

Уголовная ответственность за мошенничество с использованием информационно-телекоммуникационной сети «Интернет»

Переход на дистанционный формат работы, получение государственных услуг через удаленные сервисы и появление новых информационных технологий с одной стороны свидетельствуют о развитии, с другой стороны вместе с развитием должны быть предоставлены правовые механизмы защиты прав граждан, которые используют данные технологии.

Рост числа атак на клиентов банков, частые звонки мошенников связаны, в том числе, с развитием информационных и телекоммуникационных технологий. Все больше потребителей совершают покупки онлайн, расплачиваются картой и меньше пользуются банкоматом. При этом появляются новые и работающие схемы мошенничества, которые не требуют особой квалификации или вложений средств. Например, распространенный способ - звонки от якобы сотрудников банка с просьбой перевести деньги на защитный счет, чтобы их сохранить.

В настоящее время увеличивается розничная торговля в режиме онлайн. Отличительная черта этого вида мошенничества – низкая цена на определенный товар и отсутствие фактического адреса или телефона продавца. В этом случае предлагается подделка, некачественный товар либо деньги покупателей просто присваиваются, а товар не доставляется.

Чтобы не стать жертвой мошенников необходимо соблюдать правила цифровой или компьютерной гигиены, сохранять бдительность, использовать сложные и разные пароли.

При каждой оплате товаров или услуг с помощью электронных средств платежа необходимо помнить следующие правила: не использовать подозрительные Интернет-сайты, подключить Интернет-банк и СМС-оповещение, не сообщать данные своей карты другим людям, в том числе банковским служащим, работникам интернет-магазинов, при возможности открыть отдельную карту, на которой хранить определенную сумму денежных средств для осуществления безналичных платежей.

Основная задача граждан при принятии решения о приобретении товара через Интернет-магазин, поступлении посредством сотовой связи просьбы об оказании помощи в связи с непредвиденными обстоятельствами, сложившимися с их родственниками, быть осмотрительными и проверить доступным способом поступающую информацию, прежде чем перечислять денежные средства в адрес злоумышленников.

За мошенничество с использованием электронных средств предусмотрена уголовная ответственность (статья 159.3 Уголовного кодекса Российской Федерации).

Электронное средство платежа согласно Федеральному закону от 27.06.2011 № 161-ФЗ «О национальной платежной системе» признается средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

Также предусмотрена уголовная ответственность за мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей (статья 159.6 Уголовного кодекса Российской Федерации).

В зависимости от тяжести совершенного преступления Уголовным кодексом Российской Федерации за преступления, связанные с указанными видами мошеннических действий, предусмотрено наказание в виде штрафа, обязательных, исправительных и принудительных работ, либо лишением свободы до 10 лет.

Уголовная ответственность за хищение электронных денежных средств

Хищения денежных средств с банковского счета получили в последнее время большое распространение.

Пункт «г» части 3 статьи 158 Уголовного кодекса Российской Федерации предусматривает ответственность за кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 УК РФ — мошенничество с использованием электронных средств платежа).

Под хищением уголовный закон понимает совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества.

Тайным признается хищение чужого имущества, когда лицо совершает незаконное изъятие имущества в отсутствие собственника или иного владельца этого имущества, или посторонних лиц либо хотя и в их присутствии, но незаметно для них.

В силу статьи 15 УК РФ преступление, предусмотренное пунктом «г» части 3 статьи 158 УК РФ, относится к категории тяжких преступлений. Максимальное наказание за его совершение — лишение свободы на срок до 6 лет со штрафом в размере до 80 тысяч рублей или в размере заработной платы или иного дохода осужденного за период до 6 месяцев, либо без такового и с ограничением свободы на срок до 1,5 лет либо без такового.

- ст.159.3 УК РФ предусматривает ответственность за мошенничество с использованием электронных средств платежа. Преступление, предусмотренное ч. 1 ст. 159.3 УК РФ относится к категории преступлений небольшой тяжести)

Квалифицированными составами мошенничества с использованием электронных средств платежа являются: ч. 2 ст. 159.3 УК РФ - относится к преступлениям средней тяжести, и ч.3, ч. 4 ст. 159.3 УК РФ - тяжкие преступления).

Приведённые составы преступлений отличаются способом совершения преступления.

Пункт «г» ч.3 ст.158 УК РФ предусматривает ответственность за тайное хищение денежных средств с банковского счёта или электронных денежных средств (например, виновное лицо тайно похитило банковскую карту с пин-кодом к ней, после чего через устройство самообслуживания сняло денежные средства с банковского счёта потерпевшего).

Статья 159.3 УК РФ предусматривает ответственность в случае, когда виновное лицо похищает чужое имущество или приобретает право на чужое имущество при обмане или злоупотреблении доверием, под воздействием которых владелец имущества или иное лицо передают имущество или право на него другому лицу либо не препятствуют изъятию этого имущества или приобретению права на него другим лицом.

В соответствии с разъяснениями постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 года №48 «О судебной практике по делам о мошенничестве, присвоении и растрате» в случае, когда хищение имущества осуществлялось с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты, путем сообщения уполномоченному работнику кредитной, торговой или иной организации заведомо ложных сведений о принадлежности указанному лицу такой карты, преступление должно квалифицироваться, как мошенничество.

В случаях, когда лицо похитило безналичные денежные средства, воспользовавшись необходимой для получения доступа к ним конфиденциальной информацией держателя платежной карты (например, персональными данными владельца, данными платежной карты, контрольной информацией, паролями), переданной злоумышленнику самим держателем платежной карты под воздействием обмана или злоупотребления доверием, действия виновного квалифицируются как кража.

Усиление ответственности за совершение хищений с банковского счёта, а также электронных денежных средств связано с расширением применения информационных технологий в финансовом секторе. Следует отметить, что число указанных противоправных деяний продолжает непрерывно увеличиваться. Высокая степень общественной опасности таких противоправных деяний подтверждается спецификой преступлений, совершить которые могут лишь лица, обладающие специальными знаниями и использующие технические средства именно в криминальных целях, что приводит к нарушению не только права собственности, но и банковской тайны.