Дайджест по материалам зарубежных СМИ

#paymentstoday

№ 32/АВГУСТ 2017

Что будет, если просто взять и отменить наличные?

НПА национальная платежная ассоциация

Содержание

NCPI: Многие из перешедших на цифровые платежи вернулись к наличным

Источник: Livemint.com (Индия)

По мере поступления наличных денег в обращение многие из новых пользователей цифровых платежных инструментов возвращаются к наличным. Менее половины присоединившихся к использованию цифровых платежей после «демонетизации» продолжают использовать их на текущий день. Такие данные приводит один из руководителей NCPI.

Общее число пользователей цифровых платежей через банки выросло с 40 до 100 миллионов в первые пару месяцев после реформы, отменившей хождение наличных на сумму 86% от общего их оборота в ноябре 2016 года. Спустя еще три месяца из новоприбывших 60 миллионов осталось только 25 миллионов, говорит Дилип Асбе, COO NCPI.

«Таким образом, мы имеем 25-30 млн новых пользователей. Пришло существенно больше, но остались только 25млн. Если судить об этих цифрах с точки зрения естественного развития платежных систем, такого прироста пришлось бы добиваться пару лет» - заявил Асбе на открытии платежной платформы Benow, построенной на базе Унифицированного платежного интерфейса (UPI).

На 7 апреля в обращении находилось наличных на сумму 13,6 трлн рупий. Для сравнения на 4 ноября эта цифра составляла 17,97 трлн, а 6 января, после проведения реформы – 8,98 трлн.

В течение ноября-декабря многие системы цифровых платежей – Национальная система электронных переводов (NEFT), Сервис моментальных платежей (IMPS), мобильные банки, UPI и мобильные кошельки отметили значительный прирост числа и объемов транзакций. В феврале, однако, по мере возвращения наличных в обращение этот рост стал замедляться и число транзакций начало снижаться. В марте Банк Индии (RBI) зафиксировал 893,9 млн транзакций, что было несколько лучше данных февраля, но все-таки существенно ниже декабрьского пика в 957,5 миллионов транзакций. При этом объемы транзакций в марте стали рекордными – 149 трлн рупий (по отношению к предыдущему пику в 104 трлн рупий в декабре), что объясняется приходящимся на это время сезоном налоговых платежей, которые стали главным источником роста оборота RGTS и NEFT.

NCPI со своей стороны также занималось продвижением новых средств цифровых платежей. В марте совместно с Reliance Retail и Innoviti был представлен сервис UPI для ритейлеров, который позволяет осуществлять платежи в терминалах через

поддерживающее UPI клиентское приложение любого банка путем сканирования динамического QR-кода. NCPI озабочено расширением сети приема нового платежного инструмента в ретейле, которая, по их ожиданиям, должна сильно вырасти, когда число банков-участников системы увеличится с нынешних 20 до 30-35.

При обсуждении также готовящегося к запуску инструмента для платежей на базе Aadhaar Асбе отметил, что пока остаются открытыми вопросы комиссий для ритейлеров.

«В настоящий момент обсуждается ставка в районе 25 базовых пунктов, что сопоставимо с таковой при платежах по дебетовым картам на сумму менее 2000 рупий». ■

Банк Индии (RBI): Цифровые транзакции выросли на 2.4% в июне

Источник: Livemint.com (Индия)

Общий объем цифровых транзакций вырос за месяц на 2,36% с 111,11 до 113,73 трлн рупий.

Объем цифровых транзакций вырос за месяц, докладывает Резервный банк Индии. Рост составил 2,36% до 113,73 трлн рупий с 111,11 трлн в мае этого года, говорится в представленном RBI докладе.

При этом число транзакций сократилось – до 831,7 млн (с 858,5 млн в мае). Наибольшее же число транзакций было совершено в декабре 2016 года – 957,5 млн.

Под цифровыми транзакциями понимаются осуществленные по кредитным и дебетовым картам, через Объединенный платежный интерфейс (UPI), USSD, предоплаченные платежные инструменты и интернет-банки.

Число POS-транзакций по дебетовым и кредитным картам снизилось в июне на 4% по сравнению с маем – с 233,4 до 224,1 млн. транзакций.

Число транзакций в UPI, напротив, возросло за месяц – с 9,2 до 10,2 млн. По объему рост составил 11% - с 27,7 млрд. до 30,7 млрд. При этом, согласно отчету, с декабря объем транзакций вырос более чем в пять раз.

Также выросло и число транзакций USSD – на 3,26% по отношению к маю.

«Наблюдается экспоненциальный рост числа транзакций UPI в виду растущего присоединения банков, ритейлеров и клиентов... Объем транзакций за 11 месяцев с августа 2016 года достиг 10 миллионов» - заявляет Национальная платежная корпорация Индии (NCPI).

Использование предоплаченных инструментов, таких как мобильные кошельки, снизилось в июне и по числу, и по объему транзакций после пика, достигнутого в прошлом месяце: с 91,3 до 80,1 млн транзакций (-12,25%), с 25,3 до 22,8 млрд. рупий (-10%). В расчет в данном случае принимались только транзакции оплаты товаров и услуг по инструментам восьми эмитентов-небанковских организаций.

Число платежей в Национальной системе электронных переводов (NEFT) и RGTS снизилось за месяц на 2,23% и 5,8% соответственно. ■

Индийский Paytm планирует запустить мессенджер, чтобы конкурировать с WhatsApp

Источник: Reuters.com (Индия)

Один из лидеров цифровых платежей в Индии – компания Paytm – планирует до конца лета выпустить собственный сервис обмена сообщениями, который должен составить конкуренцию Facebook и WhatsApp, сообщает источник в компании.

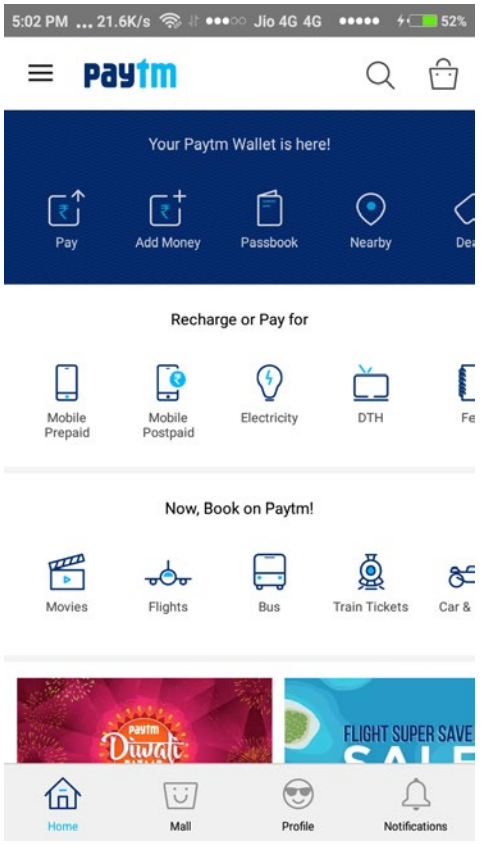
С помощью нового сервиса, встроенного в платежное приложение, Paytm, учредителями которого являются японский SoftBank и китайская Alibaba, собирается привлекать новых пользователей. Мессенджер позволит пользователям отправлять текстовые, голосовые и видео-сообщения, изображения, утверждает анонимный источник.

«В планах Paytm стать для коммерции в Индии цифровой вселенной, в которой покупатели могут и общаться, и оплачивать покупки, и использовать иные финансовые сервисы» - говорит Павел Наийя, аналитик исследовательской фирмы Counterpoint.

Клиентская база Paytm в настоящий момент составляет 225 миллионов человек в Индии. WhatsApp, который, по данным на февраль, имел 200 миллионов активных пользователей в стране, в свою очередь ищет пути вывода на местный рынок собственных платежных сервисов.

Ранее в этом году Hike – еще одна индийская мессенджинговая платформа – представила сервис электронных платежей, встроенный в их приложение, чтобы получить свою долю от стремительно растущего числа цифровых транзакций в стране.

В Индии наблюдается бум электронных платежей, спровоцированный отменой хождения старых купюр крупного номинала, и компании, типа Paytm, быстро наращивают свою рыночную долю. По прогнозам Boston Consulting Group, объем цифровых платежей в Индии



к 2020 году по отношению к 2016 вырастет в 10 раз до $500 млрд. ■

Мобильные деньги – находка для отмывщиков?

Источник: Paymentscardsandmobile.com (Африка)

Развитие международной финансовой системы в последние десятилетия привело к тому, что нахождение и блокирование средств, полученных преступным путем, становится все более сложной задачей. Использование долларов США в качестве основной валюты на черном рынке, общий тренд к финансовому дерегулированию, расцвет финансовых прибежищ, основанных на анонимности и секретности, развитие единого рынка Еврозоны – все ведет к тому, что по прогнозам доля «отмываемых» денег в совокупном мировом ВВП может составить от 2 до 5% (или $1-2 трлн.). При этом, по данным комитета по преступности и наркоторговле ООН (UNODC), правительствам удается изъять из оборота менее 1% этих денег.

«Грязные» деньги сложно отследить

Чем глубже «грязные» деньги проникают в международную банковскую систему, тем сложнее отследить источник их происхождения. Согласно данным общемирового исследования AML, проведенного KPMG в 2014 году, 92% финансовых институтов в Африке указывают, что в их регионе высок риск активности, связанной с возможным отмыванием денег, в том числе, по причине нехватки квалифицированных сотрудников, которые могли бы заниматься этой проблемой. Совместно с растущим финансовым дерегулированием, недостачей автоматизированных систем клиентского риск-менеджмента и работы с политически значимыми лицами по установлению источников их дохода это создает среду, где огромные суммы денег от торговли людьми, оружием, наркотиками, создания террористических организаций, нелегальных армий и прочей криминальной активности быстро и удобно перемещаются из любой точки мира в любую другую. Очевидно, что с усилением угрозы международного терроризма задача по перекрытию доступа различных преступных организаций к финансовым ресурсам становится все более актуальной.

Яркий пример того, как свободно могут перемещаться огромные суммы денег, история прежнего диктатора Конго Джозефа Мобуту, которому приписывают вывод из страны $55 млрд. При наличии риск-ориентированной технологической платформы в африканском регионе это было бы невозможно.

Во всем мире сейчас активно развиваются сервисы мобильных денег. В том числе и в Африке, где они выступают инструментом вовлечения населения в официальную банковскую систему. Однако есть угроза, что мобильные деньги могут быть удобным инструментом и для отмывания денег, финансирования терроризма. Особенно серьезные опасения возникают в отношении Западной и Центральной Африки, где указанная тенденция угрожает так сложно полученному экономическому росту, политической стабильности и перспективам

дальнейшего развития.

Организация по противодействию отмыванию денег в Центральной Африке GABAC указывает на ряд слабостей мобильных финансов в регионе, которые могут быть использованы для незаконной активности. Не все участвующие в цепочке оказания услуг мобильных денег организации одинаково соблюдают и не все финансовые институты и соответствующие регуляторы имеют необходимые ресурсы и могут гарантировать соблюдение надлежащих требований в отношении данной деятельности.

Главная сложность в регулировании мобильных денег проистекает из того, что своим существованием они обязаны ранее не связанным областям – телекому и банковскому сектору – имеющим каждый свое отдельное регулирование, в которое вовлечено множество министерств, ведомств и прочих правительственных институций. Это крайне усложняет и затрудняет осуществление надзора за отраслью.

Также этот рынок формирует ряд уязвимостей с точки зрения безопасности и аутентификации, кросс-платформенной совместимости и документации, которые нужны как агентам, так и клиентам для осуществления транзакций без страха быть обманутым.

Технологии могут сыграть критическую роль

Единственный прозрачный, эффективный и надежный путь противодействия указанным угрозам – технологический. Технологии могут и должны играть главную роль в обеспечении должного функционирования всей цепочки оказания услуг мобильных денег, и это та область, где важна коллаборация между центральными банками и регуляторами телекоммуникационной отрасли.

Одной из компаний, разрабатывающих подобные технологические решения для управления телекоммуникациями и финансовой безопасности, является Global Voice Group. Их продукт M3 позволяет организовывать правительственным организациям мониторинг сервисов мобильных денег путем сбора, обработки и верификации данных по транзакциям любых приложений и систем мобильных денег.

Первой страной, где был внедрен M3, стала Танзания. Регулятор теперь имеет возможность отслеживать соблюдения участниками рынка норм и требований местного законодательства, а население получило возможность повысить финансовую включенность посредством сервисов мобильных денег без угрозы национальной безопасности. Должным образом организованное регулирование принесло также свои плоды и в виде дополнительных налоговых сборов в 63 млрд. танзанийских шиллингов. ■

EBA Clearing привлекла 30 банков к тестированию платформы расчетов в режиме реального времени RT1

Источник: Paymentscardsandmobile.com (EC)

Банк UniCredit приступил к тестированию первого пан-европейского решения для моментальных платежей RT1. Первым новый продукт станет доступен клиентам банка в Германии и Италии. Еще 30 банков изъявили желание присоединиться к инициативе.

UniCredit стал первым банком, готовящимся к запуску сервиса платежей в режиме реального времени для клиентов в рамках Единого европейского платежного пространства (SEPA), который стартует с началом работы платежной системы Европейского платежного совета SEPA Instant Credit Transfer (SCT Inst). Клиенты банка в Германии и Италии первыми опробуют на себе новшество в ноябре 2017 года.

«Введение моментальных платежей в евро позволит нам улучшить поддержку платежного бизнеса как для корпоративных, так и частных клиентов. Предоставление возможности осуществления платежей в режиме 24x7x365 с мгновенным уведомлением плательщика об успешности перевода существенно повысит нашу эффективность и доверие потребителей» - говорит один из руководителей UniCredit Ян Купфер. – «Повсеместное распространение в новой инфраструктуре мгновенных платежей и новое качество сервиса, улучшающее клиентский опыт, несут дополнительные выгоды, которые будут только увеличиваться по мере реализации банком собственной программы цифровой трансформации».

«Мы рады приветствовать UniCredit в числе первых финансовых институтов, активно готовящихся к работе в системе KE1 перед запуском мгновенных платежей на всей территории Евросоюза - действительно востребованного платежного инструмента для всей многонациональной клиентской базы», - добавляет CEO EBA Clearing Хэйс Литтлджон. – «Наша цель в предоставлении платежной индустрии Европы комплексной пан-европейской инфраструктуры уже на старте SCT Inst, и мы счастливы видеть, что RT1 отвечает ожиданиям банков-учредителей и быстро растущего числа их последователей на всем континенте. В настоящий момент к тестированию привлечены банки из различных стран, а к концу лета их число еще увеличится. В ноябре ожидается, что к RT1 подключатся 30 кредитных организаций, а еще 70 сделают это в 2018 году».

UniCredit является одним из 39 учредителей инфраструктуры EBA Clearing, предназначенной для процессинга мгновенных платежей в режиме 24x7 на территории Евросоюза. С ноября 2017 года все обслуживающие счета провайдеры платежных сервисов (ASPSP) в рамках SEPA получат возможность пользоваться гибким платежным решением, полностью соответствующим стандартам ISO 20022 в части передачи сообщений при осуществлении мгновенных платежей. ■

Итоги 18 месяцев регулирования межбанковских комиссий на европейском карточном рынке

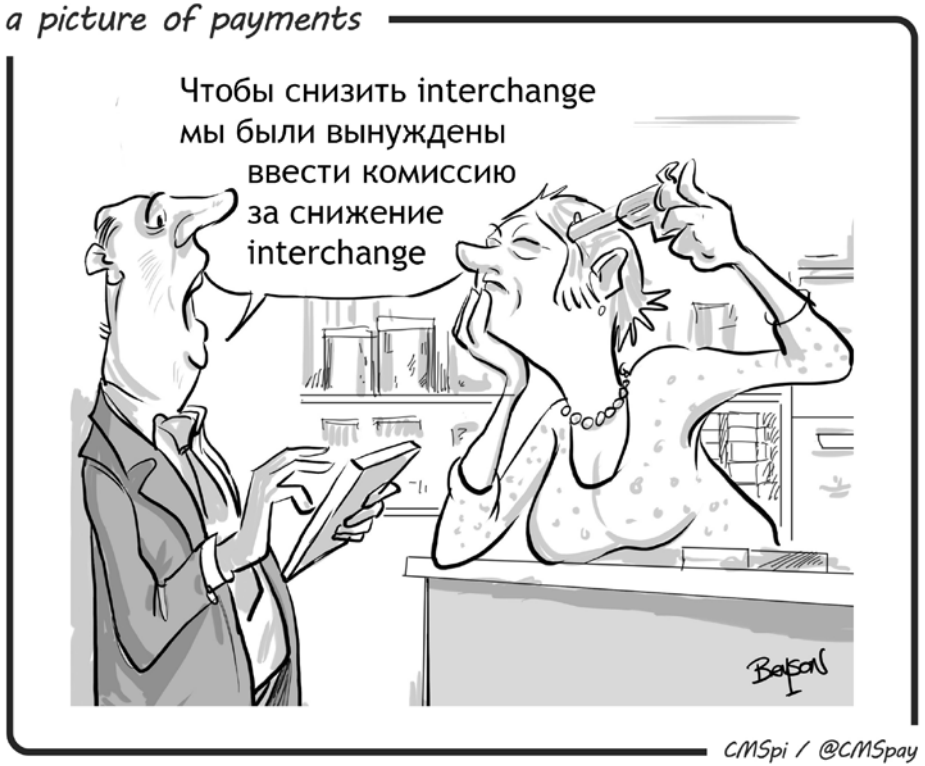
Источник: Paymentscardsandmobile.com (ЕС)

Прошло почти 18 месяцев от введения норм по межбанковским комиссиям (IFR), которые нацелены не только на ограничение размера последних, но и на изменение правил ведения бизнеса по приему и обслуживанию карт в целом. Оказались ли эти меры эффективными с точки зрения достижения поставленных целей и какие неожиданные последствия они вызвали попытался разобрать в своей статье Питер Джонс, управляющий директор PSE Consulting.

Ограничения комиссий по кредитным картам вредят эмитентам

Ограничение interchange fee в среднем на территории ЕС до 0,3% привело ориентировочно к пятидесятипроцентному (или €2 млрд. в год) падению доходов эмитентов кредитных карт. Как следствие, эмитенты значительно сократили затраты на программы лояльности и снизили размеры предлагаемого клиентам кэш-бэка. Многие также ввели комиссии за обслуживание карт.

Наибольшее влияние нормы оказали на крупнейший в ЕС – британский рынок кредитных карт. Крупнейшие ритейлеры получили значительную прибавку к доходам из-за снижения расходов на прием кредитных карт. Предприятия сегмента СМБ оказались не в таком вы-



годном положении – расходы на эквайринг для них сократились незначительно, так как эквайреры компенсировали снизившуюся из-за возросших расходов маржу изменением иных комиссий.

Потребители пока не увидели снижения цен на товары и услуги, которые можно было бы отнести к непосредственному влиянию нового регулирования.

Снижение комиссий по дебетовым картам оказалось небольшим

Во многих странах interchange fee по дебетовым картам и до введения норм находились на уровне 0,2%, однако и здесь можно отметить некоторые изменения.

Страны с традиционно низкими межбанковскими комиссиями (Голландия, Дания) пока не скорректировали их в сторону повышения. Недавно введенные двусторонние комиссии в Германии оказались в пределах установленного ограничения. В Великобритании выросли комиссии за транзакции на крупные суммы. А в Ирландии, напротив, комиссии по дебетовым картам были снижены – до 0,1%. Во Франции предоплаченные дебетовые карты приравнены к кредитным, и потому эффект оказался ниже ожидавшегося.

Согласно отзывам участников рынка, значительное снижение наблюдалось по многосторонним межбанковским комиссиям (MIF). Однако есть сведения, что в ряде случаев комиссии напротив выросли, так что общий эффект оказался незначительным.

Изменения в правилах ведения бизнеса – стимулирование эквайринга в рамках ЕС

Новые правила касаются территориальных ограничений. Можно сказать, что они буквально отменяют границы. Visa и MasterCard и до этого не видели ограничений, однако теперь их инфраструктура наполнилась картами новых франчайзинговых игроков – систем карт для путешественников и развлечений.

Для крупных пан-европейских ритейлеров это открывает возможности по оптимизации затрат на эквайринг через заключение единых лицензионных соглашений. Однако это, в свою очередь, негативным образом сказывается на бизнесе мелких национальных эквайреров, которые не в силах обеспечивать прием карт международных систем на всей территории ЕС. Под ударом оказались и многие локальные дебетовые карточные системы.

Отделение бренда от процессинга усиливает конкуренцию

Наиболее значительные изменения касаются требования по разделению бренда карточной платежной системы и процессинга.

Обозначенное еще в 2005 году в документах SEPA, оно теперь осуществлено в масштабах ЕС, в том числе международными платежными системами. Целью норм было усиление конкуренции между процессингами и уход от монобрендовых сетей. Две главных международных платежных системы полностью внедрили такие возможности и многие эквайреры теперь устраивают тендеры по выбору мультибрендовой авторизации и клиринга.

Возможность выбирать бренд негативно сказывается на локальных системах

Одно из изменений предполагает введение возможности для клиента выбирать бренд при оплате ко-брендовой картой. Решает ли это какую-либо проблему, ведь исследования среди держателей карт никогда не выявляли необходимости в наличии такой возможности?

При этом клиент теперь даже может выбирать вопреки другому правилу, разрешающему ритейлеру предлагать при платеже систему, дающую наиболее низкие цены и наиболее продвинутые возможности.

Одним из следствий стало также то, что локальные карточные схемы получили возможность

выпускать отдельные ко-бейджинговые карты для трансграничного использования и монобрендовые - для домашних транзакций, чтобы не допускать конкуренции со стороны международных брендов. А это с точки зрения задач SEPA является шагом назад.

Прозрачность начислений и их усложнение

Другое правило требует детализации комиссии с ритейлера для обеспечения прозрачности при осуществлении платежа. Предполагается, что должны отдельно указываться межбанковские комиссии, комиссии системы, комиссии за процессинг, комиссии эквайрера. Эмитенты называют это биллингом «интерчейндж ++».

Такая практика принята в США и Великобритании, однако в рамках ЕС она продвигается слабо. Крупные ритейлеры испытывают недостаток в системах по проверке валидности огромных объемов данных, которые они теперь вынуждены получать.

Мелкие ритейлеры предпочитают использовать либо комиссию без разбиения, либо единый процент за транзакции и таким образом уклоняться от исполнения норм.

Правило приема всех карт и возможность взимать дополнительные комиссии остались неизменными

Регуляторы во всем мире обсуждают правило приема всех карт, по которому ритейлер обязан принимать все карточные продукты платежной системы. Новое регулирование разрешает такую практику, но только в отношении карт, на которые распространяются установленные ограничения размеров межбанковских комиссий. При этом у ритейлеров в настоящий момент отсутствует возможность разделять карты на подпадающие и неподпадающие под регулирование. Таким образом, пока норма не может быть реализована до конца.

С другой стороны, согласно директиве PSD2, ритейлеры могут взымать дополнительные комиссии при приеме карт, которые не подпадают под ограничение межбанковских комиссий. Что, опять же, затруднительно исполнить в отсутствие возможности разделять карты.

Некоторые непредвиденные последствия

Итак, какие последствие принятия норм по ограничению межбанковских комиссий оказались не теми, как ожидалось?

Выгоду от ограничений получили крупные ритейлеры, а не потребители и предприятия сегмента СМБ. При этом комиссии по дебетовым картам в ряде стран даже выросли, а снижение интерчейнджа во многих случаях компенсируется повысившимися комиссиями платежных систем.

Крупные пан-европейские ритейлеры предпочитают теперь работать с пан-европейскими эквайрерами в ущерб национальным поставщикам услуги. Пан-европейские лицензии и право клиента самому выбирать бренд в потенции могут привести к ослаблению локальных платежных систем, а потребителей вынудить переходить на отдельные карты для трансграничного использования, которые не соответствуют логике развития SEPA.

Внедрение раскрытия информации о комиссиях носит фрагментарный характер и сталкивается с трудностями в обработке больших массивов данных со стороны ритейла.

Положительные моменты: конкуренция в долгосрочной перспективе должна позитивно сказаться на ценах для потребителей и предприятий СМБ. Для чего, однако, предстоит еще провести много работы. ■

Предоплаченным картам и кошелькам стоит поменять комиссии в ЕС

Источник: Paymentscardsandmobile.com (ЕС)

Новая директива Еврокомиссии сделает невозможным взимание дополнительных комиссий с дебетовых и кредитных карт. В Великобритании правительство расширило эти требования также на продукты AmEx и PayPal. Только в 2010 году британские потребители потратили на такие выплаты £473 млн., говорится в отчете Казначейства Великобритании.

Побочный эффект директивы может состоять в том, что она потенциально негативно скажется на предоплаченных картах и кошельках, ведь их пополнение с помощью карт через ритейлера может подпадать под действие новых норм, пишет Дэвид Паркер, CEO Polymath Consulting. Вопрос состоит в том, является ли комиссия за пополнение платой за сервис или дополнительной комиссией в терминах закона. При этом нужно принимать во внимание, что пополнение с карт (дебетовых и кредитных) сейчас обходится клиенту дешевле, чем через банк, почтовое отделение или наличными.

Анализ Polymath Consulting показывает, что в Великобритании в настоящий момент комиссия за пополнение с кредитных и дебетовых карт взымается с 45% предоплаченных карт и 49% «туристических» и «forex»-карт. Комиссии варьируются от 0,5 до 4,95%, и могут быть одинаковыми или разными в зависимости от карты пополнения. Многие компании предлагают бесплатное пополнение с дебетовых карт, но взимают плату за пополнение с карт кредитных. Теперь же, чтобы соответствовать новым требованиям, им придется либо отказаться от такого способа пополнения, либо не взимать за него плату.

Потенциально это создает большую угрозу для британского рынка предоплаченных карт, где потребители в гораздо большей степени предпочитают платить дебетовыми\кредитными картами, чем в других странах Европы (в которых предпочитаемы иные формы безналичных платежей, к примеру, прямой перевод с банковского счета). ■

Чем обусловлена мода на мега-слияния в платежной отрасли?

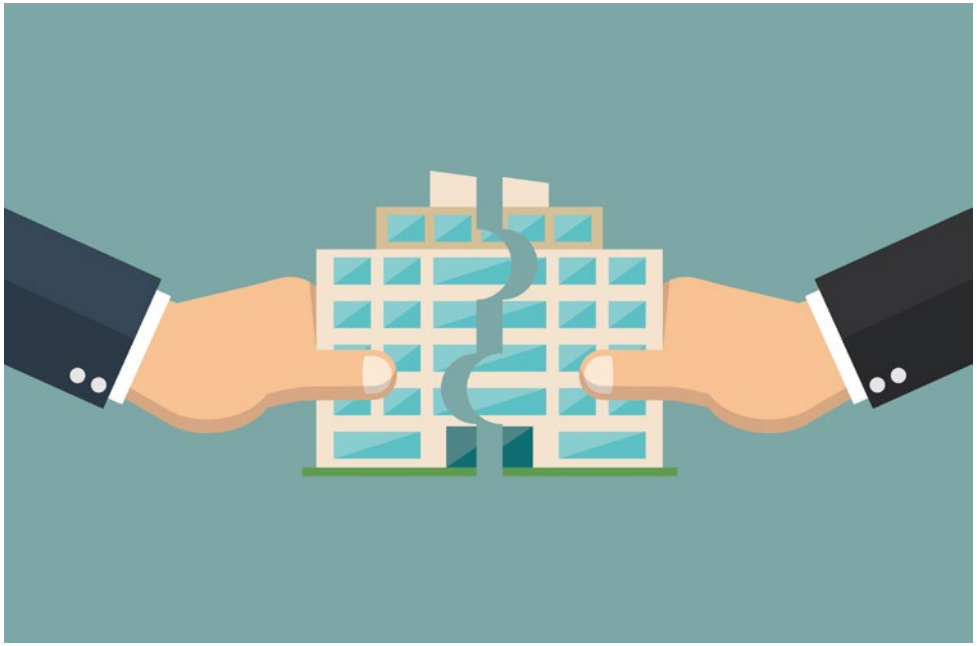
Источник:Paymentscardsandmobile.com (Великобритания)

Долгие годы процессинг платежей рассматривался как скромный пасынок платежной индустрии, незаметно делающий свое дело в глубинах бэк-офиса. Однако в последние 18 месяцев он внезапно вышел на первый план – на волне ожиданий взрывного роста, обусловленного глобальным сдвигом в сторону цифровых и мобильных платежей.

Vantiv, крупнейший процессинг в США, возглавил забег по капитализации тренда роста, сделав предложение на £9.3 млрд. британскому конкуренту Worldpay, чтобы на раннем этапе ослабить позиции другого конкурента – JPMorgan Chase. Согласно данным Financial Times, инвестиционная активность занимающего в США лидирующие позиции по капитализации Wall Street bank также свидетельствует о стратегической значимости процессингового бизнеса для существующих и новых игроков, стремящихся получить свою долю от будущих прибылей.

McKinsey прогнозирует рост выручки на глобальном платежном рынке с $1,8 трлн. в 2014 году до $2,2 трлн. в 2020 году. CEO слившихся Worldpay и Vantiv заявляют, что целью объединения является лидерство в сегменте быстро растущей электронной коммерции, где большинство платежей осуществляется онлайн и через мобильные каналы.

В отчете Capgemini приводятся данные о росте числа безналичных транзакций за 2015 год на 11,2% до 433 млрд. Эксперты прогнозируют усиление конку-



ренции на этом рыке со стороны как банков, так и новых финтех-игроков. И масштаб может стать решающим фактором в этой борьбе. Как отмечает CEO Vantiv, сделка даст объединенной компании новый масштаб и прорывные возможности на рынке. Новая компания перейдет под бренд Worldpay и станет крупнейшей в мире с точки зрения числа процессируемых транзакций.

Текущие события – только начало трансформации отрасли, которая быстро коммодизируется. Масштаб в текущих условиях – единственная возможность противостоять конкуренции, если у вас нет уникального нишевого предложения (такого, как Stripe, к примеру). Однако здесь есть и скрытые риски. Рост объемов цифровых платежей по мере перехода к безналичности означает также и снижение маржинальности платежного бизнеса в следствие консолидации цепей создания добавленной стоимости.

Проблема для рыночных монстров, типа is Vantiv/Worldpay, заключается и в том, что в процессе слияний и поглощений они получают в наследство зоопарк технических платформ, трудно поддающийся инновационному развитию и тормозящий рост добавленной стоимости.

В долгосрочном плане коммодизация будет только нарастать, подстегиваемая усилиями регуляторов в стандартизации инфраструктур и открытии доступа для широкого круга рыночных участников. Источником прибыли и добавленной стоимости станет качество оказания сервиса, к примеру, интеграция в инвойсинг и биллинг, обслуживание счетов онлайн и POS, в банковское и небанковское финансовое обслуживание, во все C2B и B2B-каналы, на локальных и международном рынках. Ситуация сходна с той, что переживает отрасль мобильной связи: деньги будут лежать не в предоставлении собственно связи, а в интегрированном ПО, обеспечивающим связь между пользователями – потребителями (путем связи карты, телефона и интернета) и бизнесом (путем инвойсинга, кэш-менеджмента и т.д.)

Контраргументом может выступать то, что платежная отрасль находится только в начале этого пути, и у гигантов еще есть много времени для того, чтобы получать прибыль от роста объемов платежей. В горизонте трех-пяти лет (а для большинства бизнесов это обычный срок принятия решений) слияния и поглощения вполне разумная практика. Банкиры, инвесторы и аналитики говорят, что платежная отрасль находится в ожидании консолидации и впереди множество новых сделок, в частности, на британском рынке, получившем дополнительную привлекательность на фоне ослабления фунта стерлингов. ■

Еврокомиссия: Цифровые валюты используются организованной преступностью крайне редко

Источник: btcbitcoinnews.com (ЕС)

В недавно подготовленном Европейской комиссией для законодателей и органов власти стран Европы отчете говорится, что использование виртуальных валют организованными преступными группами можно охарактеризовать как незначительное, а случаи вовлечения финтеха в организованную преступность крайне редки.

По мнению авторов отчета, причина этого в технологических ограничениях – прежде всего, недостатке соответствующей экспертизы у преступников.

«Ряд проведенных исследований в отношении виртуальных валют показывает, что они редко используются криминальными структурами. И хотя, в силу своих свойств (в частности, анонимности), они являются привлекательными, необходимость в освоении высоких технологий осложняет возможности их использования».

В докладе также указывается, что встречаются случаи проявления интереса к использованию виртуальных валют в целях финансирования терроризма, однако эти случаи удалось пресечь, чему способствуют усилия правоохранительных органов, отслеживающих активность в социальных сетях. При этом и тут свою роль играет недостаток знаний о новых технологиях.

В завершение авторы отчета отмечают, что отсутствие общеевропейских регуляторных рамок является слабым местом в организации мониторинга транзакций, и ратуют за создание базы данных пользователей и принадлежащих им кошельков, что является крайне спорной мерой, по мнению приверженцев виртуальных валют и приватности в сети.

«Комиссия выпустит отчет, дополнив его предложениями, в том числе о введении полномочий по созданию и ведению централизованной базы данных пользователей и адресов кошельков с доступом для служб финансовой разведки, а также форм декларирования использования виртуальных валют пользователями». ■

Треть миллениалов платили через Venmo за запрещенные вещества

Источник: qz.com (США)

В ходе недавно проведенного среди миллениалов исследования выяснилось, что треть опрошенных оплачивало через сервис Venmo, который крайне популярен у данной возрастной группы, покупку запрещенных веществ.

Опрос являлся частью серии исследований образа жизни миллениалов, проводимой по инициативе финтех-компании Lend Edu, предоставляющей студентам кредиты на обучение и прочие расходы. В данном опросе, проведенном online, приняло участие 1217 студентов различных вузов.

Комментируя приведенные выше результаты, представители Venmo указали, что они строго соблюдают регуляторные предписания и потому по условиям сервиса его запрещено использовать для оплаты ставок и наркотиков. «Если мы наблюдаем признаки того, что сервис используется для гэмблинга или иной незаконной активности, немедленно предпринимаем все должные шаги».

При этом то, что Venmo используется для оплаты наркотиков, не секрет ни для кого. Есть даже сайт Vicemo, публикующий на основе открытого списка транзакций Venmo, список якобы «покупающих наркотики, выпивку и секс». В 2015 году был арестован драгдилер, продававший запрещенные препараты в Колумбийском университете, признавшийся в использовании Venmo для получения оплаты.

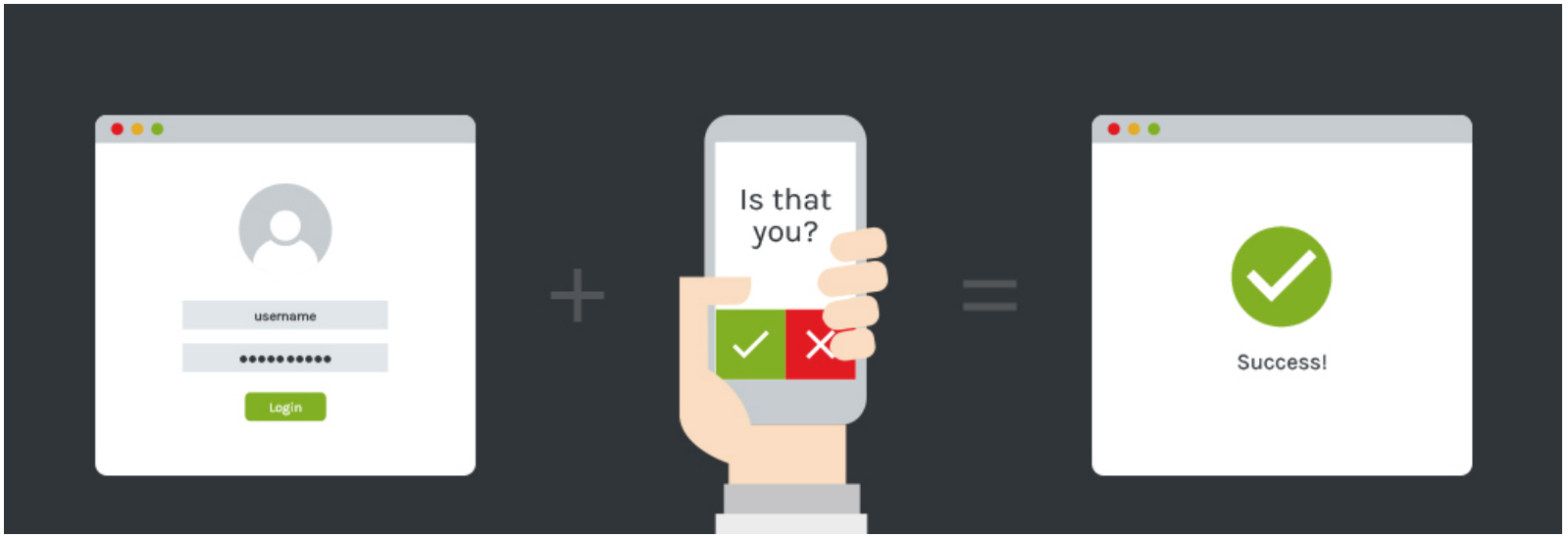
Есть также данные, что Venmo используется для нелегальных спортивных ставок. Анализ, проведенный изданием Quartz, показал скачок платежей через сервис во время баскетбольного чемпионата Национальной атлетической ассоциации колледжей NCAA. Это подтвердило и исследование Lend Edu: 21% опрошенных миллениалов указали, что делали ставки через Venmo.

По итогам 2016 года Venmo обслужило платежей на $17,6 млрд. Выручку сервис получает с торговцев за проведение платежей, для миллениалов услуги сервиса бесплатны. ■

Двухфакторная аутентификация только запутывает

Источник:theVerge.com (США)

Предполагалось, что это будет универсальное средство защиты. что же вышло на деле?



В течение долгих лет двухфакторная аутентификация (2FA) считалась главным советом по обеспечению персональной кибербезопасности, хотя массовое ее внедрение тех-компаниями началось поразительно поздно – после истории, произошедшей в 2012 году с журналистом Мэтом Хонаном. Хакеры получили доступ к аккаунту Хонана на Amazon, после чего смогли получить доступ к привязанным аккаунтам Google, Twitter и iCloud. Журналист лишился почтового ящика и всей почты, данных на всех устройствах Apple, а через его Twitter начали публиковаться посты расистской направленности. Хонан опубликовал материал о произошедшем (и других подобных случаях) в журнале Wired, после чего началась широкая общественная компания, приведшая к массовому внедрению двухфакторной аутентификации как средства от кражи аккаунтов.

Прошло пять лет, и этот совет, кажется, уже устарел. Большинство крупных веб-сервисов использует двухфакторную аутентификацию, но ее результативность вызывает большие вопросы. Хакерам не составляет труда обходить слабую реализацию систем аутентификации, к примеру, через перехват кода или с помощью средств восстановления доступа к аккаунту. О двухфакторной аутентификации говорят как об универсальном средстве защиты, но в реальности ее на сегодняшний день уже недостаточно.

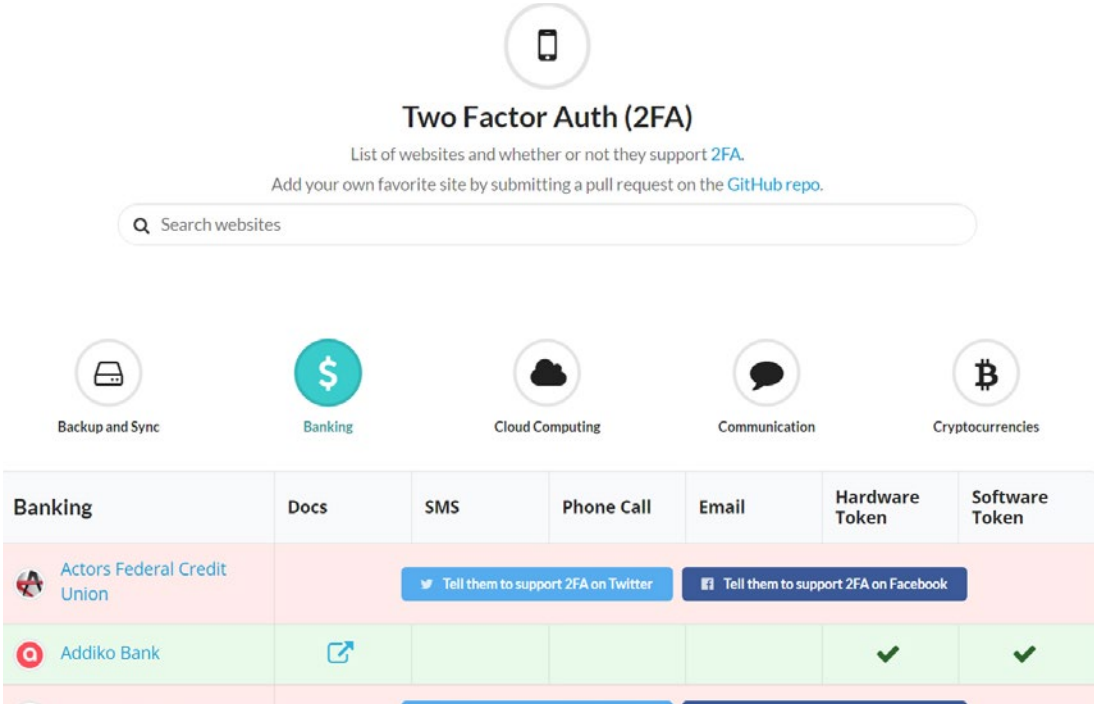
Двигателем развернувшейся кампании за двухфакторную аутентификацию в течение пяти лет был проект twofactorauth.org Карла Розенгрина, посвященный обнародованию и публичной «порке» продуктов, не использующих 2FA. На сайте ведется список веб-ресурсов с

указанием, используют они (и в какой форме) или нет двухфакторную аутентификацию, и, если какой-то сервис ее не использует, посетителю сайта предлагается тут же отправить от своего имени петицию в Facebook, Twitter и на электронную почту такой компании. Ежедневно через сайт рассылаются сотни тысяч жалоб.

Нужно признать, что кампания возымела успех, и сейчас большинство отмеченных ресурсов предлагают ту или иную форму 2FA. Так из крупнейших компаний «уклонистом» остался лишь Netflix. «Наверно, куплю торт, когда они наконец сдадутся». – шутит Розенгрин. Поздно внедрившие 2FA Amazon и BitBucket уступили под напором жалоб, как и все перечисленные на сайте сервисы VPN или криптовалютных бирж. Из почтовых сервисов «держатся» только Migadu и Mail.com. Проблемными секторами остаются сайты банков и авиакомпаний. Большинство все же усвоило посыл: клиенты хотят двухфакторную аутентификацию; у вас ее нет – выберут конкурента, у которого она есть.

Но победа оказалась не такой, какой все ожидали. Способов 2FA теперь столько, что twofactorauth.org не смог бы каталогизировать их все. Кто-то шлет SMS-коды, кто-то использует почту и приложения типа Duo или Google Auth. За $18 можно купить «железное» решение – специальный USB-брелок, поддержку которого обеспечивают многие ресурсы (надо отметить, что это самый надежный из вариантов аутентификации; по крайней мере, до тех пор, пока вы не потеряете брелок). Кто-то использует защиту с помощью длинных паролей, сложных для перебора. Каждый из методов имеет свои плюсы и минусы, и сказать, какой из методов надежнее, часто не могут и подкованные пользователи. Twofactorauth.org пытается разобраться в этом вопросе, но сервисов так много, что у них это не получается.

«Нам и самим сложно проанализировать все сервисы 2FA, которых сотни» – говорит Розенгрин, – «Представляю, каково приходится клиентам».



При этом о том, что не все так уж хорошо с 2FA, говорится уже давно. В 2014 году преступники атаковали биткойн-сервисы, найдя бреши в дополнительной защите – путем перехвата программных токенов и использования различных схем восстановления доступа к аккаунту. В одних случаях атаки осуществлялись путем получения доступа к почтовому ящику жертвы через уязвимость одного из почтовых сервисов, последующего захвата личного кабинета жертвы у мобильного оператора через сервис восстановления пароля по электронной почте, установку переадресации звонков на номер злоумышленника и получение доступа к почтовому ящику Google, привязанному к аккаунту биткойн-кошелька жертвы, путем восстановления пароля через сервис восстановления доступа к аккаунту обратным звонком от Google. В других случаях атаки осуществлялись подобным же способом, но захват личного кабинета жертвы у мобильного оператора производился через звонок в службу поддержки последнего.

В недавно опубликованном расследовании The Intercept об атаке «русских хакеров» на инфраструктуру электронного голосования в США говорится, что доступ к ней был получен путем компрометации аккаунтов госслужащих через подставные сайты почтовых сервисов, куда жертвы попадали по ссылке из писем, полученных якобы от самих сервисов, и где они оставляли свои логины и пароли. Это позволило впоследствии хакерам обойти двухфакторную аутентификацию.

Надим Кобеисси, основатель компании Symbolic Software, также недавно рассказал о случае, когда злоумышленникам удавалось неоднократно захватывать контроль над ранее компрометированным Facebook-аккаунтом его знакомой даже после смены пароля и включения 2FA. Происходило это потому, что компьютер злоумышленника, с которого была осуществлена первая атака, находился в списке «доверенных устройств» сервиса, а открытая на нем сессия не требовала повторного входа даже после такой радикальной смены способа аутентификации.

Конечно, в большинстве случаев дело не в самой двухфакторной аутентификации, а в том, что ее сопровождает. Если есть возможность пробиться через что-то, что связано с 2FA – систему восстановления пароля, доверенные сервисы, доверенные устройства, аккаунт у провайдера сотовой связи – считайте, что доступ у вас в кармане.

Самое слабое место в этой цепочке – провайдеры сотовой связи, которые, кстати, сами не спешат вводить 2FA, используя простейшие PIN-пароли или «секретные вопросы». Если есть возможность компрометировать аккаунт у оператора, то можно получить доступ к звонкам и текстовым сообщениям владельца номера. В одном из известных случаев злоумышленник методично звонил в службу поддержки оператора с просьбой восстановить доступ к аккаунту и раз за разом получал отказ, так как не мог назвать «секретный код». Однако в какой-то момент очередной сотрудник оператора, с которым говорил злоумышленник, «пожалел» последнего и выполнил его просьбу в нарушение протокола. В результате жертва лишилась средств с банковской карты через перевод в его собственном кошельке PayPal, для доступа к которому злоумышленнику понадобилось только указать адрес почты и номер телефона жертвы, а также SMS-код, пришедший на перевыпущенную злоумышленником SIM-карту.

При этом отказ от доказавших свою несостоятельность средств 2FA если и происходит, то крайне медленно. Год назад Национальный институт стандартов и технологий в США отменил поддержку 2FA с использованием SMS, отметив высокие риски перехвата или спуффинга при таком способе аутентификации. Однако тех-компании не спешат реагировать. Некоторые, такие как Twitter и PayPal, напротив, стремятся сильнее связать аккаунт с номером телефона. Защиты меньше, но зато удобно для пользователей. Пользователи же в свою очередь не видят разницы, главное, чтобы аутентификация была двухфакторной.

«Часто мы видим, что решения внедряются только для галочки» - говорит Марк Бродицкий, занимающийся созданием 2FA-систем в Twilio, - «Так, теперь у нас есть двухфакторная аутентификация, этого достаточно. Что дальше по списку?»

Стремление быстрее поставить галочку и забыть про вопрос приводит к ухудшению юзабилити и проблемам с безопасностью. Бродицкий отмечает, как быстро была внедрена система в iCloud Apple вместо просто обходимых вопросов для восстановления доступа к аккаунту, после того, как в 2014 году произошла серия краж ню-фотографий с устройств ряда знаменитостей. При этом то, что по новым правилам утрата кода восстановления и пароля делает невозможным восстановление аккаунта AppleID, теперь вызывает реальные проблемы у многих пользователей.

Можно сказать, что в каком-то смысле усиление защиты провоцирует большую незащищенность: усложняющиеся из-за хакерских атак способы защиты аккаунта вынуждают пользователей возвращаться к более устаревшей, но понятной и простой парольной защите, а это вызывает новую волну атак. «Посмотрите, как сложно

и запутанно устроена защита, скажем, в Apple» - говорит Бродицкий – «Если они не внедрят более прозрачный подход, все кончится волной массовых утечек».

Google – один из редких сервисов, активно мотивирующих уходить от слабо защищенных SMS-кодов к более серьезным методам защиты. Правда это распространяется только на корпоративных пользователей G Suite, в рамках которой администратор может самостоятельно устанавливать правила аутентификации для организации или домена. Но этот метод работает только там, где есть администратор, который может установить правила и требовать их соблюдения. Сложно представить, что такое было бы возможно в массовых консьюмерских сервисах, типа Gmail, поэтому Google даже не пытается добиваться этого.

«Правда заключается в том, что, как мы обнаружили, пользователи не используют больше защиты, чем считают необходимым» - говорит Марк Ришер, отвечающий в Google за продукты по аутентификации, - «Так что как провайдер интернет-сервисов для массового пользования мы вынуждены искать правильный баланс».

Ничто из вышесказанного не означает, что 2FA бессмысленна, но она точно не является панацеей, как виделось в 2012 году. Добавление аутентификационных кодов усложняет доступ к сервису, но хакеры находят новые возможности для обхода защиты – через аккаунт сотового оператора, доверенные устройства или службу поддержки, готовую по первой просьбе сменить пароль к аккаунту. Эти слабые места и есть реальное мерило того, насколько защищен аккаунт. Но они не видны со стороны, пока ничего не произошло. Как результат, даже опытные пользователи не могут определить, какой сервис действительно защищен, а какой нет.

По мере того, как развитие уходит вперед от двухфакторной аутентификации, обеспечение безопасности становится неизмеримо более сложным процессом. Фокус смещается на выявление угроз, оценку большого числа параметров – таких, как использовался ли сканер отпечатка пальца при входе, каково поведение на сайте и т.д. Ввод подозрительного пароля приводит к блокированию аккаунта или звонку из службы безопасности. «Проблема в том, что нет метода, который бы подходил для каждого случая» - отмечает Бродицкий, - «Так что в долгосрочном плане победит модель, предполагающая и обнаружение, и предотвращение». Для таких гигантов, как Facebook или Google, располагающих лучшими в мире подразделениями машинного обучения и безбрежными океанами данных для натаскивания алгоритмов, это действительно хороший способ ловить преступников и предотвращать преступления. Однако для конечных пользователей это может стать откатом назад, когда вопросы безопасности были уделом неизвестных экспертов из неведомых лабораторий. И это не обязательно плохо: обнаружение угроз работает не хуже 2FA. Просто конечные пользователи не смогут оценить, действительно ли работает система, и есть ли система надежнее, чтобы перейти на нее.

Такой сдвиг оставляет пользователей в недоумении. С одной стороны, двухфакторная аутентификация остается лучшим советом по обеспечению безопасности. С другой стороны, ее одной явно недостаточно. И никто не сможет дать совета, как поступить, скажем, если кто-то опасается, что содержимое его почтового ящика может быть выложено на Wikileaks.

Нет никаких инструментов, которые могли бы обеспечить полную защиту. Хотя долгие годы и казалось, что таковые существуют. ■

www.paymentcouncil.ru