Кобренд с банком: выбираем оптимальный носитель для лояльности

Как показывает анализ, оптимальным носителем лояльности в случае кобренда с банком являются white label апплеты от независимых поставщиков программных решений

Александр Спесивцев,
генеральный директор компании СКАНТЕК

Программы лояльности, внедряемые различными ритейловыми структурами, являются достаточно эффективным средством для увеличения объемов продаж. Как известно, суть программ лояльности состоит в том, что ритейлер поощряет клиента, когда тот покупает у него товары или услуги. Схемы поощрения могут быть разными. В настоящей статье рассматривается популярная модель программы лояльности, называемая «балловой» (или «бонусной») схемой.

Специфика балловой схемы

В общих словах суть «балловой» схемы заключается в следующем. Ритейлер присваивает клиенту некоторый идентификатор лояльности и ассоциирует с ним лояльный счет. Каждый раз, когда клиент покупает товары у ритейлера, он может предъявить идентификатор лояльности, и на его лояльный счет добавляются «баллы». Накопив некоторое количество баллов, клиент может обменять баллы на товары и/или услуги ритейлера. После такого обмена потраченные баллы со счета клиента списываются.

В этой статье мы сравним различные варианты реализации лояльного приложения на картах и в терминалах, когда оно интегрируется с имеющимся на карте платежным приложением банка. Наша цель – проанализировать, как выбор носителя лояльного приложения определяет на кобрендовой карте такие ключевые его параметры, как безопасность, удобство использования и возможность самостоятельного развития решения заказчиком.

Кобренд с банком и особенности его реализации

Если ритейлер достаточно крупный, он может договориться с банком, эмитирующим платежные карты, о выпуске кобрендовых карт, т. е. таких карт, на которых:

- располагаются бренды (логотипы) и банка, и ритейлера.
- хранятся данные клиента, необходимые для проведения как платежной, так и лояльной транзакций.

Кобрендовые карты активно используются участниками рынка, так как имеют очевидную синергию: обороты как банка, так и ритейлера увеличиваются. При этом у ритейлера обороты растут, так как владельцы кобрендовых карт более охотно покупают товары именно у него, а не у конкурента, предлагающего аналогичные услуги/товары, поскольку при покупке именно у этого ритейлера им начисляются баллы. В свою очередь, обороты банка также растут, так как владельцы кобрендовых карт более охотно оплачивают покупки картами именно этого банка, покупая товары у его партнера-ритейлера и получая при этом бонусные баллы. Справедливости ради следует сказать, что клиент может

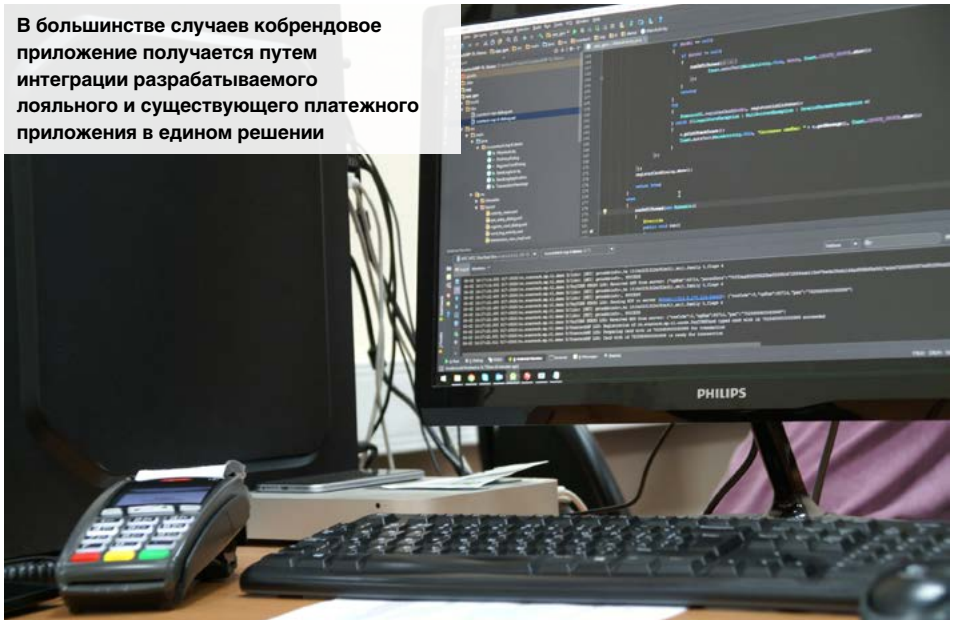
оплатить покупку у ритейлера – участника программы – и наличными деньгами. В этом случае при предъявлении ритейлеру кобрендовой карты клиенту также зачисляются баллы на его лояльный счет (но это уже не кобренд, а «просто» программа лояльности, поскольку банк при такой схеме не получает дополнительного дохода в виде торговой уступки).

Вначале дадим ряд определений, которые будем использовать в дальнейшем.

Платежное приложение (ПП) – совокупность данных и программ, хранящихся на карте и в терминале, которые обеспечивают возможность проведения платежных транзакций при покупках.

В связи с этим будем считать, что банк использует ПП, принадлежащее одной из платежных систем (ПС). Платежные приложения, используемые современным банком, удовлетворяют EMV-стандартам как в карточных, так и в терминальных приложениях. В связи с этим участие банка вносит специфику в реализацию лояльного приложения в кобренд-схеме по сравнению с тем, если бы участником такой программы была бы небанковская структура. Эта особенность состоит в том, EMV-стандарты строго определяют спецификации карт и терминалов и алгоритмы проведения транзакций.

В большинстве случаев кобрендовое приложение получается путем интеграции разрабатываемого лояльного и существующего платежного приложения в едином решении



Кобрендовые карты имеют очевидную синергию: обороты как банка, так и ритейлера увеличиваются

Наиболее популярными ПС в России являются Национальная система платежных карт (НСПК) «Мир» и международные платежные системы (МПС) Visa и Mastercard. Все три системы имеют следующие типы платежных приложений: во-первых, платежное приложение, построенное на данных магнитной полосы, которое используется для совместимости с устаревшим терминальным оборудованием, что гарантирует максимально широкий прием карты, во-вторых, EMV-приложение с контактным и/или бесконтактным интерфейсами. Заметим, что в настоящее время все контактные интерфейсы МПС являются EMV-совместимыми, в отличие от бесконтактных интерфейсов, построенных на базе проприетарных спецификаций каждой МПС.

Лояльное приложение (ЛП) – совокупность данных и программ, хранящихся на карте и в терминале, которые обеспечивают возможность проведения лояльных транзакций. К лояльным относятся транзакции по начислению и списанию баллов на лояльный счет клиента. Основу данных лояльного приложения составляет идентификатор лояльности.

Кобрендовое приложение (КП) – совокупность данных и программ, хранящихся на карте и в терминале, которые реализуют платежное и лояльное приложения. В дальнейшем подразумевается, что как терминал, так и карта поддерживают оба приложения – платежное и лояльное.

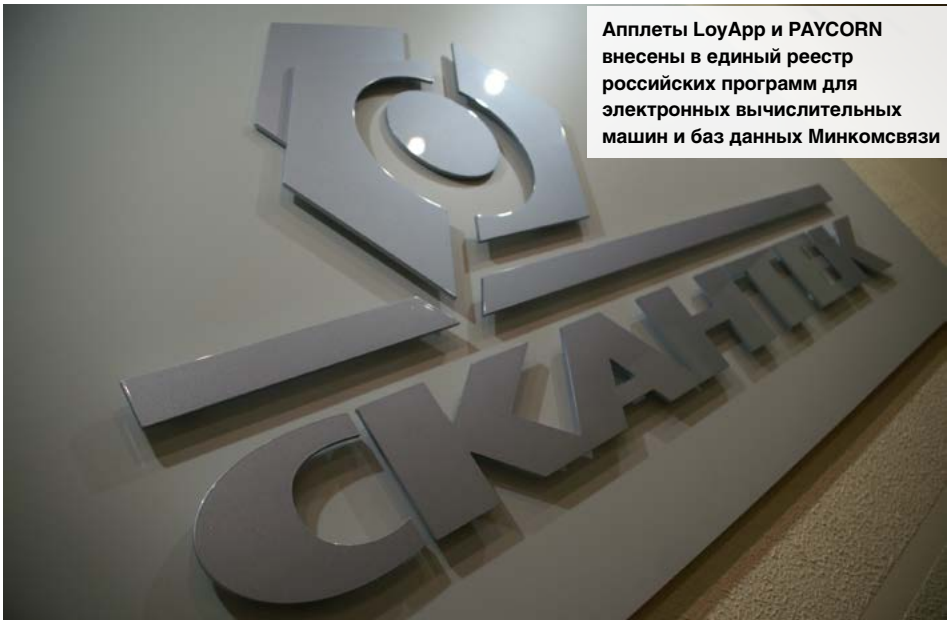
В большинстве случаев кобрендовое приложение получается путем интеграции разрабатываемого лояльного и существующего платежного приложения в едином решении. Интеграция затрагивает персонализационное, карточное и терминальное решения. Интеграция персорешения состоит в том, чтобы обеспечить запись как банковских, так и лояльных данных и программ на карту. Интеграция карточного решения состоит в том, чтобы обеспечить функционирование банковского и лояльного приложений при взаимодействии карта-терминал. Интеграция терминального решения заключается в поддержке процедур обслуживания банковских и лояльных транзакций как при работе с картой, так и с кассой и платежным и лояльным процессингами.

Носитель лояльности

Для реализации лояльного приложения на кобрендовой карте необходимо выбрать некоторый «носитель», на котором хранятся данные лояльности клиента. Наиболее популярными являются четыре следующих носителя лояльности:

1. Графическое изображение. Идентификатор лояльности может быть размещен на карте при графической персонализации в виде штрихкода, QR-кода или просто в виде номера, напечатанного/эмбоссированного на поверхности карты.

2. Магнитная полоса. Идентификатор лояльности можно записать на третьем



Апплеты LoyApp и PAYCORN внесены в единый реестр российских программ для электронных вычислительных машин и баз данных Минкомсвязи

треке магнитной полосы, и он не будет мешать работе банковского приложения, использующего первый и второй треки.

3. Теги платежного приложения. Данные лояльности можно хранить в области дополнительной информации платежных приложений «Мир», Visa и Mastercard, не имеющих прямого отношения к проведению платежной транзакции. В соответствии с EMV-стандартами такие данные выделяются специфическими идентификаторами, тегами. Поэтому в дальнейшем под тегом в этой статье будем понимать информационное поле в платежном приложении, в котором могут храниться данные лояльных приложений.

4. Апплет. Данные лояльности можно хранить в карточном приложении – апплете. Рассматриваются два типа таких апплетов:

- EMV-апплеты
- Не-EMV апплеты, т. е. специализированные апплеты.

EMV и не-EMV-апплеты в кобрендовых проектах

Под EMV-апплетом будем понимать апплет, совместимый со спецификациями EMV в контактной части и поддерживающий некоторые проприетарные спецификации по доступу к EMV-апплету в бесконтактной части интерфейса. Использование проприетарных спецификаций объясняется тем, что до настоящего времени просто не опубликованы бесконтактные EMV-спецификации, и каждая ПС вынуждена решать вопрос разработки бесконтактного интерфейса к EMV-апплету по-своему, т. е. в соответствии со своими «фирменными» спецификациями.

Реализация карточных приложений в виде EMV-апплетов вызывает большой интерес в различных проектах, где требуется обеспечить прием карточного приложения на банковском платежном терминальном оборудовании. Действительно, поскольку любой платежный банковский терминал в настоящее время является EMV-терминалом, он должен уметь обслуживать все EMV-апплеты, хранящиеся на карте. Именно это обстоятельство делает EMV-апплет привлекательным для банковского кобренда. Заметим, в настоящее время все МПС предлагают проприетарные интерфейсы для бесконтактного доступа к своим платежным приложениям на карте.

Под не-EMV-апплетом будем понимать специализированным апплет, который разработан специально для решения той или иной задачи. Спецификации специализированного апплета могут быть не полностью совместимы с EMV-спецификациями. В дальнейшем будем рассматривать специализированные апплеты, в которых реализована офлайн- и/или онлайн-аутентификация.

Специализированные апплеты имеют ряд достоинств по сравнению с EMV-апплетами, одно из них – существенно меньшее время выполнения по сравнению с EMV-апплетом. Это обстоятельство особо важно в бесконтактном режиме, когда время выполнения чтения данных карточных приложений и их аутентификации ограничено требованиями ПС. Примером апплета, специально разработанного для лояльных приложений, является апплет LoyApp [6].

Будем говорить, что апплет является white label апплетом, если его компания-разработчик предусматривает такую реализацию прав на апплет компании-покупателю, что последняя может использовать его под своим брендом. Принадлежность апплета к классу white label, безусловно, позитивно сказывается на экономике как проектирования, так и эксплуатации любых систем, в том числе и систем лояльности. Позитивность состоит в снижении финансовых и временных затрат ритейлера для достижения договоренности с владельцем апплета как при разработке, так и по роялти, отчисляемых ритейлером ПС за пользование апплетом в процессе эксплуатации систем лояльности.

В настоящее время владельцами EMV-апплетов большей частью являются сами ПС. Однако есть и редкие (пока) исключения. Кроме ПС, права на EMV-апплеты принадлежат еще некоторым производителям карт, а также некоторым разработчикам ПО для карт и/или терминалов. Примером white label апплета, права на который принадлежат компании разработчику ПО, является апплет PAYCORN [6].

Договориться с ПС об использовании их EMV-апплета сложно в силу того, что, как известно, «Chase Manhattan» не торгует семечками». Особого интереса продавать EMV-апплет нет и у производителя карт, поскольку его интерес состоит в продаже именно карт, т. е. готового продута.

Наличие white label EMV-апплета у производителя просто наделяет его карты конкурентным преимуществом перед теми конкурентами, которые не имеют таких апплетов. Действительно, если производитель карт продал свой white label апплет покупателю в лице той или иной структуры, то последний может использовать его на картах другого производителя карт, обеспечив таким образом первому производителю упущенную выгоду, так как цена апплета в структуре цены карты – это как раз те самые «семечки». Кому действительно интересно продавать EMV-апплеты, так это производителям ПО для карт и терминалов, ибо продажа «семечек» – их основной бизнес.

Параметры сравнения лояльных приложений на кобрендовой карте

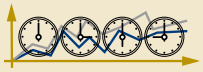
Для сравнения лояльных приложений на кобрендовой карте введем ряд параметров. Далее будут оцениваться разные лояльные приложения при условии, что они находятся в сочетании с определенным платежным приложением, размещенным на кобрендовой карте. Это важно помнить, т. к. значения параметра зависят от того, насколько лояльное приложение «сочетается» с платежным и может воспользоваться «достоинствами» последнего.

Рассмотрим следующие параметры сравнения лояльных приложений на кобрендовой карте:

Безопасность. Параметр определяет, насколько лояльное приложение защищено от подделок. Все известные реализации хранения данных лояльности на магнитной полосе или в тегах не являются стойкими в том смысле, что данные лояльности легко копируются на другую карту и/или подделываются. Даже если попытаться аутентифицировать тэг средствами платежного приложения, то такой способ защиты также нельзя считать стойким, так как DDA-аутентификация может быть взломана с помощью метода relay attack [1] и spy устройств [2–5]. Для приобретающих все большую популярность безоператорных терминалов на АЗС, где никто не следит за тем, что за устройство (карта или spy-устройство) вставляется в терминал, это особенно опасно. В специализированном апплете реализованы процедуры офлайн/онлайн-аутентификации, позволяющие терминалу (процессингу) опознать действительную карту, поэтому оба апплета позволяют исключить подделку карты и, соответственно, данных лояльности. В связи с этим карты со специализированным апплетом стойки к подделке, так же как и карты с EMV-апплетом. Сразу оговоримся, что если носитель лояльности устойчив к подделке, то безопасность лояльных приложений, построенных на базе этого носителя, также можно обеспечить на высоком уровне. Поэтому в этом разделе мы рассмотрим только не стойкие к подделке носители лояльности (графическое изображение, магнитную полосу и теги). Говоря о безопасности лояльного приложения, следует проанализировать два риска: во-первых, несанкционированное начисление баллов (начисление баллов, заработанных одним пользователем, другому пользователю), во-вторых, несанкционированное списание баллов, честно заработанных пользователем, злоумышленником, подделавшим носитель лояльности. Оба несанкционированных действия связаны для ритейлера с репутационными рисками, которые могут скомпрометировать программу лояльности, существенно снизив ее эффективность. Несмотря на то что некоторые носители лояльности могут быть легко подделаны, риск несанкционированного начисления баллов угрозы может быть существенно снижен, если клиент при оплате использует банковское приложение кобрендовой карты. Процесс в данном случае можно организовать таким образом, чтобы сначала (при платеже) происходила аутентификация карты посредством аутентификации платежного

Графическая персонализация и магнитная полоса занимают последние места в рейтинге носителей лояльности

КАЛЕЙДОСКОП



ХХХХовал единичные успешные атаки WannaCry на российские банки

1000

Решить задачу обслуживания EMV-транзакции с одновременным чтением дополнительных данных из апплета лояльности технологически просто

приложения, и только затем – зачисление баллов на лояльный счет клиента.

Если же клиент платит наличными, то терминал не в состоянии аутентифицировать карту. Злоумышленник, например, кассир ТСП, может этим воспользоваться для зачисления баллов на некоторый «левый» счет. Впоследствии злоумышленник может списать с него баллы.

Риск несанкционированного списания баллов представляет реальную опасность для лояльных приложений, построенных на не стойких к подделке носителях. Действительно, при списании баллов может не происходить покупки, поэтому карта не будет аутентифицирована платежным терминалом/процессингом. Следовательно, если у носителя лояльности отсутствует взломостойкость, то данные лояльности легко поменять на поддельные. Это приводит к тому, что злоумышленник получает возможность распоряжаться баллами клиента. Особенно легко осуществить несанкционированное списание баллов в уже описанной ситуации, когда злоумышленник является оператором платежного терминала (кассиром).

Удобство пользования для клиента. Эта группа параметров определяет, насколько удобно для клиента обслуживание с помощью лояльного приложения. Различные неудобства, с которыми сталкивается клиент при использовании лояльного приложения на кобрендовой карте, могут сделать малоэффективным весь кобренд. Для формального определения удобства пользования лояльным приложением рассмотрим следующие критерии:

- Одно окно (интерфейса платежного и лояльного приложений). Проектируя приложение лояльности на кобрендовой карте, ритейлер должен стремиться к тому, чтобы лояльное приложение работало по такому же интерфейсу карта–терминал, что и платежное приложение. Это позволит исключить «танцы с бубном» у терминала, когда клиент, например, сначала вставляет карту в чиповый ридер для проведения платежной транзакции, по завершении транзакции вынимает карту и вставляет ее уже в ридер магнитной полосы для проведения лояльной транзакции.
- Одно предъявление. Помимо принципа одного окна, клиенту удобно предъявлять карту терминалу один раз, а не два: сначала для выполнения платежного, а потом лояльного приложений (даже если оба раза предъявлять карту нужно по одному интерфейсу – контактному либо бесконтактному). Ограничения по времени взаимодействия терминал–карта, а также техническая сложность реализации терминального ПО, которое обслуживает два карточных EMV-приложения (платежное и лояльное) за одно предъявление карты терминалу, являются причиной отсутствия таких решений на рынке.

> Если у носителя лояльности отсутствует взломостойкость, данные лояльности легко поменять на поддельные

В то же время решить задачу обслуживания EMV-транзакции с одновременным чтением дополнительных данных из апплета лояльности технологически просто. Примером терминального ПО, осуществляющего обработку кобрендовой карты за одно предъявление ее терминалу, является внесенное в единый реестр российских программ для электронных вычислительных машин и баз данных Минкомсвязи России ПО SmartEngine v63x [6], при этом на карте платежное приложение является одним из приложений МПС/НСПК, а лояльное приложение реализовано с помощью апплетов LoyApp™ или PAYCORN™ [6].

Табл. Сравнительный анализ лояльных приложений на банковской кобренд карте

Параметр		A	B	C	D	E	F	G
Безопасность		низкая	низкая	низкая	средняя	высокая	высокая	высокая
Удобство	Одно окно	нет	нет	да	да	да	да	да
	Одно предъявление	нет	нет	да	да	не известно	не известно	да
Независимость	От Платежной системы	да	да	нет	да	да	нет	да
	От Производителя карт	да	да	да	да	нет	да	да

A – графическая персонализация

B – магнитная полоса

C – тэги платежного приложения

D – специализированный апплет, например, LoyApp

E – апплет производителя карт

F – апплет ПС

G – white label EMV совместимый апплет от независимого проставщика ПО, например, PayCorn

Независимость. Оставляя в стороне саму возможность оставаться независимым в области платежных технологий, приведем два высказывания:

«Кто не нуждается в чужом, но живет независимо, тот всех богаче» (Иоанн Златоуст) и «Тот, кто имеет союзников, уже не вполне независим» (Гарри Трумэн).

Учитывая вышесказанное, будем считать лояльное приложение независимым, если владелец системы лояльности может использовать имеющееся у него лояльное приложение (в любой платежной системе и на любых картах) без согласования с платежной системой и производителем карт.

Примером зависимого приложения является лояльное приложение, в котором носителем лояльности являются теги платежного приложения. Зависимость от ПС заключается в том, что для использования тегов необходимо получить согласование ПС. Заметим, что если карточное приложение зависимо, то с его помощью сложно будет построить *еще одно* кобрендовое приложение, в котором платежное приложение принадлежит другой ПС. Очевидно, что ритейлеру выгодно иметь независимые приложения. Действительно, если ритейлер захочет запустить кобренд с другим банком, являющимся эмитентом карт другой ПС, то, имея независимое лояльное приложение, он сможет сделать это значительно быстрее.

Результаты анализа носителей лояльности

В таблице приведены значения параметров для рассмотренных носителей лояльности при условии, что на дуальную карту загружено банковское приложение, поддерживающее контактно-бесконтактную функциональность.

Анализ таблицы позволяет сделать вывод о том, что такие носители лояльности, как графическая персонализация и магнитная полоса, занимают последние места в рейтинге. Эта два носителя можно использовать для низкостоимостных проектов с минимальными требованиями к безопасности.

Лояльное приложение, использующее в качестве носителя специализированный апплет, занимает более высокое место в рейтинге по сравнению с приложением, использующим теги платежного приложения. Заметим, что компания Apple, выпустив свои спецификации, также далеко не случайно предпочла другим решениям использование специализированных апплетов в программах лояльности, в том числе совместимых с банковским функционалом.

Носители лояльности на базе апплета производителя карт и апплета ПС имеют схожие значения параметров. Целесообразность использования одного из этих апплетов определяется конъюнктурой заказчика. В случае, если заказчик предпочитает быть независимым от ПС и планирует использовать лояльное решение в разных ПС, он выбирает апплет от производителя карт. Если же заказчик хочет быть независимым от производителя карт, например, проводить тендеры по закупке карт, то он выбирает апплет платежной системы.

Список литературы

1. Saar Drimer, Steven J. Murdoch. Keep your enemies close: distance bounding against smartcard relay attacks. Computer Laboratory, University of Cambridge, cl.cam.ac.uk/research/security/banking/relay/bounding.pdf

2. Steven J. Murdoc, Saar Drimer, Ross Anderson, Mike Bond. Chip and PIN is broken. Computer Laboratory, University of Cambridge, cl.cam.ac.uk/~rja14/Papers/nopin-final-submitted.pdf

3. micropross.com/RandD-protocol-analysis-Portable-NFC-spy-MP007-61-p

4. ul-ts.com/industries/ul-card-spy/c-36/p-108

5. youtube.com/watch?v=CU34Oc3n-t0

6. Официальный сайт ООО «СКАНТЕК» scantech.ru

Лидируют в нашем рейтинге лояльные приложения, в которых носителем лояльности являются white label апплеты от независимых поставщиков программных решений, например, апплет PAYCORN[6]. Такие апплеты позволяют свободно перемещать лояльное приложение в любую платежную систему и на карты любого производителя.

В заключение заметим, что апплеты LoyApp и PAYCORN внесены в единый реестр российских программ для электронных вычислительных машин и баз данных Минкомсвязи, что еще больше усиливает их привлекательность для российских заказчиков.