УДК 004.056:336.71

ПУТИ СНИЖЕНИЯ РИСКОВ ИНТЕРНЕТ-ЭКВАЙРИНГА

Голиков С.Е.

ФГАОУВО «Севастопольский государственный университет», Севастополь, e-mail: kcl@mail.ru

Сервисы ведения бизнеса в Интернете используют многие жители России. Любое предприятие или индивидуальный предприниматель может вести свою деятельность или предоставлять услуги через интернет-магазин по всему миру. Для этого необходимо всего лишь создать веб-сайт, который будут использовать потенциальные покупатели для заказа необходимого им товара и/или услуги. Для проведения платежей при помощи платежных карт интернет-магазины заключают договоры эквайринга с соответствующими банками. В статье описан алгоритм совершения покупок при помощи платежных карт, факторы риска, возникающие при проведении платежей в среде Интернет. Исходя из описанных факторов риска, определено, что задействование недобросовестных торгово-сервисных точек влечет возникновение финансовых и репутационных рисков для финансового учреждения. На основании приведенной обобщенной схемы рисков построена классификация основных видов мошенничества, используемых злоумышленниками. Выделенные пути снижения рисков позволили автору разработать методы снижения вероятности наступления рисковых событий в области интернет-эквайринга, состоящие из технических и организационных мероприятий. Описанные практические рекомендации направлены на увеличение эффективности функционирования организованной контрольной среды с целью максимального снижения вероятности реализации рисков.

Ключевые слова: интернет-эквайринг, риски, фрод, электронная коммерция, процессинг

WAYS TO REDUCE THE RISKS OF INTERNET ACQUIRING

Golikov S.E.

Sevastopol State University, Sevastopol, e-mail: kcl@mail.ru

Many residents in Russia are using payment services in the Internet. Any business or individual entrepreneur can conduct their activities or provide services through an online store around the world. To do this, you just need to create a website that potential buyers will use to order the product and/or service they need. To make payments using payment cards, online stores enter into acquiring agreements with the relevant banks. The article describes the algorithm for making purchases using payment cards, risk factors that arise when making payments in the Internet environment. Based on the described risk factors, it is determined that the use of unfair trade and service points leads to the occurrence of financial and reputational risks for a financial institution. Based on the given generalized risk scheme, a classification of the main types of fraud is constructed used by hackers. The identified ways to reduce risks allowed the author to develop methods to reduce the probability of occurrence of risk events in the field of Internet acquiring, consisting of technical and organizational measures. The described practical recommendations are aimed at increasing the effectiveness of the functioning of the organized control environment in order to minimize the likelihood of risk realization.

Keywords: Internet acquiring, risks, fraud, e-Commerce, processing

В связи со стремительным развитием информационных технологий и Интернета, огромную популярность приобрели сервисы ведения бизнеса посредством Всемирной сети.

Любое предприятие или индивидуальный предприниматель может вести свою деятельность или предоставлять услуги через интернет-магазин по всему миру. Для этого необходимо всего лишь создать вебсайт, который будут использовать потенциальные покупатели для заказа необходимого им товара и/или услуги.

Цель исследования: на основании рассмотрения механизма проведения транзакции интернет-эквайринга и выявления основных факторов риска и видов мошенничества определить пути снижения рисковых событий в области интернет-эквайринга, а также перечень технических и организационных мероприятий, направленных на повышение эффективности внутреннего контроля.

Материалы и методы исследования

На рис. 1 показана схема интернет-эквайринга [1; 2].

Алгоритм покупки выглядит следующим образом:

1. При выборе оплаты заказа пластиковой картой покупатель переадресуется на авторизационную страницу провайдера, где им вводятся платежные реквизиты.
2. Провайдер формирует запрос на авторизацию и перенаправляет покупателя в систему авторизации банка-эмитента (ACS).
3. После проведения аутентификации провайдер направляет информацию для авторизационного запроса в процессинговый центр (ПЦ).
4. Процессинговый центр направляет запрос на авторизацию операции в международную платежную систему (МПС).
5. В зависимости от результата авторизации ПЦ формирует сообщение провайдеру о совершении операции либо отказе.

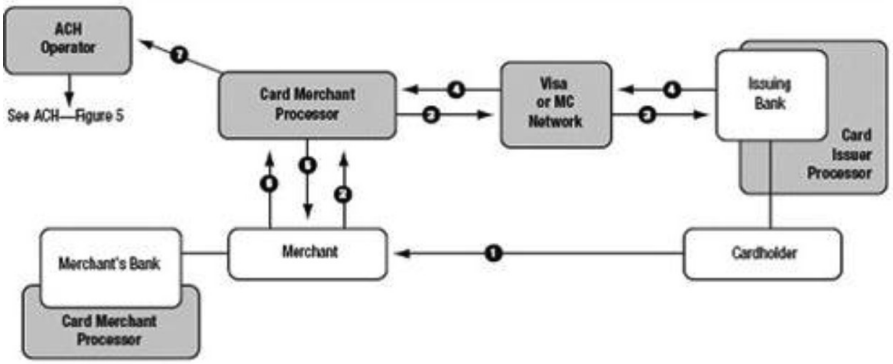

Рис. 1. Диаграмма транзакции интернет-эквайринга

6. Провайдер информирует интернет-магазин и клиента о результатах операции.

7. В зависимости от результата операции интернет-магазин совершает продажу или аннулирует заказ.

8. ПЦ направляет клиринговый файл для проведения расчетов в расчетный банк.

9. Расчетный банк переводит возмещение по совершенным операциям на счет интернет-магазина.

Рассмотрение механизма проведения интернет-транзакции позволяет выявить основные факторы риска:

– расширенные возможности для недобросовестных пользователей, так как покупатель физически может находиться в любой точке мира;

– мощный, недорогой инструментарий и быстрота осуществления транзакций (быстрота открытия интернет-магазина и небольшие затраты могут привести к большим финансовым потерям в случае слабой защищенности);

– постоянная доступность (круглосуточная функциональность, круглосуточная уязвимость для злоумышленников);

– отсутствие единого стандарта (Интернет не имеет установленных централизованных стандартов безопасности онлайн-торговли и регламентов деятельности. Эквайреры в странах, где не предусмотрена уголовная ответственность за преступления с применением платежных карт, где правоохранительные органы не придают данным вопросам должного внимания, не заключены договоры о выдаче преступников, подвергаются большим угрозам со стороны мошенников);

– уязвимость конфиденциальной информации (перехват информации о карточном счете в Интернете является менее сложной задачей, чем проведение транзакции типа МО/ТО);

– достаточно низкая эффективность стандартных механизмов авторизации (анонимность в сети Интернет осложняет ведение любого расследования);

– торговля виртуальным товаром (товары покупаются электронным способом, транзакции проходят очень быстро. Если клиент сообщил вымышленные данные или использовал мошеннический способ оплаты, отследить его будет достаточно сложно);

– трансграничная миграция интернет-магазинов (возможность ТСП вступать в договорные отношения с целью мошенничества, переезд в другую страну, возможность заключения договора эквайринга на менее развитом рынке).

Исходя из вышесказанного, недобросовестные ТСП могут принести следующие виды рисков для банков [3]:

1) финансовые – убытки от оспоренных операций, за превышение уровня фрода, запрещенную деятельность, нарушения правил работы и т.п.;

2) репутационные и правовые – убытки от судебных исков со стороны держателей платежных карт, потеря деловой репутации.

На рис. 2 приведена обобщенная схема рисков [4]:

Основными видами нарушений являются:

– дистанционная продажа рецептурных препаратов, спайсов, табачных изделий, наркотиков, распространение детской порнографии и т.п.;

– нарушение авторских и смежных прав и продажа поддельных товаров;

– продажа и распространение вредоносного программного обеспечения;

– нелегальный гемблинг – проведение азартных игр. Данный тип бизнеса требует приобретения отдельной лицензии, особой обработки транзакций и т.п.

За каждое нарушение предусмотрены со стороны МПС высокие штрафы, которые

доходят до двухсот тысяч долларов, а также исключение из числа участников МПС вплоть до пожизненного.

В подкатегорию «фрод» включены остальные виды мошенничества. Сюда можно отнести [5]:

– работа «под витрину»: прикрытие противоправной деятельности законной;

– нарушение действующего законодательства и правил МПС;

– пирамиды, хайпы, однодневки.

Возможными видами мошенничества, связанные с интернет-платежами, являются:

– использование поддельных номеров карт;

– незаконное получение товара. Клиент товар получил, но ложно сообщает, что товар не доставлен или услуга не оказана;

– использование карты законного держателя другим человеком для заказов посредством сети Интернет;

– кража денег злоумышленниками из системы обработки платежей;

– создание интернет-магазина с целью сбора данных о платежных картах;

– «отмывание денег»;

– поддельные сайты – клоны.

Результаты исследования и их обсуждение

Исходя из вышесказанного, определены следующие способы снижения рисков (рис. 3).

1. Первоначальная проверка ТСП при подключении. Сюда входит проверка анкеты (информация о реквизитах организации, название торговца, юридический и фактический адреса, контактные телефоны, данные о сайте, IP-адрес сервера, на котором расположен интернет-магазин, данные о товарах/услугах, Ф.И.О. должностных лиц, их идентификационные данные). Также проверяются:

– копии решения общего собрания участников торговца, копии приказов о назначении директора и главного бухгалтера;

– копии страниц паспортов должностных лиц;

– копии данных о присвоении ИНН, свидетельства о государственной регистрации, справки об открытии счета, прочие копии учредительных документов.

В случае возникновения проблем с проверкой первичных документов (некорректно заполнена анкета, форма деятельности в уставе и анкете различаются, выявлена регистрация ТСП по поддельным документам, наличие судимостей должностных лиц ТСП, деятельность ТСП направлена только на зарубежных покупателей, торговля «воздухом» и пр.). ТСП отказывают в заключении договора на обслуживание.

К сайту торговца должны быть предъявлены следующие требования:

– наличие полной и четкой информации о торговце (название, адрес, наличие лицензий, адреса для контактов);

– наличие информации о каких-либо ограничениях в обслуживании, если таковые есть;

– указание типов принимаемых к оплате платежных карт, логотипы платежных систем;

– описание условий доставки и передачи товара клиенту;

– описание предоставляемых услуг;

– информация о сроках гарантийного обслуживания;

– описание порядка отказа от платежа и возврата денежных средств;

Рис. 2. Обобщенная схема рисков

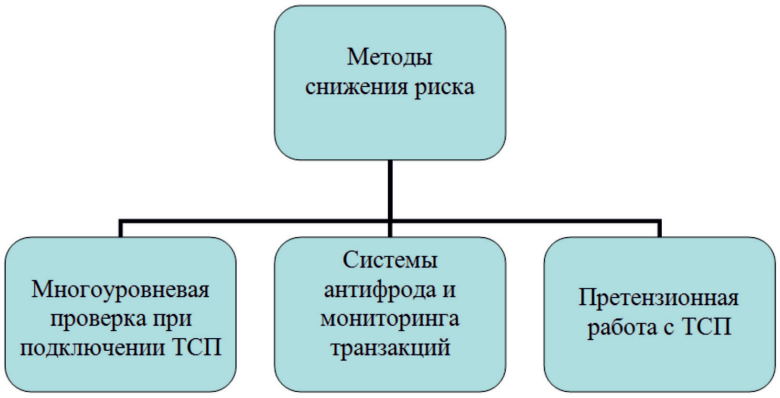

Рис. 3. Методы снижения рисков

– описание валют платежа;

– информация о политике неразглашения и защиты конфиденциальной информации о клиентах, в т.ч. персональных данных.

В случае обнаружения несоответствия сайта торговца предъявляемым требованиям эквайрер предлагает привести содержание сайта к установленным требованиям. ТСП может быть подключено только после устранения всех замечаний.

После осуществления проверок документов и содержания сайта проводится ряд дополнительных мероприятий:

– запрашивается информация о счетах ТСП в других банках;

– проверяется кредитная история учредителей торговой точки, списки поставщиков;

– если торговая точка обслуживалась в другом банке-эквайрере, проводится работа по проверке дополнительных показателей;

– рассчитываются риски банка в случае принятия торговой точкой предоплаты за товары и услуги;

– запрашиваются образцы товаров/услуг, которыми торгует продавец.

2. Системы антифрода и мониторинга транзакций. Основными видами фрода являются:

– кардинг (использование платежной карты или ее реквизитов не санкционировано держателем);

– фишинг (использование поддельных сайтов, внешне похожих на сайт банка-эквайрера);

– «дружеский антифрод» (владелец карты совершает покупку, а затем требует возврата средств на карту вследствие неоказания услуги).

Данные системы позволяют выявить чрезмерный всплеск активности торговой точки, что позволяет проводить анализ. В системах антифрода используются лимиты и ограничения на проведение операций (ограничение количества транзакций по одной карте за определенный промежуток времени, ограничение на максимальную сумму, количество пользователей, использующих одну банковскую карту, и пр.). Обязательным требованием к подобным системам является наличие блока распознавания пользователя. Фрод-мониторинг позволяет оценивать поведение покупателя в процессе проведения электронного платежа. После проведения мониторинга транзакция отправляется на авторизацию по протоколу 3D-Secure (Master Card Secure Code). Если банк не поддерживает данную технологию, то транзакция будет отправлена в процессинговый центр напрямую. Технология 3D-Secure (Master Card Secure Code) позволяет осуществлять аутентификацию держателя карты на специальном сервере банка-эмитента, выпустившего карту.

Претензионная работа с ТСП позволит избежать убытков или хотя бы их уменьшить после того, как произошел фрод или операция была оспорена. В случае обнаружения факта мошенничества необходимо:

1. Установить непосредственный контакт с ТСП и запросить всю имеющуюся информацию по проведенным транзакциям.

2. Если факт мошенничества подтверждается или имеются веские основания предполагать, что мошенничество имело место, надо предпринять следующие действия:

– заморозить счета для получения возмещения по операциям с картами или прочих счетов ТСП;

– расторгнуть договор на эквайринг с данным ТСП;

– уведомить правоохранительные органы о мошенничестве и сотрудничать с ними в целях привлечения злоумышленников к уголовной и иной ответственности;

– обратиться в суд с иском о возмещении убытков;

– внести название ТСП в список ТСП, с которым расторгнут договор на эквайринг.

Заключение

Таким образом, эффективное снижение рисков возможно только тогда, когда соответствующие бизнес-подразделения банка принимают активное участие в риск-менеджменте. Методы снижения рисковых событий в области интернет-эквайринга состоят из технических и организационных мероприятий. Для качественного выполнения организационных мероприятий необходимо разработать систему мотивации всех подразделений, участвующих в обеспечении эквайринга, а также эффективную систему внутреннего контроля, включающую как периодические контрольные процедуры и аудит, так и ежедневные процедуры контроля, встроенные в бизнес-процессы. Чем эффективнее будет организована контрольная среда, тем меньше будет вероятность реализации рисков.

Список литературы

1. Интеренет-эквайринг для «чайников». [Электронный ресурс]. URL: https://habr.com/ru/post/157565/ (дата обращения: 11.03.2020).

2. RETAIL PAYMENT SYSTEMS. [Электронный ресурс]. URL: https://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/retail-payment-systems-risk-management/retail-payment-instrument-specific-risk-management-controls/merchant-acquiring.aspx (дата обращения: 11.03.2020).

3. How to Minimize Risks of Online Merchant Acquiring. [Электронный ресурс]. URL: https://evercompliant.com/minimize-risks-online-merchant-acquiring/ (дата обращения 11.03.2020).

4. Бочаров Н. Мерчанты как повышенный источник риска для Интернет-эквайринга. [Электронный ресурс]. URL: https://bosfera.ru/bo/merchanty-kak-povyshennyy-istochnik-riska-dlya-internet-ekvayringa (дата обращения: 16.03.2020).

5. Анти-фрод системы и как они работают. [Электронный ресурс]. URL: https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/339929.php (дата обращения: 11.03.2020).