кода обслуживания карты при переносе данных на заготовку с магнитной полосой и использование карты в режиме floor limit).

Значительную брешь в операциях с микропроцессорными картами создает использование банками режима Fallback. Платежные системы уже обязали банки отказаться от этого режима в банкоматных транзакциях (Fallback разрешается под ответственность обслуживающего банка). Более того, в ближайшее время сегодня обязательное использование режима Fallback в POS-терминалах будет заменено на опциональное решение для страновых рынков. В этом случае в странах, где уровень соответствия стандартам международных платежных систем высокий, банки откажутся от использования резервной авторизации по магнитной полосе.

Организационные процедуры управления рисками при эмиссии и эквайринге банковских карт

Общий подход к управлению рисками при эмиссии банковских карт с магнитной полосой

Несмотря на введение платежными системами чиповых или микропроцессорных технологий в процесс обслуживания банковских карт, задача обеспечения безопасности при использовании карт с магнитной полосой остается актуальной. Это связано с тем, что темпы эмиссии карт на микропроцессорные технологии не столь высоки, как хотелось бы, из-за значительной стоимости проектов по миграции карт банка с технологии магнитной полосы на ЧИП-технологию. Поэтому банки продолжают эмиссию банковских карт с магнитной полосой, успокаивая себя тем, что с точки зрения рисков для них практически ничего не изменилось. Разве что, упускается возможность сократить свои потенциальные потери. В этом смысле стратегия банка оправдана, ведь это его право выбирать инструмент управления рисками: технологически (микропроцессор, магни-принт, биометрия, онлайновый мониторинг и т. д.) или организационно (службы поддержки клиентов, службы мониторинга, привлечение услуг страхования и т. д.). С другой стороны, ни одна платежная система не гарантирует 100% защиты микропроцессорных карт от подделки в перспективе, это только вопрос времени и средств, вкладываемых мошенниками для производства поддельных карт. Поэтому средства банка, вложенные в организацию системы управления рисками при использовании карт с магнитной полосой, не пропадут, а уже существующий потенциал Банка с успехом может быть использован и при применении ЧИП-технологий.

В общем случае управление рисками при эмиссии сводится к минимизации влияния рисковых факторов использования банковских карт на доходность бизнеса в целом. Вопрос заключается в поиске компромисса между возможными потерями от мошенничества и теми средствами, которые затратит банк при реализации собственных проектов по предотвращению мошенничества с банковскими картами. С другой стороны, действует всеобщий закон сохранения энергии, материи и т. д.: избыточные меры по обеспечению безопасности операций с банковским картами неизбежно ведут к конфликту с процессом развития бизнеса и качеством обслуживания клиентов и, наоборот, безоглядное развитие бизнеса ведет порой к катастрофическим потерям. Поэтому задача выбора стратегии при минимизации риска мошеннических операций с картами носит актуальный характер.

Рассмотрим выбор стратегии банка в зависимости от этапа развития бизнеса банковских карт в банке:

1) банк только начал эмиссию (до 20 тыс. карт). Страховка. Стандартные отчеты платежной системы — требование страховых компаний;

2) банк достиг среднего уровня — 100 тыс. карт. Страховка, формирование собственной службы мониторинга, подготовка EMV миграции (если не начали сразу);

3) банк достиг уровня массового выпуска и обслуживания карт. Собственная служба мониторинга, call-center, система предотвращения мошенничества, основанная на определенных жестких правилах, которым она следует в режиме онлайн (*on-line rule-based*), система страхования, система мобильного информирования клиентов, формирование технологических инструментов (услуг), позволяющих клиентам самостоятельно управлять рисками.

1 этап эмиссионной программы — начало эмиссии

Очевидно, что при старте программы эмиссии издержки банка и так значительны, чтобы вкладывать серьезные средства в организацию мер по предотвращению потерь от мошенничества. Тем более, что базовые функции обеспечения безопасности уже заложены платежной системой в процесс эмиссии при сертификации Банка, как участника платежной системы. Довольно часто программное обеспечение процессингового центра (ПЦ, собственный или процессор третьей стороны (*third party*)) уже в базовом комплекте содержит набор средств по управлению рисками, часть из которых является обязательными в соответствии

с требованиями платежной системы. С другой стороны, уровень использования банком инструментов управления рисками зависит от его стратегии развития бизнеса, ведь это подразумевает привлечение дополнительных человеческих ресурсов. А увеличение штата сотрудников на первом этапе развития бизнеса всегда является непопулярным. Именно поэтому довольно часто можно встретить банки с эмиссией более 50 тыс. карт, где за вопросы безопасности и мониторинга операций с банковскими картами отвечает один, максимум два сотрудника. И руководство банка можно понять, ведь на его основной вопрос: «А каковы наши риски?», к сожалению, редко можно дать сколько-нибудь аргументированный ответ, особенно при старте эмиссии, когда Банк еще не сталкивался с проблемами такого рода. Ведь ссылки на прессу, пугающую массовыми подделками карт, и статистику платежных систем об убытках банков, разбиваются о «железные аргументы» в виде следующих вопросов руководства с соответствующими комментариями: «Сколько карт мы выпустим в течение первого года? Каков будет средний остаток средств на каждой карте или клиентскому сегменту? Какова вероятность изготовления подделки для каждого сегмента? А теперь посчитайте каков может быть максимальный ущерб банку и сравните с затратами на привлечение дополнительных сотрудников и организацию технологии предотвращения мошенничества.».

По итогам беседы в лучшем случае будет предложено поднять этот вопрос в следующем году. Существует и еще более неприятный вопрос руководства: «Что даст организация мониторинга операций по банковским картам на предмет выявления мошенничества?» Ответ, что мы сможем увидеть, когда у клиента уже похитили со счета все средства (а так обычно и бывает, карточку редко «щиплют» по чуть-чуть, изо дня в день) вряд ли убедит руководство в необходимости создания службы по предотвращению мошенничества с банковскими картами. Единственным сильным аргументов является требование платежных систем выполнять предписанные Банку мероприятия по минимизации рисков, а именно соответствовать стандартам мониторинга и выполнять требования платежных систем по отчетности и регламентным мероприятиям по реагированию на предупреждения, поступающие из платежных систем. Кстати, не помешает упомянуть про возможные штрафные санкции со стороны платежных систем, если будет выявлено несоответствие Банка требованиям по предотвращению мошенничества.

Учитывая вышесказанное, при старте программы эмиссии необходимо убедить руководство банка в необходимости уделить внимание развитию направления обеспечения безопасности операций с банковскими картами. Чтобы быть более убедительным, предложите руководству план развития подразделения в зависимости

от уровня эмиссии банковских карт. Для этого можно запросить региональное подразделение платежной системы о рекомендациях и так называемые «лучшие практики» (*best practice*) по организации подразделений безопасности по банковским картам и зависимости численности подразделения от уровня эмиссии карт. Получив от платежной системы рекомендации и, чтобы не шокировать руководство необходимостью нанять «армию» специалистов по обеспечению безопасности операций с банковскими картами, лучше всего предложить компромиссное решение в лице страховой компании. Тем самым вы уберете неопределенность в процессе решения управления рисками — уплатив страховую премию, банк будет уверен в возмещении оговоренной в договоре суммы по мошенническим операциям. С другой стороны вы получаете еще один стимул в развитии подразделения по обеспечению безопасности. Страховая компания по каждому страховому случаю будет требовать от банка предоставить доказательства того, что банк предпринял все необходимое, чтобы предотвратить потери, связанные с мошенничеством по банковским картам. А сюда как раз и относятся результаты мониторинга и документированные действия банка по предотвращению мошенничества (блокировка карты, отчеты системы мониторинга и т. д.).

Страхование рисков — дело недешевое и соизмеримо с убытками, которые может понести банк от мошенничества. При эмиссии до 20 тыс. карт банк может уложиться в страховую премию до 20 тыс. долл. США в зависимости от условий страхования. При этом покрыто будет практически 100% рисков. Однако с ростом эмиссии страховая премия начинает принимать пугающие значения, значительно превышающие потери банка за предыдущий период, поэтому необходимо искать пути оптимального сочетания страхования с применением иных методов управления рисками.

2 этап — эмиссия до 100 тыс. карт

При эмиссии до 100 тыс. карт количество потихоньку начинает переходить в иное качество. Все чаще возникают случаи мошенничества, и, если служба мониторинга не заметила и не отреагировала должным образом, то возможны конфликты со страховой компанией. Учитывая значительный объем страховой премии, приходится перераспределять финансовой бремя борьбы с мошенничеством между страховой компанией, содержанием службы мониторинга и организацией технологической поддержки.

Обычно банки идут по пути включения в пакет страховых услуг различных франшиз[159], посредством которых значительно сокращается страховая премия, а банк осознанно страхуется только от крупных потерь. Тем самым банк принимает на себя риск потерь, попадающих под франшизу и, как следствие, возрастают требования к подразделению, ответственному за обеспечение безопасности платежей. Размер страховой премии так же стимулирует принятие решение об организации более высокого уровня технологической поддержки службы по предотвращению мошенничества — онлайновый мониторинг, службы поддержки клиентов и проч.

3 этап — массовая эмиссия карт

Конечно страхование рисков остается актуальным, однако с ростом эмиссии Банк начинает понимать, что затраты на страховку несоизмеримы с реальными потерями Банка от мошеннических операций по банковским картам. При значительных объемах эмиссии все разумные пределы франшизы уже израсходованы, и Банк вынужден искать новые пути минимизации рисков. Как и говорилось ранее, Банк идет по пути развития службы мониторинга и инструментов, позволяющих на ранней стадии идентифицировать попытки мошеннического использования карт. Однако, на определенном этапе развития Банк понимает, что никакие системы онлайнового мониторинга, включая чрезвычайно дорогие «нейронные сети», не дают ожидаемого результата. Становится ясно, что без применения качественно иного подхода к управлению рисками нельзя обеспечивать требуемую доходность бизнеса.

Платежная система предлагает переход на микропроцессорную или чиповую технологию. Безусловно, это многократно снизит потери Банка от мошенничества. Но необходимо помнить, что затраты на миграцию на микропроцессорные карты многократно перекроют убытки от мошенничества, даже потенциальные. Переход на ЧИП будет оправдан, если Банк будет рассматривать переход на новую технологию не только как повышение уровня защиты карты, а в основном как процесс, вызванный потребностями бизнеса. Размещение на ЧИПе различных бизнес приложений: программы лояльности, бонусные программы, возможность оптимального офлайнового управления операциями значительно повышают потребительские свойства карты и могут значительно снизить затраты банка, связанные с онлайновой авторизацией. Это является достаточно сильными аргументами для перехода на микропроцессорную технологию.

Так как к этому моменту Банк обычно подходит к аналогичной ситуации в развитии бизнеса, а именно к поиску новых каналов продаж и коммуникации

---

[159] Франшиза — в страховом бизнесе убыток, не покрываемый страховкой (оговаривается в договорах банка со страховой компанией).

с клиентами (CRM-система), возникает мысль о симбиозе бизнеса и безопасности. Наиболее интересным является Интернет и мобильный банкинг, с помощью которых осуществляется информирование клиента и обеспечивается «обратная» связь с клиентом. Естественно, такой механизм коммуникации с клиентом, необходимо дополнить неким юридическим аспектом, перекладывающим на клиента ответственность за убытки от мошеннических операции в случае невыполнения им оговоренных в Соглашении по использованию дополнительных сервисов условий. Естественно, действия клиентов должны быть должным образом замотивированы со стороны банка.

Минимизация влияния рисковых факторов использования банковских карт: взаимодействие банка и клиента

В основу процесса минимизации может быть положена среднестатистическая модель поведения клиента-держателя карты, характеризующаяся рядом параметров, отклонение от которых система онлайнового мониторинга может воспринимать как мошенничество и отказывать в проведении операции. Однако построение адекватной статистической модели поведения клиента требует значительного времени и больших вычислительных ресурсов. Построение подобных статистических моделей поведения клиента хорошо зарекомендовало себя в установившихся системах банковского обслуживания, а при становлении рынка банковских услуг эта задача весьма сложная и вряд ли выполнима для всего спектра клиентов, так как использование карт клиентами в основном носит недетерминированный характер.

Для решения задачи предотвращения мошенничества целесообразно передать часть функций управления рисками непосредственно держателям карт. А именно, на стадии выпуска и функционирования карты держатель карты сможет сам определять стандартную для себя модель поведения. Для этого банк должен обеспечить держателя карты возможностью оперативно изменять параметры модели использования карты. Такой подход требует со стороны банка определенных ресурсных затрат на доработку программного обеспечения, разработку новых технологий по управлению параметрами функционирования карты, доработку программного обеспечения Call Center и организацию соответствующей рекламной компании в среде держателей карт.

Большое значение имеет обеспечение клиента возможностью оперативно, по запросу, получать информацию о состоянии счета, оперативно

блокировать (разблокировать) карту, оперативно получать информацию о проведении (попытках) проведения операций.

К параметрам, определяющим модель поведения клиента можно отнести следующие:

- регион использования карты с детализацией до конкретной страны (чем регион меньше, тем меньше риск успешного использования поддельной карты);
- лимиты на сумму и количество операций выдачи наличных и покупки (на 1 день, на 3 дня, неделю, месяц и т. д.);
- определение категорий торговых точек (группы MCC[160]), где карта не будет использоваться (например, Интернет, заказы по почте и т. д.);
- определение MCC, для которых будет разрешено использование карты, (например, 6010 и 6011).

Управление параметрами риска клиент может осуществлять через:

- 24-часовую службу помощи;
- автоматизированную службу помощи, позволяющую получать информацию по счету и блокировать (разблокировать) карту.
- систему мобильный банк, позволяющую в режиме онлайн: получать смс-сообщения о любом движении по счету; узнавать остаток по счету; блокировать (разблокировать) карту; устанавливать регион использования карты.

Для усиления мотивации клиентов в установке региона использования карты можно ввести некоторые ограничения на использование карты в странах повышенного риска использования банковских карт, соответствующим образом оповестив об этом клиентов. Установка региона использования карты позволит снимать ограничения на использование карты в этих странах на определенный срок, а за одно, можно порекомендовать клиенту на будущее установить регионы использования карты.

Введение ограничений на использование карты самим клиентом в значительной степени повышает эффективность работы систем офлайнового мониторинга банка и позволяет без финансовых потерь, на ранней стадии выявить случаи подделки карт.

В этом разделе будут рассмотрены проблемы управления рисками при обслуживании операций с банковскими картами, связанные только с внешними факторами воздействия на систему «банк-держатель карты», а именно:

- для случаев утраченных/украденных карт;

---

[160] MCC (merchant category code) — тип торговой точки по правилам карточной платежной системы: 6010 — выдача наличных в банке, 6011 — выдача наличных в банкомате.

- для случая мошеннических операций типа «возврат покупки»;
- для случаев транзакций по поддельным картам.

Утраченные (украденные) карты

Этот тип мошенничества приносит наибольшие убытки банкам и, к сожалению, слабо поддается минимизации. Если карта попадает в руки злоумышленников, то время ее использования не превышает 2–3 часов. В среднем по статистике утраченные (и украденные) карты используются не более 3-х дней. Таким образом, самое главное в процессе минимизации потерь банка от этого типа мошенничества — максимально быстрое блокирование карты. Для этого необходимо обеспечить держателя карты соответствующими пособиями, объясняющими его действия в случае утраты карты. Со стороны банка должна быть организована доступная, круглосуточная служба поддержки, отвечающая на телефонные запросы держателей карт. Желательно, в этой службе выделить отдельный телефонный номер для блокировки карт. Можно организовать автоматическую службу поддержки клиентов, позволяющую клиенту по телефону в автоматическом режиме, указав номер карты и кодовую последовательность самостоятельно блокировать карту.

Предоставление клиентам услуги «мобильный банк» позволяет блокировать карту, послав соответствующие смс-сообщение на номер банка или выбрав в меню мобильного телефона пункт блокировки карты. Воспитание у клиента привычки держать карту заблокированной и разблокировать карту, используя «мобильный банк» на время покупки, позволит избежать потерь при утрате карты.

Как превентивную меру от потерь можно рекомендовать клиентам использовать систему лимитов на операции (дневные лимиты, недельные и т. д.).

Применение офлайнового мониторинга позволяет выявить случаи мошеннического использования утраченных карт, однако это не приносит ощутимого финансового результата.

Мошеннические операции «возврат покупки»

Этот вид мошенничества характеризуется тем, что на счет клиента поступает операция «возврат покупки» и увеличивает доступный баланс, а через определенный промежуток времени поступает операция списания на ту же сумму и из той же торговой точки. Если за этот интервал времени доступный баланс будет израсходован то, соответственно,

на счете клиента возникнет неразрешенный овердрафт. Обычно для этой схемы используются карты, держатели которых введены в заблуждение мошенниками и возмещение ущерба вызывает большие проблемы. Сама процедура возникновения подобных пар («возврат покупки»- операция списания) может происходить по двум причинам:

- мошенник работает в торговой точке. Тогда процессирование сначала кредитной операции, а затем через определенный промежуток времени, дебетовой операции не отражается на балансе предприятия;
- мошенник — хакер и использует несовершенство технологии возврата покупки в некоторых интернет-магазинах. Осуществляется мошенническая операция покупки товара в интернет-магазине (например, по чужой карте) и затем оформляется возврат покупки, но для возврата подставляется нужный номер карты, и деньги снимаются в банкомате. После урегулирования претензий держателя карты, с которой была списана мошенническая транзакция, интернет-магазин соответственно дебетует номер «подставной карты» и на счету возникает овердрафт.

Для исключения подобного рода проблем необходимо организовать автоматическую процедуру сопоставления всех входящих операций «возврат покупки» с транзакциями, проведенными по счетам клиентов. Сопоставление необходимо осуществлять за определенный промежуток времени и, начиная с определенной суммы, исключив из него ряд стандартных операций возврата: возврат НДС (VAT — value added tax) и т. д. по усмотрению банка. Сопоставление осуществляется по номеру карты, имени и типу торговой точки при условии не превышения суммы возврата сумме платежа. Если операция «возврат покупки» не сопоставилась, то осуществляется автоматическое блокирование суммы на счету клиента до окончания проведения расследования по этому случаю.

Операции по поддельным картам

Операции по поддельным картам наносят большой ущерб банкам. В последнее время отмечается рост подобного мошенничества. Это связано с высоким технологическим уровнем устройств, позволяющих копировать магнитную полосу карты и доступностью средств производства высококачественного поддельного пластика. Единственным способом, которым может эффективно ответить банк-эмитент в этом случае, является отказ на авторизационный запрос на проведение какой-либо операции. Но как банк может принять решение, какой запрос одобрять, а какой отклонять? Речь, конечно, не идет о банальной ситуации, когда карта заблокирована или когда не достаточно средств для проведения операции. Какой инструмент может использовать банк для управления рисками? В идеале, это онлайн-система,

которая на основе статистических данных поведения каждого клиента сама определяет уровень валидности авторизационного запроса и принимает решение. На практике такие системы чрезвычайно дороги и полностью переложить принятие решения на систему не рискнет ни один банк — ведь это огромный риск конфликта с клиентом. В конечном итоге, даже онлайн-системы, основанные на технологии «нейронных сетей», эффективны только для сбора и анализа информации о модели поведения клиента, а принятие решения в онлайн-режиме по конкретному авторизационному запросу осуществляется на основе свода правил, устанавливаемых для конкретного клиента или группы клиентов. Создание этого свода правил и применение к различным группам клиентов и является основной задачей группы обеспечения безопасности операций по банковским картам.

Правила авторизации операций

Как определить правила принятия банком решения по авторизации операций с банковскими картами?

1. Необходимо постоянно осуществлять мониторинг параметров всех случаев мошенничества с картами в банке и информации, поступающей из платежных систем, с целью формализации угроз банку. Таким образом, можно будет определить страны повышенного риска использования карт, рисковые категории торгово-сервисных точек, а также конкретные торгово-сервисные точки с большим риском проведения мошеннических операций.

2. Зная, откуда исходит угроза банку, можно определить адекватные меры противодействия мошенничеству. Конечно, уровень противодействия в основном определяется степенью готовности процессинговой системы анализировать параметры авторизационного запроса и принимать решение. Эффективность управления рисками определяется сочетанием двух факторов: количеством параметров авторизационного запроса, доступных для управления, и возможностью применения различных правил одобрения запроса к различным группам клиентов, вплоть до отдельного клиента. Таким образом, можно заблокировать использование карты для конкретного клиента в определенной рисковой среде использования карты. Из соображений гуманности по отношению к клиенту, целесообразно использовать так называемые «мягкие коды отказа», а именно «01– свяжитесь с банком эмитентом». При получении такого

кода торговая точка для оформления покупки вынуждена будет связаться со своим обслуживающим банком для получения инструкций. Конечно, ситуация не очень красивая по отношению к клиенту, но это намного лучше чем просто «отказ», или того хуже, «изъять карту». В этой ситуации при настойчивости клиента он все-таки получит товар (услугу), связавшись самостоятельно или через банк-эквайрер с банком-эмитентом. Банк-эмитент, получив сообщение через платежную систему или от клиента по телефону, идентифицирует его и, изменив параметры авторизации для этого клиента, сделает доступным возможность проведения авторизации.

3. Правила могут всеобщими, т. е. для всех клиентов банка, применимые к группе клиентов, и применимые к конкретному клиенту.

К *всеобщим правилам* можно отнести, например, запрет использования карты в сети Интернет (если конечно это оговорено в правилах использования карты). Активация этой услуги происходит лишь после обращения клиента с соответствующей просьбой в банк. Это могут быть ограничения по использованию карты в странах повышенного риска. В этом случае банк уведомляет клиентов через выписки о действующих ограничениях в странах из списка. Например, часто используется такой сценарий: сумма покупки в этих странах не может превышать эквивалент 200 долл. США в день, запрещены получение голосовой авторизации по транзакции, зато разрешены аренда автомобилей и оплата отелей, авиабилетов, а также доступны без ограничений рестораны и т. д. При попытке провести операцию, превышающую установленные общие лимиты, торговая точка получит сообщение «01 — свяжитесь с банком эмитентом». Как показывает опыт, большинство клиентов, побывав в так называемых рисковых странах, ни разу не сталкиваются с установленными лимитами, а Банк, в свою очередь, минимизирует риск мошеннического использования карты.

К *групповым правилам* можно отнести такое ограничение, как установление лимита для корпоративных карт на снятие наличных в конкретной стране или запрет на их использование в казино и т. д. Конечно, банк должен иметь инструмент для управления этим параметром и исключать карту из групповых правил по необходимости.

Правила, применимые к *конкретному клиенту*, это основной инструмент управления рисками. Возможность установления правил использования карты в разрезе каждого клиента позволяет очень гибко управлять рисками, не нанося ощутимых неудобств клиенту. Например, получив сообщение от клиента о проблемах с использованием карты в рисковой стране или получив данные мониторинга о попытках использования карты в рисковой стране и убедившись, что клиент действительно находится там, можно снять на определенный срок (обычно на две недели) все ограничения на использование карты. После окончания действия снятия

ограничений в рисковой стране желательно для таких клиентов принудительно устанавливать режим использования карты — «только в России», соответствующим образом уведомив об этом клиента. Это связано с тем, что мошенничество с банковскими картами носит интернациональный характер и, зачастую, мошенническое использование карты начинается совсем в другом регионе через 7–15 дней после того, как клиент покинул страну повышенного риска. В этом случае операции без ограничений будут разрешены только в России, а во всем остальном мире карта будет работать по приведенному выше сценарию (весь мир, кроме России превратится в рисковый регион), и мошеннические авторизации из других стран будут отклоняться. Теперь клиент будет вынужден уведомлять банк о своих перемещениях по странам, с целью установки соответствующего региона использования карты. Например, можно на определенный срок установить определенную группу стран, которую собирается посетить клиент. Естественно, по желанию клиента должна существовать возможность снятия всех наложенных ограничений. Как показывает опыт, в начале использования такой методики управления рисками клиенты воспринимают ее агрессивно, рассматривая как ограничение своих свобод. Однако со временем и при должной информационной подготовке со стороны банка и средств массовой информации приходит понимание необходимости данных мероприятий и конфликты исчезают.

Управление рисками как общая задача клиенториентированных подразделений банка

Очевидно, что все мероприятия, связанные с управлением риском связаны с большими затратами со стороны банка по организации поддержки клиентов, мониторинга операций и обработки информационных потоков. Ежедневно служба мониторинга банка осуществляет:

- контроль всех авторизационных запросов и операций, поступающих из стран повышенного риска по картам, для которых страна не была открыта клиентом, или клиент уже покинул страну. Формируются запросы в подразделения банка, ответственные за работу с клиентами. Цель запроса- получить подтверждение (опровержение) законности авторизационного запроса или определить местонахождение клиента. Если по косвенным признакам клиент находится в стране повышенного риска (можно проследить

маршрут клиента по транзакциям из duty free магазинов, одиночным успешным операциям из банкоматов и т. д.), но связаться с ним не удалось, то принимается решение о снятии ограничений на определенный срок для исключения неудобств, вызванных ограничениями, установленными для этой страны;

- всем клиентам, побывавшим в странах повышенного риска или торговых точках повышенного риска, направляется уведомление о том, что для карты установлен регион использования Россия и о том, что для сокращения риска мошеннического использования карты клиент может выбрать любой регионы использования карты. Например, Россия, Турция, Египет или Россия и вся Европа и т. д. Соответственно необходимо обрабатывать обратный поток информации, поступающий из бизнес-подразделений о необходимости установки для клиента региона использования карты;
- для карт, у которых установлен регион использования, осуществляется мониторинг транзакций и авторизационных сообщений, поступающих из стран, которые не входят в регион использования. Это делается для выявления попыток мошеннического использования карт и для снятия ограничений, в случае если клиент действительно находится в этой стране, но забыл проинформировать банк и испытывает затруднения в использовании карты.

Управление рисками — это сложная, трудоемкая работа, требующая вовлечения всех клиентоориентированных подразделений Банка. Необходимо отдавать себе отчет, что мы только минимизируем риски, а не стараемся 100% их исключить, так как сие невозможно. Поэтому необходимо помнить, что процедура по идентификации клиента при отработке кода «01-свяжитесь с банком-эмитентом» или при снятии ограничений на использование карты должна быть максимально упрощена. Сочетание двух факторов: фиксация авторизационной системой кода «01» и звонок клиента о проблеме в использовании карты вполне достаточно, чтобы принять решение о снятии ограничений. Не нужно утомлять и раздражать клиента допросом о его номере паспорта, девичьей фамилии матери, адресе и т. д. Нужно отдавать себе отчет, что ни один мошенник не будет ждать завершения процедуры «свяжитесь с банком-эмитентом» и если в Банк поступил звонок, будьте уверены, что это проблемы у клиента банка, а не у мошенника. И ему нужно как можно быстрее помочь. Конечно, можно ввести некоторые процедуры на авторизацию крупных покупок, но они все равно требуют более длительного оформления и в магазине, а несколько вопросов от банка не повредят.

Как уже отмечалось, эффективным способом уменьшения потерь банка является сочетание ограничения функциональности карты с мониторингом активности, а также подключение клиентов к услуге «мобильный банк». Данная услуга позволяет клиенту быстро среагировать на первую мошенническую операцию

и заблокировать карту, однако ущерб от одной операции может оказаться значительным. Оптимальным является пропаганда в среде держателей карт, пользующихся услугой «мобильный банк», возможности разблокировки карты только на период проведения операции (все остальное время карта должна быть заблокирована).

В среде держателей карт, не подключенных к услуге «мобильный банк», целесообразно рекламировать возможность ограничения региона использования карты с целью минимизации риска проведения мошеннических операций. Особенно важно это делать для клиентов, посетивших страны повышенного риска мошеннического использования банковских карт. Таким клиентам необходимо рекомендовать установить для карты регион ее использования, например Россию. И, в случае, выезда клиента в другой регион, ему будет необходимо позвонить в службу поддержки клиентов и открыть для карты требуемую страну, регион.

Эквайринг

В отличие от управления рисками при эмиссии карт управление рисками при обслуживании торгово-сервисной сети требует повышенного внимания с момента старта проекта любого масштаба (даже если это одна торговая точка). Это потребует от банка дополнительных ресурсов по организации мониторинга сети и проверке торгово-сервисных точек. Возникает такая же коллизия с руководством банка, как и при эмиссии карт — а зачем все это нужно, каковы наши риски? Действительно, если не учитывать риск «перехода ответственности на банк-эквайрер» при обслуживании по магнитной полосе карт с ЧИПом, финансовый риск потерь невелик. Однако, отсутствие мотивации у банка-эквайрера в проведении мероприятий по борьбе с мошенничеством не могло остаться без внимания со стороны платежных систем. Как «переход ответственности по ЧИП картам на банк-эквайрер» стимулирует развитие сети терминальных устройств, принимающих ЧИП карты, так административные меры контроля уровня мошенничества со стороны платежных систем заставляют Банк уделять внимание этому вопросу. Система предупреждений и штрафов со стороны платежных систем, с последующим отзывом лицензии не оставляет сомнений в необходимости проведения мероприятий по минимизации рисков мошеннических операций в торгово-сервисной сети Банка.

Управление рисками при обслуживании торгово-сервисной сети заключается в реализации комплекса организационных и технологических процедур направленных на ограничение возможности проведения несанкционированных платежей и создание устойчиво-непривлекательного имиджа торгово-сервисной сети банка у мошенников.

Организационные методы направлены на повышение уровня образованности сотрудников торгово-сервисной сети по приему карт и методам противодействия мошенничеству. Особое внимание необходимо уделять наглядным пособиям и четкости инструкций по противодействию мошенничеству. При заключении с торгово-сервисной точкой соглашения по приему карт необходимо тщательным образом проверить ее на предмет проведения возможных мошеннических операций. Должно насторожить желание предприятия как можно быстрее ускорить заключение соглашения с банком, уклонение от инспекции торговых площадей и предоставления документов по аренде или на право собственности на торговые помещения. С точки зрения мошенников, подложная торговая точка очень выгодное предприятие, если оно еще и работает в сотрудничестве с поставщиками поддельных/украденных карт. Фальшивые карты в огромных количествах используются в такой точке без риска повстречаться с правоохранительными органами. Банк воспринимает высокую активность новой точки как нормальную, и исправно перечисляет на счет мошенников средства по проведенным транзакциям за якобы проданный товар или оказанные услуги. Полученные средства ежедневно переводятся со счетов мошеннической фирмы и обналичиваются. Особенно популярны в этом плане кассы продаж авиа (железнодорожных) билетов, так как не требуют больших затрат на организацию, а 20–30 транзакций в день по поддельным картам на общую сумму 8–10 тыс. долл. США выглядят с точки зрения мониторинга вполне правдоподобно. В дополнение ко всему сказанному, нужно помнить, что мошенники могут заключить соглашения с другими банками и работать параллельно на терминальных устройствах этих банков, тем самым многократно увеличивая доходность этого «бизнеса». Ведь речь идет о фиктивном (неработающем) предприятии, ничто не мешает проводить мошеннические операции. Во всех банках эта точка естественно будет фигурировать под разными наименованиями с вполне адекватными показателями активности. Тревожные сигналы могут поступить через месяц, два в виде уведомлений из платежной системы о проведенных мошеннических операциях. К этому времени мошенники переведут все средства со счетов предприятия и прекратят свою деятельность, переключившись на другие банки. Как с этим бороться?

1. Осуществлять регулярные, частые проверки предприятия в начальной стадии его работы, под разными предлогами: проверка оборудования, рекламные материалы, инструктаж и т. д.

2. Установить на начальный период работы, например на 6 месяцев, задержку в перечисление средств предприятию на 14 рабочих дней с момента транзакции и по достижению определенной суммы.

3. Осуществлять мониторинг предприятия, с установкой параметров, которые предполагают повышенный уровень генерации запросов на подтверждение операций в банки-эмитенты.

При возникновении подозрений, немедленно блокировать работу предприятия для проведения расследования.

Технологические процедуры предотвращения мошенничества:

- 100% авторизация всех операций в торгово-сервисной сети (конечно, это не относится к специфическим сетям с микро-платежами и пр.);
- принудительный ввод на терминале последних 4 эмбоссированных цифр номера карты при формировании авторизационного запроса и автоматическое сопоставление их с данными на магнитной полосе. В случае если данные не совпали, операция не разрешается. Это защитит банк от мошенничества с поддельными картами, когда на магнитную полосу валидной карты, принадлежащей мошеннику, записывается магнитная полоса другой валидной карты ничего не подозревающего добропорядочного клиента банка, скопированная в торгово-сервисной сети;
- лимит на максимальную сумму покупки, на максимальное количество операций, максимальную сумму операций по одной карте и т. д. При превышении лимита авторизационная система банка-эквайрера направляет в торговую точку сообщение «01 — свяжитесь с банком» для проведения дополнительной проверки держателя карты. Сотрудники службы мониторинга должны иметь возможность оперативно изменять значения лимитов, отменять их вообще на какой-то период времени или количество транзакций. Использование этого метода требует от банка дополнительных ресурсов по организации службы по обслуживанию запросов «01», поступающих из торговой сети и инициированных системой мониторинга банка. Сценарий действий банка по ситуации «01» может варьироваться от «симуляции» инициации запроса по держателю карты в банк-эмитент, до реального запроса в банк-эмитент по подтверждению личности держателя карты. Это все зависит от политики банка. Вообще, смысл всех действий заключается в разумном компромиссе между безопасностью и бизнесом. Лимиты,

оптимально установленные предприятиям, оперативность банка в принятии решения по собственному коду «01» должны минимизировать влияние этого процесса на время обслуживания клиента, в то же время возможность применения кода «01» отпугнет мошенника. Трудно вообразить человека с поддельной картой, который спокойно будет ждать завершения процедуры «01-запрос в банк-эмитент», когда будут сверяться данные предъявленной карты и документов с информацией, хранящейся в Банке-эмитенте. Поэтому, если торгово-сервисная точка дозвонилась в банк по коду «01», который был инициирован собственной системой мониторинга, вероятность того, что карту предъявил мошенник, мала, и можно значительно упростить процедуру идентификации клиента, вплоть до ее симуляции. И наоборот, если уровень запросов «01» будет высок, предприятие может отказаться от работы с банком. Поэтому, настройка системы мониторинга таким образом, чтобы минимизировать воздействие на бизнес обеспечив разумную нагрузку на службу авторизации при заданном максимально допустимомый уровне мошенничества в торгово-сервисной сети банка — это своего рода искусство;

- процедура сопоставления операции «возврат покупки». Все операции «возврат покупки» сопоставляются с операциями в торговой точке за определенный период. В случае если операция не сопоставлена по определенному алгоритму, она откладывается из обработки до окончания расследования. Конечно, нет смысла расследовать все случаи не сопоставленных операций, разумным является применение пороговых лимитов: сумма операции, сумма операций за день, неделю. Все случаи превышения лимитов можно отправлять на расследование и по результатам, процессировать операции.

Мониторинг операций в торгово-сервисной сети

Мониторинг операций в торгово-сервисной сети позволяет выявить подозрительные и мошеннические операции на ранней стадии, контролировать положение с мошенничеством в торгово-сервисной сети банка на предмет соответствия стандартам платежной системы по критерию допустимого уровня мошенничества. Набор обязательных отчетов системы мониторинга Банка регламентирован стандартами платежных систем. По результатам мониторинга необходимо проводить мероприятия по расследованию случаев возможного мошенничества для создания у торговых точек устойчивого ощущения постоянного контроля со стороны банка. Естественно, степень расследования должна быть адекватна размерам мошенничества, иногда достаточно одного телефонного звонка в торгово-сервисную точку о необходимости подготовить документы по конкретной операции, чтобы предотвратить возможные мошеннические действия в будущем.