Защита банковских транзакций: советы потерпевшему

Игорь Собецкий, *разработчик и автор курсов по экономической безопасности*
Учебный центр «Информзащита»

– Официант, что это у вас в счете? «Прокатило – 400 рублей», это как?
– Извините, не прокатило.

Практика ручного контроля транзакций

Анализируя безопасность банковских транзакций, в том числе при электронной торговле, можно четко выделить три подхода: со стороны клиента, со стороны банка и со стороны продавца (или поставщика услуг). Встанем вначале на позицию **клиента**.

Первая и наиболее частая угроза – несанкционированное снятие денег со счета клиента третьими лицами. Данная угроза может быть реализована через внутреннее мошенничество в компании-клиенте или в банке, но значительно чаще деньги снимаются с помощью перехвата информации о кредитной карте клиента (например, с помощью скиммера в банкомате) или управления клиентским терминалом платежной системы.

Обеспечить полную защиту клиента от неправомерного доступа к своему счету практически невозможно. Но при использовании нескольких простых приемов можно минимизировать вероятность неблагоприятных последствий. При использовании клиентом-физическим лицом кредитной карты[1] желательно пользоваться только надежными банкоматами, например, в отделении банка. При использовании кредитной карты в торговых точках или предприятиях общественного питания контролировать все действия персонала с кредитной картой, не разрешая уносить карту из поля зрения. Даже если, со слов персонала, требуется «позвонить в банк», «терминал находится на кассе» и т. п., владелец карты ни на минуту не должен выпускать ее из вида. Кредитную карту не требуется предъявлять по требованию каких-либо должностных лиц, в том числе сотрудников полиции.

Если в целях безопасности карта привязана к номеру мобильного телефона, клиент при обращении с телефоном должен соблюдать те же меры безопасности, что и при пользовании картой. Телефон не следует оставлять в общественных местах без присмотра или даже на короткое время передавать посторонним ли-

[1] *Эти соображения полностью справедливы и для корпоративных кредитных и дебетовых карт.*

цам. В случае утраты телефона необходимо немедленно обратиться с заявлением в полицию и одновременно связаться с банком и заблокировать свою карту. Для этого можно воспользоваться телефонами, установленными в общественных местах, в том числе в полицейском участке. В случае возникновения конфликтной ситуации талон-уведомление из полиции послужит хорошим доказательством точного момента утраты телефона.

Зафиксированы случаи перехвата мошенниками доступа к счету без получения физического доступа к мобильному телефону его законного владельца, – с использованием возможностей оператора связи. Поэтому неожиданное исчезновение связи при включенном телефоне, в том числе и в ночное время, – повод для немедленного звонка с любого телефона оператору связи. Если окажется, что SIM-карта клиента была перевыпущена, необходимо срочно позвонить в банк и заблокировать свою карту. Кроме того, следует при первой возможности (если оператор связи не может обойтись без личной явки клиента в офис) заблокировать SIM-карту, полученную мошенниками, и вернуть себе доступ к счету. Наилучшим решением в такой ситуации было бы введение кодового слова, без которого оператор связи не производил бы любые операции по доверенности[2], или обязательная проверка оператором связи подлинности доверенности через удостоверившего ее нотариуса.

Для защиты корпоративного счета от несанкционированного снятия средств проще всего для начала честно исполнить договор с обслуживающим банком. При оформлении договора на удаленное банковское обслуживание в раздел «Обязанности клиента» банк включает много полезных мер, позволяющих существенно снизить вероятность мошенничества. В частности, система «Клиент-банк» должна быть развернута на отдельном компьютере, не используемом для других бизнес-задач, на котором установлен надежный межсетевой экран и антивирусная программа. Необходимо также установить на него средства защиты от несанкционированного доступа, как минимум, электронный замок с двухфакторной аутентификацией. Корпус компьютера должен быть опечатан, причем целостность печати следует проверять, как минимум, ежедневно. Компьютер должен иметь собственный физический или, в крайнем случае, логический канал выхода в сеть Интернет. Техническое обслуживание и поддержка пользователей должны осуществляться специально выделенным специалистом ИТ-подразделения без использования каких бы то ни было средств удаленного администрирования. Работу с системой «Клиент-банк» необходимо передать в руки специально выделенного работника бухгалтерии. Для удостоверения транзакций электронной подписью клиента следует использовать только криптосредства на базе внешних аппаратных носителей ключей, например e-token или RU-token. Внешние носители ключей не должны храниться на рабочем месте бухгалтера, а выдаваться только на время работы с системой.

Банк может включать в договор и другие полезные правила, соблюдение которых благотворно сказывается на безопасности клиентского счета. Помимо перечисленных мер, чрезвычайно полезны для компании-клиента неформальные связи со службой безопасности банка. Благодаря таким связям может быть организовано «ручное» подтверждение наиболее крупных или нетипичных для данного клиента транзакций и немедленная блокировка счета при выявлении мошенничества.

Второй по значению угрозой для клиента является возможная утечка данных о его банковской карте третьим лицам. Очевидно, что после передачи данных своей кредитной карты продавцу клиент не может быть уверен в безопасном хранении этих данных на стороне продавца. Поэтому надежнее делать покупки в электронных магазинах, прибегающих к услугам платежных систем типа Assist или Cyberplat. Таких систем сравнительно немного, и взлом каждой из них очень быстро становится достоянием гласности, предоставляя клиенту возможность сберечь свои деньги. В то же время взлом информационной системы небольшой компании-продавца может пройти незамеченным (в том числе и для самой компании), после чего таинственное исчезновение денег со счета станет полной неожиданностью для клиента. Поэтому пользование магазинами, поддерживающими собственный биллинг, считается небезопасным.

По той же причине не рекомендуется использовать для дистанционных покупок банковскую карту, привязанную к основному счету. Гораздо спокойнее открыть дополнительную карту (возможно, виртуальную), на счет которой перед покупкой перебрасывается соответствующая сумма.

Третьей существенной угрозой являются произвольные действия банка по отношению к клиенту. В условиях российской банковской системы, когда клиент руководствуется в своих действиях, главным образом, телевизионной рекламой банка, а репутация не стоит ничего, многие банки позволяют себе откровенное самоуправство, такое как неправомерное снятие денег со счета клиента, неправомерную блокировку карты клиента, несвоевременную обработку платежей и другие нарушения.

Так, достоянием гласности стал инцидент с одним из крупных российских банков. Работники банка предположили, что бывший заемщик этого банка несколько лет назад не полностью выплатил кредит, задолжав около двух рублей. С учетом прописанных в договоре с заемщиком пеней и штрафов банк стал требовать от него около 65 тысяч рублей. Разумеется, клиент отказался оплачивать своими деньгами некомпетентность банковского персонала. Банк обратился в суд, где потерпел полное поражение: иск банка был отклонен по причине истечения срока исковой давности. Но клиент ра-

[2] *Один из российских операторов мобильной связи именно так и поступил.*

но обрадовался, поскольку после вступления судебного решения в законную силу банк продал несуществующий долг коллекторскому агентству. Точку в этой печальной истории поставила уже полиция.

Другой не менее крупный банк нашел еще более хороший способ поправить свои дела. Когда некая компания оформила в этом банке зарплатную карту своему работнику, тот лишился сразу всей зарплаты: работники банка списали ее в погашение наскоро придуманного «долга» пятилетней давности. Увы, креативное решение не было поддержано судом – по иску, по сути, ограбленного средь бела дня работника, деньги все же пришлось вернуть.

В ряде случаев российские банки произвольно блокируют карты и привязанные к ним счета клиентов, сочтя ту или иную транзакцию мошеннической. Особенно приятно клиентам-физическим лицам, когда банк блокирует единственную карту клиента, оказавшегося за границей, а для разблокировки карты последнему предлагают лично явиться в банковский офис.

Нередки случаи грубых нарушений банков по срокам обработки платежей, в том числе внутрибанковских. В результате на клиентов возлагается ответственность за просрочку платежа. Российские банки, в отличие от большинства иностранных, не защищают интересы клиента в случае несанкционированного списания денег. При рассмотрении жалоб клиентов на подозрительные транзакции в выписке банки не проводят полного и детального расследования, ограничиваясь формальными отписками. Обычной практикой считается списание денег со счета клиента по опротестованной транзакции, не дожидаясь окончания расследования. Банки не пытаются защищать своих клиентов от мошенников, блокируя опротестованные транзакции. Кроме того, большинство российских банков также возлагает на клиентов ответственность за ошибки при обработке платежей. Несмотря на то, что ошибка допущена банком, все материальные последствия (пени и штрафы за просрочку платежа, срыв сделок, упущенная выгода и т. п.) «почему-то» ложатся на клиента.

Некоторые российские банки без санкции клиента произвольно устанавливают разнообразные лимиты – на количество транзакций в сутки, на объем переводимых средств, на сумму снимаемой наличности и пр. Неудобства, испытываемые клиентами, столкнувшимися с подобными лимитами, никого при этом не интересуют.

Для клиентов-юридических лиц можно посоветовать внимательно изучить договор с банком и подправить не удовлетворяющие компанию положения. Практика показывает, что крупные компании легко могут парировать негибкость банка («Это стандартный договор, изменения не допускаются») простым обещанием сменить банк на более клиентоориентированный. Физическим же лицам можно только посоветовать внимательно изучить перед оформлением карты отзывы о том или ином банке и обращаться в итоге в наиболее толерантные учреждения.

Четвертой угрозой для клиента является недобросовестность со стороны продавца. Сюда входит как прямое мошенничество, так и элементарные различия в законодательстве различных стран. Например, целый ряд лекарств «для похудания», свободно продающихся в Китае и Таиланде и, соответственно, свободно отправляемых российским покупателям, в нашей стране официально считается наркотиками. В результате клиента, решившего поправить фигуру, при получении заказанного лекарства может ожидать крайне неприятная встреча с оперативниками ФСКН. Аналогичные проблемы клиент может получить, приобретя в иностранном магазине прибор, считающийся у себя на родине электронной игрушкой, а в нашей стране – специальным радиоэлектронным средством для негласного получения информации. Универсального рецепта здесь не существует, наилучший способ избежать неприятностей – делать все покупки либо в проверенных магазинах, либо на электронных торговых площадках, гарантирующих безопасность сделки.

К счастью для обобранных клиентов-физических лиц, в российской судебной практике давно уже действует понятие «слабой стороны». В случае несанкционированного снятия денег со счета кем бы то ни было у клиента есть хорошие шансы вернуть утраченные активы. Клиентам-физическим лицам при поступлении информации о несанкционированных транзакциях (например, по SMS) следует предпринять ряд неотложных мер.

Зафиксировать наличие банковской карты у себя. Для этого, если поблизости есть банкомат стороннего банка, немедленно вставить карту в банкомат и произвести какие-либо действия, например, проверить баланс, и сохранить чек банкомата. Банкомат «своего» банка в этом смысле использовать не рекомендуется, поскольку лог-файлы с него могут таинственно пропасть. Если никакого банкомата поблизости нет, то заручиться показаниями любых находящихся рядом лиц: коллег по работе, попутчиков, соседей и т. п. Этим людям надо показать свою банковскую карту, после чего составить акт в произвольной форме с указанием паспортных данных свидетелей, что карта в самом деле находилась у клиента. Если владелец карты находится в общественном месте типа гостиницы, мотеля и т. п., то составить такой акт может администрация этого учреждения.

Немедленно сообщить о несанкционированной транзакции в банк. При наличии технической возможности разговор следует записать. Если такой возможности нет, то удостоверить содержание разговора показаниями свидетелей.

Сообщить о несанкционированной транзакции в полицию. В данном случае совершенно неважно местонахождение владельца карты. Если он находится на территории РФ, то заявление делается в ближайший полицейский участок. Самое главное здесь – получить талон-уведомление о сделанном заявлении, где будет указана дата и время обращения. Если владелец карты находится за границей, следует попросить подать такое заявление знакомого или члена семьи.

Затем уже в спокойной обстановке клиент пишет заявление в банк об отказе от несанкционированных им транзакций, обязательно указав ключевой момент – карта все время находилась при клиенте, он никогда не передавал ни карту, ни PIN-код к ней третьим лицам, а во время снятия денег находился в совершенно другом месте. Теперь клиент полностью готов к возвращению своих денег. Главное – клиент должен четко представлять, что он не является потерпевшей стороной даже в случае возбуждения уголовного дела. Потерпевшим будет банк, который лишился денег и теперь должен возместить убытки из своих средств.

Возможны два варианта: банковская карта может быть кредитной или дебетовой. Если карта была кредитной, то, собственно, никакого ущерба клиент и так не понес: несанкционированная транзакция – проблема исключительно банка. В такой ситуации клиент просто не должен оплачивать возникшую вследствие деятельности мошенников «задолженность» по кредиту. Причем следует игнорировать любые требования банка по схеме «Оплатите долг сейчас, иначе у вас будут большие проблемы, а разбираться банк будет потом». Так поступать нельзя ни в коем случае, поскольку в соответствии с Гражданским кодексом РФ оплата клиентом банка долга или его части означает признание им этого долга. Поэтому ответ банку должен быть простым: вначале расследование инцидента банком, затем, в случае несогласия клиента с результатами расследования, судебное разбирательство, и только после проигрыша в суде – какие-то выплаты. Впрочем, последнее маловероятно, так как большинство судов в такой ситуации российскими банками традиционно проигрывается.

Если клиент владеет дебетовой картой, то возврат средств несколько усложняется. Предстоит обратиться в банк с досудебной претензией, предложив вернуть похищенные с карты средства. И только после отрицательного ответа на эту претензию или 10-дневного молчания клиент самостоятельно должен обращаться в суд. При наличии указанной выше доказательной базы результат будет тем же, что и в предыдущем случае.

К сожалению, принцип «слабой стороны» не действует для клиентов-юридических лиц. Поэтому в случае несанкционированного списания денег со счета юридического лица подготовка к процессу должна быть более тщательной. В такой ситуации желательно заключить договор с адвокатом, имеющим опыт подобных процессов. При этом как нельзя более справедлив старый принцип «время – деньги».

Со стороны **продавца** *основной проблемой* электронной коммерции[3] будет приобретение товаров по чужим кредитным картам, что влечет за собой аннулирование транзакции и принудительное списание средств банком. Для защиты от такой напасти желательно применять несколько простых мер:

- обращать внимание на соответствие государства банка-эмитента карты и государства проживания клиента (например, оплата покупки российским клиентом с помощью карты австрийского банка должна вызывать здоровую подозрительность);
- принимать оплату картами только от клиентов, не стесняющихся указывать свой домашний адрес для получения заказанных ими товаров, владельцам абонентских ящиков придется оплачивать свои заказы как-то иначе;
- при заказе особо дорогостоящих или эксклюзивных товаров не постесняться попросить у клиента скан его паспорта или иные доказательства подлинности личности.

Второй серьезной проблемой для электронных магазинов могут стать хакерские атаки с целью завладения базой данных клиентов. Эта угроза особенно актуальна, если электронный магазин не доверяет платежным системам и решает самостоятельно организовать обработку платежей. В таком случае в информационной системе магазина хранится лакомая добыча хакеров – база данных клиентов с данными их банковских карт, включая код CVV. Такой магазин будут атаковать снова и снова, пока не добьются своего. Помимо возможного выхода из строя информационной системы магазина многократные атаки чреваты серьезными расходами. Деньги, списанные мошенниками со счетов граждан, чьи персональные данные были украдены из базы данных, в дальнейшем по решению суда могут быть взысканы с этого магазина. Наилучший способ защиты от данной угрозы – заключить договор с платежной системой типа Assist или Cyberplat. В таком случае магазин тут же теряет популярность в хакерской среде, ведь он не хранит информацию о чьих-либо банковских картах.

Третьей угрозой является внутреннее мошенничество работников электронного магазина, фальсифицирующих в базе сведения о якобы произведенной оплате. Решение этой проблемы в большей степени относится к экономической и кадровой безопасности. Тем не менее следует обеспечить, как минимум, эффективный контроль за действиями работников магазина в информационной системе. Это может быть достигнуто посредством DLP-системы или обыкновенного кейлоггера. Важно, правда, не только хранить протоколы работы своих сотрудников, но и хотя бы изредка их читать.

Наконец, третьей стороной в электронных банковских операциях является сам **банк**. Именно банк (как бы ни пытались некоторые безответственные банковские служащие доказывать обратно) несет все риски, связанные с использованием подложных карт и несанкционированным списанием средств со счета клиента.

К сожалению, найти мошенников и, тем более, взыскать с них украденные деньги удается далеко не всегда. Поэтому лучший способ защиты интересов банка – минимизировать неправомерные списания средств. Для достижения этой цели

[3] *На самом деле это далеко не самая большая проблема для российских электронных магазинов, но те, что более актуальны, лежат в сфере экономической, а не информационной безопасности.*

банк может использовать несколько несложных мер.

Пунктуально выполнять требования стандартов Банка России в части, касающейся безопасности. Это позволит существенно снизить риск мошенничества.

Как можно быстрее перевести всех своих клиентов-физических лиц на карты с чипом и технологию 3D-Secure. Конечно, и эта технология не идеальна, но ее использование позволяет снизить вероятность мошенничества и переложить часть рисков банка на оператора связи.

По возможности внести в договоры с клиентами-физическими лицами положение о необходимости личной явки клиента в офис банка для санкционирования обслуживания карты за границей с обязательным указанием доступных для оказания этой услуги стран.

Внести в договоры об автоматизированном банковском обслуживании юридических лиц положения о неукоснительном соблюдении клиентом перечисленных в договоре правил информационной безопасности, а также о праве банка контролировать соблюдение клиентом этих правил и приостанавливать автоматизированное банковское обслуживание при выявлении халатного отношения клиента к вопросам безопасности.

Постоянно контролировать банкоматы банка на предмет установки скиммеров и других устройств для несанкционированного получения данных о банковской карте. При выявлении подобных устройств проводить детальное расследование и перевыпускать все скомпрометированные карты.

Немедленно реагировать на жалобы клиентов о несанкционированном списании средств, проводя детальное расследование. В ходе такого расследования постараться собрать все первичные материалы, включая слипы с POS-терминалов, видеозаписи с банкоматов, детализации соединений по номеру телефона клиента. При выявлении признаков мошенничества со стороны клиента немедленно уведомлять об этом правоохранительные органы. При отсутствии таких признаков возмещать убытки клиента в досудебном порядке.

Заключить договор с одной или несколькими страховыми компаниями, переложив на них риск несанкционированного списания средств со счета клиента.

И самое главное. Всем участникам электронного банкинга стоит помнить народную мудрость: «Не знаешь, как делать, – делай по закону». В долгосрочной перспективе работа по закону оказывается гораздо выгоднее бизнеса по понятиям с периодическими визитами судебных приставов.