Сведения
о видах и способах совершения преступлений, связанных с мошенническими действиями, совершаемыми с использованием телекоммуникационных и информационных технологий

Проведенным анализом возбужденных в 2019 году на территории Республики Адыгея уголовных дел по преступлениям, связанных с мошенническими действиями, совершенными с использованием телекоммуникационных и информационных технологий, а также зарегистрированных в КУСП материалов по сообщениям о преступлениях данной категории, можно выделить несколько наиболее распространенных способов совершения мошенническими действиями рассматриваемой категории:
«Проблема у родственника (знакомого)»;
«Банковская карта заблокирована» или иные проблемы с банковским счетом (пластиковой картой);
«Купля-продажа товара через интернет-сайты» (например: «Авито»);
«Под видом сотрудника правоохранительных органов»;
«Помощь в получении кредита, трудоустройстве и т.п.»;
«Взлом страницы в социальной сети»;
«Вредоносная программа (вирус)»;
«Выигрыш приза, лотереи и т.п.»;
«Под предлогом оказания медицинских услуг».

1. «Проблема у родственника (знакомого)»: Преступник осуществляет звонок на телефон (мобильный, стационарный) потерпевшего и сообщает о том, что у его родственника (знакомого) проблема (попал в ДТП, участвовал в драке, задержан с наркотиками, иное). Далее преступник предлагает разрешить проблему, для чего просит перечислить денежные средства. Потерпевший, поверив в то, что родственник попал в беду, соглашается и следует дальнейшим указаниям преступника. Далее преступник, как правило, просит потерпевшего подойти к банкомату (терминалу), где сообщает ему номер телефона либо банковской карты, на которые необходимо осуществить перевод денежных средств. Потерпевший с помощью банкомата (терминала) осуществляет перевод денежных средств на номера телефонов либо банковские счета, указанные ему преступником.
2. «Банковская карта заблокирована» или иные проблемы с банковским счетом (пластиковой картой): Потерпевшему поступает звонок, либо он получает СМС - сообщение с текстом «Ваша карта заблокирована». СМС-сообщения от мошенников, как правило, могут содержать информацию о блокировке банковской карты, о совершенном переводе средств или другую информацию,

побуждающую клиента перезвонить на указанный в сообщении номер телефона для уточнения информации. Перезвонившему держателю карты преступник представляется сотрудником службы безопасности банка, специалистом службы технической поддержки и в убедительной форме предлагает подойти к ближайшему банкомату. Потерпевший, дойдя до банкомата, созванивается с преступником и выполняет все его действия, в результате которых, впоследствии, злоумышленник получает доступ к счетам потерпевшего.

3. «Купля-продажа товара через интернет-сайты» (например: «Avito»); При совершении данного вида мошенничеств могут быть использованы различные сайты и интернет-магазины, основной целью преступника является получение информации о карте, для получения доступа в личный кабинет Сбербанк Онлайн, подключение услуги Мобильный банк к карте, для завладения деньгами потерпевшего. Например: к продавцу, разместившему объявление на сайте бесплатных объявлений «Avito» поступает звонок от преступника, который сообщает о готовности купить товар, при этом, под различными предлогами (например, перечислить задаток на карту продавца) выясняет личные данные, номер и код банковской карты, срок его действия, либо просит сообщить пароли и коды доступа, полученные потерпевшим в СМС - уведомлении, что дает возможность получить доступ к счетам потерпевшего.

Другой пример мошенничества, совершаемого с использованием сайта «Avito»: преступник размещает на сайте объявление о продаже товара. Потерпевший, желая приобрести товар, звонит преступнику по контактному номеру, указанному в объявлении, либо вступает с ним в переписку. Преступник в ходе беседы (переписки) сообщает, что для отправки (пересылки) потерпевшему товара по почте необходимо оплатить его полную (частичную) стоимость. Потерпевший перечисляет денежные средства на абонентские, банковские либо электронные счета, указанные преступником. После получения предоплаты преступник скрывается, не выполняя свои обязательства.

4. «Под видом сотрудника правоохранительных органов»: Преступник звонит на абонентский номер потерпевшего и представляется сотрудником правоохранительных органов, например работником прокуратуры. В ходе разговора преступник предлагает приехать в здание прокуратуры (основанием вызова могут быть различные причины, например выявленные недостатки при прокурорской проверке организации), по пути, как правило, просит купить дорогостоящий алкоголь и продукты для проверяющих из Москвы, которые находятся в

его кабинете. Далее в ходе разговора просит перечислить деньги на определенные абонентские номера, обещая вернуть деньги по приезду. По просьбе преступника потерпевшие переводят денежные средства на абонентские номера либо другие счета указанные преступником. По прибытию в прокуратуру потерпевшие узнают, о том, что они стали жертвами мошенников.

5. «Помощь в получении кредита, трудоустройстве и т.п.»: Преступник размещает объявления о предоставлении работы в Администрации, прокуратуре, полиции, и т.д. При этом обязательным условием устройства на работу является внесение денег за заключение договора. После перечисления денег преступник перестает выходить на связь. Общение с преступником может происходить как по телефону, так и в ходе переписки.

Другим способом хищения денег является мошенничество под предлогом оказания помощи в получении кредита. Преступник размещает в интернете объявления об оказании помощи в получении кредита в различных банках, в том числе с плохой кредитной историей. Потерпевший вступает с ним в переписку, либо созванивается по телефону. В ходе общения преступник просит перечислить деньги необходимые для оформления и получения кредита: проценты, страховой взнос, оплата услуг курьера, прочее. После получения денег преступник скрывается.

6. «Взлом страницы в социальной сети»: Преступник путем взлома получает доступ к странице потерпевшего в социальной сети (ВКонтакте, Одноклассники, Инстаграмм и другие) и от его имени вступает в переписку с родственниками и друзьями и под различными предлогами просит предоставить реквизиты банковской карты, пароли и коды смс-уведомлений. После того как потерпевший сообщает информацию преступнику, последний получает доступ к счетам потерпевшего. Также преступник, переписываясь от имени друга (родственника) со «взломанной страницы» может попросить денежные средства в долг, при этом, как правило, для того чтобы избежать разоблачения преступник сообщает, что его телефон сломался и общение возможно только путем переписки через интернет.

7. «Вредоносная программа (вирус)»: В данном случае преступниками используется вредоносная программа, которая самостоятельно рассылает СМС с телефона потерпевшего. Данная программа устанавливается на телефон при получении СМС или ММС сообщений, а также при входе на различные сайты в интернете.

На мобильный телефон абонента поступают сообщения со ссылками на различные сайты, при переходе по которым происходит заражение телефона, который получил данное сообщение. Возможно получение потерпевшим СМС с номера 900 о различной информации, которую он не запрашивал. Одним из причин списания денежных средств, при таком способе хищения денег со счетов, является отсутствие на мобильном телефоне антивирусной программы.

8. «Выигрыш приза, лотереи и т.п.»

Преступник осуществляет звонок на телефон потерпевшего и сообщает, что он выиграл ценный приз, лотерею и т.д. (либо на телефон потерпевшего поступает сообщение о выигрыше приза, лотереи т.д.). Далее преступник в ходе общения с потерпевшим сообщает, что для получения приза необходимо заплатить определенную сумму денег (например: оплата доставки, налог и т.д.). Потерпевший, поверив преступнику, соглашается и следует его инструкциям, в результате чего осуществляет перевод денежных средств на указанные им счета, после получения денег преступник скрывается.

9. «Под предлогом оказания медицинских услуг»:

Как правило, жертвами данного вида мошенничества являются пожилые люди. Преступник осуществляет звонок на телефон потерпевшего и, представляется сотрудником здравоохранения. В ходе разговора он убеждает потерпевшего о наличии у него серьезного заболевания, требующего медицинского обследования и лечения. Потерпевший с целью оказания ему медицинских услуг перечисляет денежные средства преступнику, на лечение, либо оплату лекарственных препаратов, биологически активных добавок (БАДов). После получения денежных средств преступники скрываются, не выполняя свои обязательства.