Финансы , 16 сен, 05:00 86 875

Мошенники перевели деньги клиентов Сбербанка на счет «Трансконтейнера»

Эксперты полагают, что это может быть частью новой схемы по выводу средств с карт
Неизвестные перевели на счета «Трансконтейнера» свыше 3 млн руб., сообщила компания. Часть из них принадлежит клиентам Сбербанка, узнал РБК.
Использование счета юрлица может быть новой схемой мошенничества, говорят эксперты

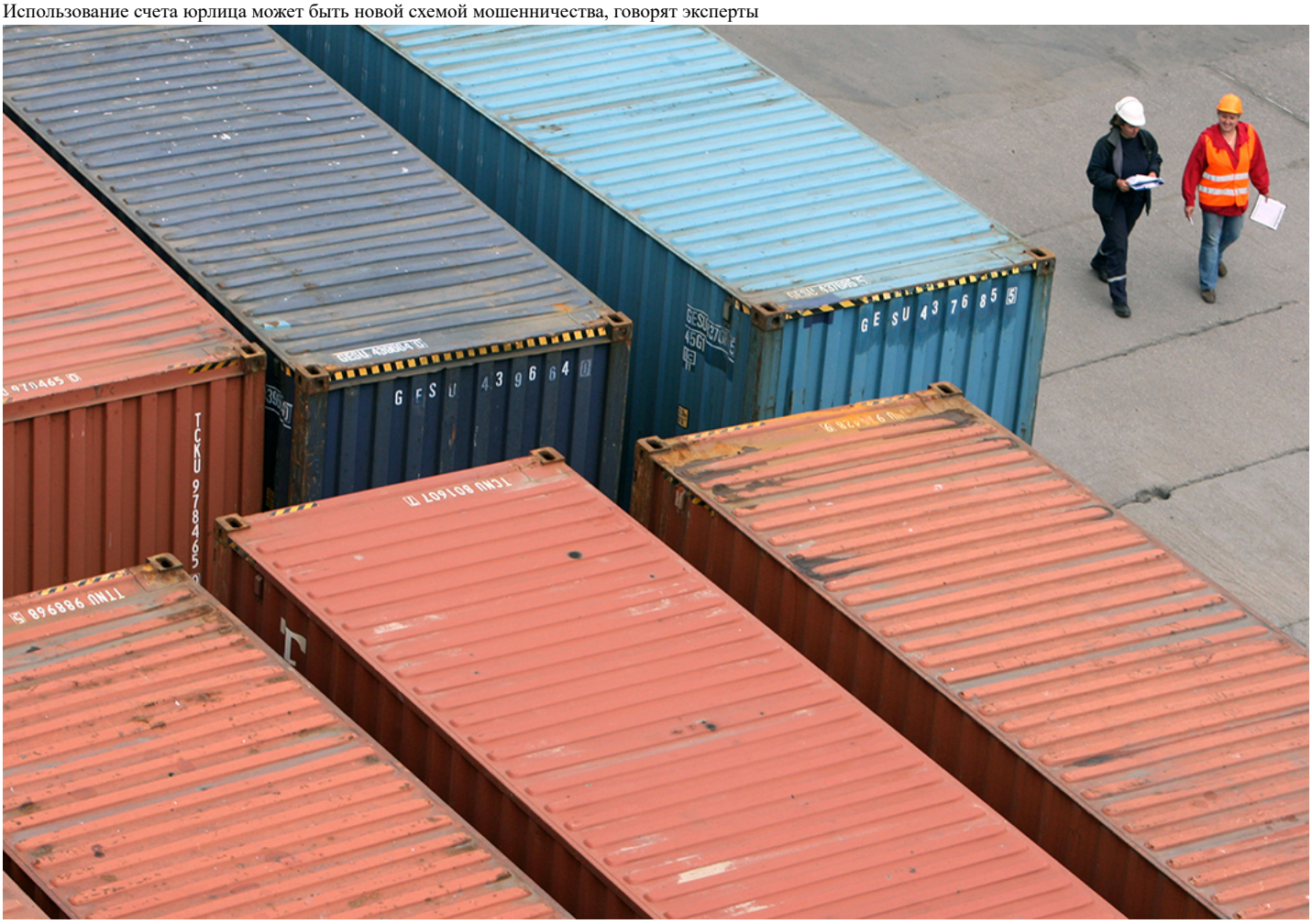


Фото: Игорь Заремба / РИА Новости

Мошенники переводили украденные средства банковских клиентов на счета крупнейшего в России контейнерного оператора «Трансконтейнер» (принадлежит ГК «Дело» Сергея Шишкарева), выяснил РБК. Информацию подтвердили представители компании и банка.

Клиент Сбербанка Александр Ездаков рассказал РБК, что мошенники украли у него с кредитной карты около 200 тыс. руб., получив доступ в приложение «Сбербанк Онлайн». Деньги были переведены на расчетный счет ПАО «Центр по перевозке грузов в контейнерах «Трансконтейнер», следует из выписки по операции, с которой ознакомился РБК.

ЦБ и Visa предупредили банки об утечке данных 55 тыс. карт
Финансы



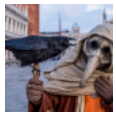
Представитель «Трансконтейнера» рассказал, что служба безопасности зафиксировала всего порядка 80 случаев поступления денежных средств от лиц, не пользовавшихся услугами компании, на общую сумму более 3 млн руб. По результатам проверки фактов мошенничества в отношении ПАО

«Трансконтейнер» выявлено не было, способов, при помощи которых мошенники могли бы воспользоваться ошибочно поступившими на счет компании денежными средствами, не существует, сказали в контейнерном операторе. «Таким образом, можно сделать вывод, что вероятное мошенничество совершено исключительно в отношении клиентов Сбербанка», — пояснил представитель «Трансконтейнера». Сбербанку известно об инцидентах, однако банк не подтверждает объем и число списаний — их значительно меньше, сказал представитель банка.

«Трансконтейнер» принял решение вернуть деньги пострадавшим. Компания направила заявление в Волго-Вятский банк Сбербанка, со счетов которого поступали платежи, о предоставлении реквизитов для возврата средств по сомнительным транзакциям, чтобы банк, в свою очередь, перевел их клиентам. «Ввиду того что транзакции совершены с признаками компрометации реквизитов счетов (карточек, личного кабинета и т.д.) клиентов Сбербанка, прямой обратный возврат имеет риски хищения мошенниками денежных средств», — подчеркнули в «Трансконтейнере». Представитель Сбербанка заверил, что денежные средства вернут клиентам.

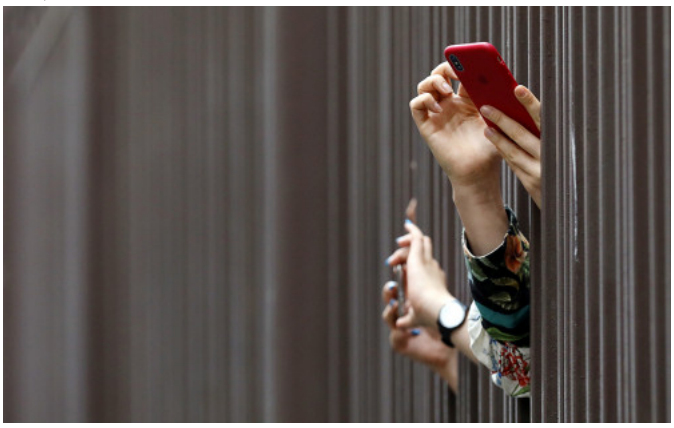
«Трансконтейнер» — оператор с крупнейшим в России парком грузовых контейнеров (более 74 тыс. штук) и платформ для их перевозки (27 тыс. штук). ГК «Дело» выиграла аукцион по покупке актива у РЖД в ноябре прошлого года, повысив цену к стартовой почти в два раза — до 60,3 млрд руб. за контрольный пакет. За «Трансконтейнер» также боролись структуры миллиардеров Владимира Лисина и Романа Абрамовича. В начале августа 2020 года Шишкарев консолидировал 100% оператора.

Схема мошенничества

Читайте на РБК Pro
 Назло Кавасаки: как лояльность победила в России компетентность  Почему руководителю необходима эмпатия и как ее развить
 Миллиардер-дауншифтер: как продавец ипотеки озолотился на сравнении цен  Пять личных навыков, которым стоит научиться в условиях неопределенности

По словам Ездакова, перед списанием денежных средств он получил сообщения о том, что «Сбербанк Онлайн» зарегистрирован на телефоне модели iPhone (у потерпевшего устройство другой модели) и код на регистрацию, в которых говорилось о необходимости связаться с банком, если эти действия выполняет не он. Оперативно соединиться с оператором по номеру 900 ему не удалось. После списания личные кабинеты в мобильном приложении и интернет-банке оказались заблокированы.

Число дел о мошенничестве рекордно выросло на фоне пандемии
Общество



В Сбербанке потерпевшему после его обращения подтвердили, что перевод осуществлялся с другого устройства, однако по итогам проверки всей информации пришли к выводу, что операция проведена корректно и основания для возврата средств отсутствуют, сообщается в письменном ответе банка на обращение клиента, с которым ознакомился РБК. Поскольку верификация в мобильном приложении проходила в полном соответствии с правилами обслуживания, у банка не возникает обязанности по возврату средств, соглашается глава юридической компании AVG Legal Алексей Гавришев.

Представитель Сбербанка рассказал РБК, что мошенники получили доступ к мобильному приложению, так как клиенты сами оставили необходимые данные на фишинговых сайтах, которые предлагают пройти фиктивные опросы для получения бонусов «Спасибо». «В процессе прохождения опроса клиента просят указать номер своей карты якобы для получения бонусов. С использованием номера карты мошенники инициируют регистрацию в «Сбербанк Онлайн» от имени клиента на своем устройстве. При этом для подтверждения регистрации «Сбербанк Онлайн» банк направляет СМС-пароль на номер телефона клиента в том числе с предупреждающим текстом «Код для регистрации iPhone — xxx. Никому не сообщайте код. Если вы не совершали регистрацию, позвоните по номеру 900». Данный пароль клиент самостоятельно вводит на фишинговом сайте, и он передается мошенникам, которые подтверждают им регистрацию на своем устройстве», — описали схему в банке.

По словам самого Ездакова, подобные сайты ему не попадались. Еще одним способом получения доступа в мобильное приложение может быть установка вредоносной программы или программы для удаленного управления, предполагает директор по стратегическим коммуникациям компании Infosecurity Softline Александр Дворянский.

Так как мошенникам в подавляющем большинстве случаев, даже попав в профиль клиента, не удается вывести средства на свои карты, они иногда делают переводы в разные крупные «белые» компании, например в компанию «Трансконтейнер» или благотворительные фонды, объясняет представитель Сбербанка: «Сразу после выявления таких кейсов банком были внедрены новые алгоритмы выявления и блокировки таких операций. Необходимо отметить, что вторую операцию, совершенную мошенниками, банк отклонил, после чего связался с клиентом для подтверждения перевода».

Мошенники стали чаще предлагать услуги по изменению кредитных историй

Финансы



«В дальнейшем деньги могли бы быть выведены из транспортной компании, например, через скомпрометированные аккаунты клиентов. Однако, не зная всех деталей произошедшего, судить об этом было бы преждевременно», — предполагает Дворянский. Такие случаи встречаются редко, чаще мошенники переводят средства на счета подставных физических лиц или на обезличенные электронные кошельки, добавляет Гавришев. Перевод на счет юридического лица мог быть выполнен для того, чтобы в дальнейшем осуществить возврат платежа, но уже не на счет потерпевшего, допускает управляющий партнер санкт-петербургского офиса коллегии адвокатов Pen & Paper Алексей Добрынин: «Мошенники производят платеж в адрес организаций, а затем обращаются к ним с требованием вернуть ошибочно переведенные денежные средства». Подобные схемы были недавно внедрены мошенниками и пока еще только обкатываются — как видно на практике, не совсем гладко, добавляет Добрынин. Возможно, это какая-то новая креативная схема, пока не известная на рынке, допускает и Гавришев.

Авторы
Евгения Чернышова, Мария Кокорева

мошенники Сбербанк переводы