А.В. Антоневич
ОАО «АСБ Беларусбанк»
(Республика Беларусь, Минск)

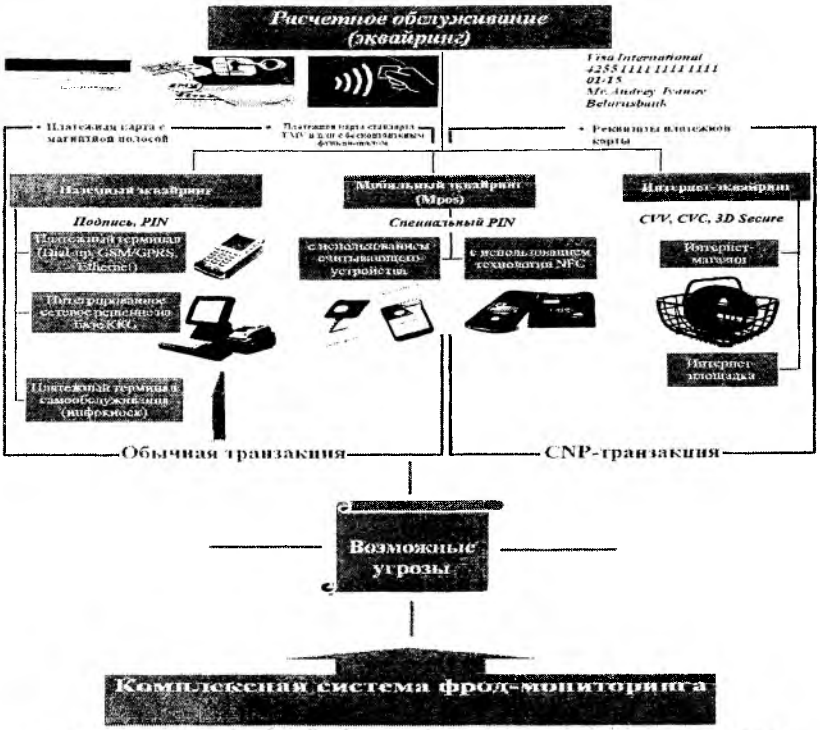
СЕКЬЮРИТИЗАЦИЯ БАНКОВСКОГО РАСЧЕТНОГО ОБСЛУЖИВАНИЯ (ЭКВАЙРИНГА) В РЕСПУБЛИКЕ БЕЛАРУСЬ: ТЕКУЩЕЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

В настоящее время в условиях усиливающейся конкуренции банки, которые являются участниками рынка розничных услуг, нацеливают свои усилия на совершенстование спектра услуг, оказываемых населению, повышение скорости проведения расчетных операций. Борьба за клиента выходит на первый план и для сохранения лидерских позиций на рынке, требует от банков регулярных инноваций как на уровне продуктов и маркетинга, так и на уровне технологий и бизнесс-процессов.

Особое внимание уделяется вопросам минимизации операционного, репутационного рисков банка при осуществлении расчетного обслуживания (эквайринга) и обеспечения безопасности проводимых с использованием банковских платежных карточек (их реквизитов) операций.

Под секьюритизацией банковского расчетного обслуживания (эквайринга) понимают комплекс мероприятий, проводимых банком с использованием программно-аппаратного, технического, аналитического, информационного, административно-экономического инструментария, направленных на поиск, распознавание и устранение потенциальных угроз с целью минимизации рисков банка и обеспечения безопасности проводимых операций с использованием банковских платежных карточек (рисунок).

Рассматривая деятельность банка, включающую осуществление расчетов с организациями торговли (сервиса) (далее – ОТС) по операциям при использовании карточек, а также обслуживание держателей карточек по операциям при использовании карточек выделяют три основных сегмента.



Основные компоненты секьюритизации расчетного обслуживания ОТС

Примечание – Источник: собственная разработка

1. Наземный эквайринг – предполагает организацию обслуживания держателей карточек в ОТС с использованием терминального оборудования, платежно-справочных терминалов самообслуживания (преимущественно в ОТС, осуществляющих реализацию нефтепродуктов и сопутствующих товаров).

2. Мобильный эквайринг – предполагает проведение операций по карточкам с использованием специального считывающего карт-ридера, подключаемого через аудиоразъем к смартфону, а также дополнительно установленного в него специализированного приложения.

3. Интернет-эквайринг – осуществление расчетов с организациями торговли (сервиса) по операциям в глобальной компьютерной сети Интернет, проведенным клиентами с использованием реквизитов карточек.

Следует отметить, что существует множество схем нарушения безопасности проведения расчетов с использованием платежных кар-

точек (их реквизитов), суть которых заключается в получении злоумышленниками карточных данных, необходимых для проведения расчетов и, соответственно, несанкционированному овладению финансовыми средствами, размещенными на счете держателя карточки или причитающихся ОТС за операции по карточкам. Так, например, для наземного (мобильного) эквайринга характерны такие схемы компрометация карточных данных как скимминг, использование накладных PIN-клавиатур, несуществующие платежные терминалы, операции с «белым пластиком», для интернет-эквайринга – фишинг, подделка доменных имен, почтовых адресов, мошенничество на интернет-аукционах и др. Дополнительно к возможным угрозам нарушения безопасности можно отнести:

– нарушение держателем карты правил ее использования: передача близкому родственнику для проведения операций, нанесение Pin-кода с обратной стороны карты и др.;

– допуск персонала ОТС к обслуживанию держателей карточек, не прошедшего обучение Правилам совершения операций на терминальном оборудовании;

– нарушения персоналом ОТС требований Правил совершения операций на терминальном оборудовании в части обслуживания клиентов без проведения предварительной проверки карточки;

– использование платежных терминалов не соответствующих требованиям платежных систем: отсутствует возможность обслуживания микропроцессорных карт и операция проводится по магнитной полосе с игнорированием ввода PIN-кода (в дальнейшем такая операция может быть оспорена, возмещение денежных средств согласно требованиям платежных систем (Lyability shift) осуществляет ОТС);

– уязвимая комплексная система фрод-мониторинга: некорректно выбраны критерии мониторинга при осуществлении операций с использованием реквизитов карт (временные интервалы, количество и объем транзакций, периодичность, лимиты по операциям), отсутствие информации по ранее выявленным случаям нарушения безопасности проведения расчетов с использованием карточек (их реквизитов) и др.

Исходя из банковской практики обслуживания держателей карт в Республике Беларусь в рамках мониторинга операций и контроля рисков при проведении транзакций с использованием платежных карт наблюдаются следующие тенденции:

– наибольший удельный вес fraud-транзакций приходится на долю скиминга;

– более 45% приходится на долю мошенничества с использованием реквизитов карточек. При этом наблюдается значительны рост таких траназакций по сравнению с прошлыми периодами;

– средняя сумма fraud-транзакций по подельным картам уменьшилась в 2 раза и во столько же увеличилась средняя сумма мошеннических операций, совершенных с использованием реквизитов карточек;

– рост количества fraud-транзакций которые не могут быть оспорены в соответствии с правилами переноса ответственности международных платежных систем (lyability shift). Особенно это характерно для CNP-траназакций, при условии предоставления банками технологий безопасности проведения платежей (3D-Secure) держателям карточек и незначительным количеством пользователей данных технологий.

Наибольший удельный вес скомпроментированных карточек банков Республики Беларусь зафиксирован в Украине (30% скомпроментированных карточек), 10% – приходится на долю России, 7% – Болгарии и Таиланда, около 40% на такие страны, как Нигерия, США, Бразилия, Великобритания, Турция. К списку стран, в которых впоследствии совершается большая часть мошеннических операций по поддельным картам, относятся Таиланд, Украина, Россия, США, Болгария, Филипинны и др. Это также характерно для стран, в которых проводятся международные турниры, мероприятия и мировые соревнования, в том числе и для Республики Беларусь.

Основными инструментами по обеспечению безопасности проведения операций с использованием банковских платежных карточек (их реквизитов), в том числе активно используемых в нашей стране по обычным транзакциям является ввод держателем карты на терминальном оборудовании PIN-кода или проставление подписи на карт-чеке по совершенной операции (в зависимости от настройки терминального оборудования), по CNP-транзакциям – использование сервисных кодов (CVV, CVC), технологии 3D-Secure. Дополнительно (в случае необходимости) применяются Token-механизмы, в виде кодов, отдельно генерируемых специальными устройствами или заранее выданных в банке.

Также в рамках функционирования комплексной системы фрод-мониторинга должны применяться инструменты блокировки платежных карт (в том числе с признаком «несанкционированные операции»), идентификаторов терминального оборудования в ОТС, в которых совершены операции определенные как «предположительно мошеннические операции», в т.ч. ОТС, в которых умышленно проводилось копирование реквизитов; осуществляться взаимодействие с ОТС по проведению разбирательства по подозрительным операциям с предоставлением копий карт-чеков по совершенным операциям.

С внедрением международного стандарта EMV (Europay, MasterCard и VISA), обеспечивающего секьюрность платежей в рамках технологии chip & PIN (обязательный ввод PIN-кода при совершении транзакций), банки стремительно приступили к реструктуризации карточных портфелей своих клиентов преимущественно в сторону микропроцессорных карт и оснащению ОТС оборудованием, обслуживающим такие карты.

Применение на практике вышеуказанных подходов, инструментов и технологий, направленных на обеспечение безопасности проведения операций с использованием банковских платежных карточек (их реквизитов) будет способствовать увеличению скорости расчетов, минимизации операционного, делового рисков банка, укреплению позиций на рынке.

А.Г. Беляй
УО «Белорусский государственный экономический университет»
(Республика Беларусь, Минск)

СИСТЕМА ТРАНСФЕРТНОГО ЦЕНООБРАЗОВАНИЯ: ПРОБЛЕМА ВЫБОРА ОБЪЕКТИВНОЙ КРИВОЙ ДОХОДНОСТИ В УСЛОВИЯХ ФИНАНСОВОГО РЫНКА РЕСПУБЛИКИ БЕЛАРУСЬ

Важнейшим стратегическим направлением банковского менеджмента является повышение качества и эффективности управления. Это вынуждает банки искать новые инструменты управления, позволяющие улучшить конкурентные преимущества их банковских продуктов, снизить риски, вызванные, прежде всего, несбалансированностью активов и пассивов, а также объективно оценить эффективность проводимых операций относительно каждого продукта и подразделения