такой страховой риск.

Впрочем, нельзя однозначно утверждать, что страхование банковских карт – продукт бесполезный. Мошенничество со списанием средств без ведома и помощи владельца имеют место, как есть и риск ограблений у банкоматов. Словом, все то, что «не покрыто» законом о национальной платежной системе, когда иными способами часто вернуть похищенное невозможно, страхование может покрыть нанесенный ущерб хотя бы в части.

Еще в апреле этого года Банк России опубликовал обращение, в котором рекомендует банкам при выявлении нетипичных операций по картам и счетам временно приостанавливать дистанционный доступ к управлению счетом для усложнения вывода этих денег мошенниками и повышения возможности их возврата владельцу счета. Клиент при этом должен уведомляться о причине приостановки, а возобновление операций происходит после личного обращения клиента в банк.

Кроме того, с конца сентября 2018 г. операторы по переводу денежных средств в случае наличия признаков перевода денег без согласия клиента обязаны приостанавливать выполнение такой операции.

Банк России формирует базу (ФинЦЕРТ), куда вносятся подозрительные счета и устройства, «замеченные» и попытках осуществления перевода денежных средств без согласия клиента. Перевод на счет, значащийся в этой базе, предварительно блокируется для возможности возврата средств потенциальному потерпевшему. Кроме того, к признакам переводов без согласия клиента относятся случаи, когда параметры устройства, с использованием которого производится перевод, совпадают с параметрами устройства, внесенного в указанную базу данных.

С 20 октября 2022 г. МВД получило доступ к базе ФинЦЕРТ для возможности пополнения базы по результатам правоохранительной деятельности и оперативного обмена сведениями о подозрительных операциях в онлайн-режиме без дополнительных запросов.