**Наиболее распространены способы совершения преступлений**

**1. «Предоплата» (обман продавца)**

Суть данного способа заключается в том, что злоумышленник выступает в роли покупателя. На одной из интернет-площадок с объявлениями он находит продавца и копирует его контактные данные. После чего ищет его в мессенджерах (социальных сетях), представляясь покупателем. В ходе переписки, злоумышленник сообщает, что товар ему понравился и он хочет его приобрести в связи с чем уже якобы совершил предоплату (зачастую высылается скриншот электронного карт-чека о перечислении средств). Для того, чтобы получить данные средства продавцу высылают ссылку на поддельную страницу (она выглядит как один из разделов официального сайта интернет-площадки или банковского учреждения), где продавцу нужно ввести номер своей карты, имя держателя, срок действия, CVV-код указанный на оборотной стороне карты (информацию, содержащуюся в СМС-сообщении, поступившем из банка, для подтверждения получения предоплаты). После получения конфиденциальных сведений, злоумышленник совершает хищение средств.

**2. «Доставка» (обман покупателя)**

Злоумышленник размещает объявление на интернет-площадке о продаже товара по крайне выгодной цене. После того, как потенциальный покупатель начинает вести переписку во внутреннем чате площадки, злоумышленник под различными предлогами убеждает его продолжить общение в мессенджере или социальной сети. Во время общения мошенник уговаривает покупателя внести предоплату или оформить доставку, и чтобы развеять сомнения покупателя, сообщает о якобы новой услуге удержания (холдирования) средств, которая появилась на торговой площадке, т.е., если доставка не произойдет, то торговая площадка автоматически вернет средства на карту. При этом покупателю высылается ссылка на поддельную страницу, которая имитирует официальную страницу торговой площадки или интернет-банкинга, где нужно ввести данные карты (далее осуществляются действия по схеме обмана продавца).

**3. Использование социальных сетей**

Осуществив несанкционированный доступ к персональным аккаунтам пользователя сети Интернет, злоумышленник рассылает всем виртуальным «друзьям» потерпевшего просьбу под различными предлогами сообщить реквизиты банковской платежной карты. Это может быть ее фото или просто номер, срок действия и иные реквизиты, при этом, хоть в большинстве своем школьники банковских карт не имеют, но желая помочь «другу» очень часто используют карты своих родственников и друзей. Порой преступники просят просто номер мобильного телефона и либо пытаются похитить со счета телефона деньги или наоборот используют его как промежуточное звено, направляя на этот счет чужие деньги, переводя их затем дальше, чтобы запутать свои следы (практически во всех случаях хищения денежных средств со счетов мобильных телефонов потерпевшие еще сообщали преступнику персональные коды, приходящие в виде смс-сообщений на телефон).

**4. Звонок от «представителя» банка с просьбой срочно предоставить необходимую информацию**

Преступники от имени сотрудников банка сообщают, что необходимо осуществить какие-либо действия с банковской платежной картой, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит или производит подозрительную оплату. Для маскировки преступники используют функцию «подмены номера», как следствие у потерпевшего на экране мобильного телефона может отображаться совершенно любой абонентский номер телефона, заданный злоумышленником. Это могут быть номера банковских учреждений или иных абонентов, которые на самом деле никому звонки не осуществляют, а сам звонок по своим внешним признакам ничем не будет подозрительным. Получив необходимую информацию о реквизитах карты, преступники осуществляют хищение.