

АВТОРСКАЯ АНАЛИТИЧЕСКАЯ СТАТЬЯ

Редакционная дата: 22 сентября 2026 г.

Бабушка, которую заподозрила система борьбы с мошенничеством

Когда осторожность заперла счёт

Эмили привела дела в порядок ещё до того, как ей понадобилась чужая помощь. Она выдала двум внукам доверенность на случай утраты дееспособности. А однажды дверь её счёта не открылась: карточка перестала работать, интернет-доступ был закрыт. Эмили не утрачивала дееспособности и по-прежнему регулярно пользовалась счётом. Но банк зарегистрировал доверенность и изменил права доступа, не задав дополнительных вопросов, которые могли бы выявить простую истину, потерянную процедурой: хозяйка денег здесь, понимает происходящее и хочет распоряжаться своими средствами. Она отменила доверенность и прислала подтверждение. Юридическая запись быстро вернулась в прежнее состояние, а дверь счёта — нет. Восстановление карточки и онлайн-доступа заняло недели. Из-за ограниченной подвижности Эмили ездила в отделение на такси, чтобы каждый раз снять пятьдесят фунтов. Служба финансового омбудсмена Великобритании обязала банк возместить поездки и выплатить 350 фунтов за неудобства и задержку.1

Это реальный случай, когда бабушка пострадала от системы защиты полномочий. Но, строго говоря, никакая модель искусственного интеллекта не объявляла её мошенницей — утверждать обратное нельзя. История задаёт более широкий вопрос: как мера, придуманная для защиты денег, превращается в барьер между деньгами и их владельцем? В другом деле той же службы женщина по имени Вера переехала в дом ухода из-за деменции, а её дочь Джоан оплачивала счета по доверенности. Когда Джоан попыталась сделать крупный перевод, антифрод-система банка остановила необычную операцию; сотрудники впоследствии убедились, что она настоящая. Однако проверка обнаружила, что дочь пользуется данными входа матери вопреки условиям банка. Омбудсмен признал прекращение такого доступа правомерным, но банк не помог доверенному лицу воспользоваться доступной альтернативой со своего телефона. В итоге он предоставил практическую помощь и выплатил 200 фунтов. Здесь система обнаружения мошенничества уже прямо вошла в сюжет, но проблема была не только в точности подозрения — важнее оказалось то, что случилось после его снятия.2

28 июня 2025 года клиент HSBC, чьё имя омбудсмен скрыл под буквой M, попытался через банковское приложение перевести другу 400 фунтов. Антифрод-система приостановила операцию и прислала просьбу позвонить. С первого раза голосовая проверка не сработала. Клиент перезвонил, успешно прошёл её и услышал от сотрудника, что перевод будет выпущен. Тем временем первый сотрудник уже начал блокировать счёт, а второй не видел, что происходит в параллельном процессе. На следующий день клиент не смог войти в приложение, и его направили в отделение. 30 июня он потерял полдня работы и приехал туда, хотя к тому моменту уже отправил деньги другу другим способом. Омбудсмен не счёл само подозрение ошибкой: первоначальные проверка и блокировка были разумны. Возмещения потребовала другая ошибка — человеку сказали, что деньги уйдут, хотя это уже было невозможно. Компенсация составила 200 фунтов.3

Эти бюрократические подробности правдивее удобной сказки о злом банке и глупом алгоритме. Деньги заблокировали не потому, что машина юридически «обвинила» владельца в мошенничестве, и омбудсмен не признал несправедливым каждый шаг. Вред возник на стыке систем, каждая из которых была отчасти права: движок заметил аномалию, голосовая проверка дала сбой, один сотрудник изменил статус счёта, другой не увидел изменения, приложение не объяснило владельцу происходящее. Каждый компонент мог отлично пройти собственный тест, а путь клиента целиком остался плохим. В этом парадокс: система может успешно поднять красный флаг, а учреждение — не суметь его опустить после выяснения обстоятельств. Если успех измеряют в момент сигнала, куда записать часы, которые владелец счёта провёл под этим флагом?

Большие суммы и малая доля

Банки правы в исходной необходимости таких систем. Мошенничество — не мелкая помеха, которую можно оставить дружелюбному сотруднику с бесконечным временем на каждую операцию. По данным отрасли, приведённым UK Finance в мае 2025 года, британские учреждения в 2024 году предотвратили несанкционированное мошенничество на 1,45 миллиарда фунтов. Заявленные потери от него составили 722 миллиона фунтов в 3,13 миллиона подтверждённых случаев. Ещё 450,7 миллиона фунтов клиенты и организации потеряли из-за обманных переводов, которые владельцы счетов санкционировали сами. Цифры серьёзные, но они не являются сравнительным испытанием, доказывающим оправданность каждой остановки. Они не сообщают, сколько законных переводов задержали и сколько людей заставили практически доказывать свою невиновность перед автоматическим подозрением.5

Масштаб сумм искушает учреждения одной метрикой: «Сколько преступлений мы поймали?» Здесь начинается тихое математическое искажение. Представим миллион операций, из которых тысяча действительно мошеннические, то есть одна десятая процента. В чисто учебном расчёте, не описывающем конкретный банк, модель обнаруживает 90 процентов мошенничества, но ошибочно сигнализирует об одном проценте нормальных операций. Она найдёт 900 мошеннических случаев — впечатляющий слайд. И остановит 9 990 законных операций. Проверяющим достанутся 10 890 сигналов, из которых верными окажутся примерно 8,26 процента. На один правильный сигнал придётся более одиннадцати сигналов о нормальной операции. Вывод не в бесполезности модели. Он в том, что фраза «мы поймали девяносто процентов зла» говорит о повседневном опыте людей куда меньше, чем кажется.7

Так проявляется эффект базовой частоты (Base Rate) в редких явлениях. Легко прочитать полноту обнаружения (Recall) как вероятность того, что любой сигнал верен. Но последняя — точность положительных прогнозов (Precision) — зависит ещё и от распространённости мошенничества. Банк может понизить порог, поднять полноту и найти дополнительные атаки, отправив при этом ещё тысячи настоящих клиентов на проверку. Поднимет порог — часть мошенников снова пройдёт. В статистике это знакомый компромисс между ложноположительными (False Positives) и ложноотрицательными (False Negatives) решениями. В банке он не остаётся на бумаге: становится неоплаченным счётом, пропущенной сменой, задержанной зарплатой медсестры и человеком, который убеждает телефон, что его голос всё ещё принадлежит ему.

Но нельзя позволять лгать и самому расчёту. Доли в примере с миллионом операций целиком гипотетические: это не мировой уровень мошенничества и не оценка качества HSBC. Даже термин «ложное срабатывание» требует точности. Операция может оказаться законной после расследования, хотя её временная остановка была разумна

по данным, доступным в момент решения. Правильная оценка спрашивает не только, обнаружился ли риск в конце. Она проверяет, были ли степень подозрения, сила вмешательства, продолжительность ожидания и доступные альтернативы соразмерны риску, который можно было видеть тогда. Нельзя задним числом осуждать всякую прежнюю осторожность. Но нельзя и прикрывать необходимостью осторожности всякую последующую задержку.

Мошенничество бывает разным

Отчасти путаницу создаёт само слово «мошенничество». Бывает операция, которую совершает злоумышленник, укравший карточные данные или захвативший средство аутентификации. Бывает перевод, который настоящий владелец счёта отправляет сам, поверив обманной истории. В первом случае необычное устройство, место и способ поведения могут быть ценными признаками. Во втором и телефон, и отпечаток, и сам человек подлинны; ошибочна история, побудившая его дать распоряжение. Совместный отчёт Европейского банковского управления и Европейского центрального банка за декабрь 2025 года отметил: строгая аутентификация остаётся действенной против видов мошенничества, для которых создавалась, а преступники всё чаще склоняют владельцев самостоятельно подтверждать мошеннические операции. В отчёте приведена сумма заявленного платёжного мошенничества в Европейской экономической зоне за 2024 год — 4,2 миллиарда евро. Это денежная стоимость, не доля от числа платежей; смешивать её с предыдущим примером нельзя.6

Если банк оценивает риск вопросом «у плательщика его обычный телефон?», он может лучше отвечать на прежнюю задачу, пока мошенничество переходит к другой: «зачем он платит, кому и какой рассказ его убедил?» UK Finance описывает преступников, выманивающих одноразовые коды, и сохраняющуюся связь мошенничества с санкционированными переводами и коммуникацией вне банка. Это не делает проверку устройства бесполезной. Это означает, что обучающийся противник постарается заставить человека выполнить все правильные шаги за него. В машинном обучении это называют дрейфом концепции (Concept Drift): меняется связь между выученными моделью признаками и реальным мошенничеством. Меняется и нормальное поведение невиновного клиента — в путешествии, после выхода на пенсию, во время болезни или переезда. Статистически странное тогда оказывается жизненно обычным.568

Чему алгоритм не научится на предотвращённых операциях

Исследования в этой области давно вышли за рамки сравнения алгоритмов по общей точности. В работе Андреа Даль Поццоло и коллег, представленной на конференции IEEE в 2015 году, описаны реальные антифрод-системы: они видят потоки операций, а следователи способны изучить лишь небольшую группу самых рискованных сигналов. Ранняя информация поступает от сотрудника, связавшегося с клиентом; окончательное подтверждение приходит через несколько дней, когда клиенты сообщают о несанкционированных операциях. Выборки неодинаковы. Увиденное сотрудником уже отобрала прежняя система как подозрительное, а остальные операции такого отбора не проходили. Исследователи отдельно обработали обратную связь проверяющих и поздние подтверждения, затем объединили результаты и повысили точность сигналов в своей среде.7

В последующей статье IEEE 2018 года команда изучила более 75 миллионов реальных карточных операций за три года и показала, как дисбаланс классов и дрейф паттернов влияют на оценку и обновление системы. Эти данные не позволяют объявить одинаковые доли у каждого современного банка или обещать модели, успешной на одном рынке, наборе карт и временном отрезке, тот же результат в другой стране. Но методологический вывод принципиален: чистая обучающая выборка, составленная постфактум, плохо отражает решение, принимаемое за секунды при недостатке сведений. Превосходство в историческом тесте не определяет поведение системы после того, как мошенники к ней приспособились, клиенты изменили привычки, а истина об операциях запаздывает относительно сигналов на месяцы.8

Есть более глубокая проблема — назовём её «слепотой предотвращённой операции». Если система отклонила перевод до отправки, она не увидит, что произошло бы при разрешении. Деньги ушли бы мошеннику и исчезли? Или пришли бы арендодателю? В первом случае остановка выглядит успехом, во втором — срывом услуги. Но контрфактической истины в журнале может вообще не быть. Более того, система способна пометить остановленную операцию как «предотвращённое мошенничество» в силу самого правила подозрения, если независимой проверки не было. Когда такую метку используют для обучения новой модели, та рискует научиться подтверждать прежние суждения системы. Это не обвинение конкретного учреждения, а проблема причинного вывода: решение изменило наблюдаемый результат, и порождённых им данных недостаточно, чтобы доказать правильность решения.

Проблема усиливается, если мера зависит от уровня риска. Операции с высоким баллом идут на тщательную ручную проверку, низкие проходят без вопроса, средние получают дополнительную аутентификацию. Выборка становится следствием модели, возникает смещение отбора (Selection Bias). Если следующую систему обучать только на

случаях, дошедших до сотрудников, жизнь покажется ей почти сплошным мошенничеством. Если считать законной всякую операцию, о которой не заявили как о мошеннической за неделю, потеряются жертвы, обнаружившие ущерб позднее, и те, кто не умеет подать жалобу. Решение не в проверке человеком всего подряд. Нужны ограниченные управляемые измерения, ясно оцениваемые контрольные выборки, запись степени уверенности, времени появления истины и её источника. Проверяющий здесь не декоративная кнопка «человек в контуре», а инструмент получения знания, которого один балл не даёт.

От вероятности к решению

Отсюда видно, почему просьбы «повысить точность» недостаточно. Алгоритм может выдавать вероятность, которую сначала нужно откалибровать (Calibration): оценка 0,8 должна не просто стоять выше 0,6, а по возможности соответствовать реальной частоте события на подходящих выборках. После калибровки остаётся отдельное решение: что делать при заданной вероятности? Для крупного перевода новому получателю разумно запросить дополнительную проверку даже при умеренном риске. Если же речь о срочном счёте за лекарство, неисполнение которого причинит немедленный вред, одной необычности операции мало. Следует учитывать цену остановки и возможность проверить её менее разрушительно.

В простой модели решений ожидаемую стоимость разрешения — вероятность мошенничества, умноженную на ущерб, — сравнивают с ожидаемой стоимостью блокировки — вероятностью законности, умноженной на причинённый блокировкой вред, — добавляя стоимость вмешательства и остаточный риск. Реальность сложнее: один убыток банк компенсирует, другой нет; остановка может спасти клиента от обмана, которого тот пока не понимает; закон иногда требует мер, не сводимых к прибыли. Но сложность — повод расширить расчёт, а не исключить из него цену для клиента. Исследования стоимостно-чувствительного обучения (Cost-Sensitive Learning) предлагают разные пороги в зависимости от цены ошибки в конкретном переводе, вместо предположения, будто ошибки всех операций равны.[9]

Главный принцип: обратимость защитного решения (Reversibility) — свойство безопасности, а не любезность интерфейса. Банк может остановить перевод на час, чтобы связаться с владельцем по надёжному каналу; такую предосторожность можно разрешить. Но когда остановка превращается в заморозку всего счёта, затем в запрет цифрового доступа, затем в телефонное сообщение, которое не ведёт к сотруднику, учреждение переносит операцию из области финансового риска в область конфискации времени и дееспособности. В надзорном отчёте за июль 2024 года Бюро финансовой защиты потребителей США (CFPB) описало учреждения, замораживавшие счета из-за подозрительной активности и не уведомлявшие часть клиентов или не объяснявшие,

как восстановить доступ. Некоторые отклоняли или блокировали большинство звонков с номеров, связанных с замороженными счетами. Люди неделями и месяцами не могли воспользоваться деньгами; проверяющие признали часть практик несправедливой.4

Организация, умевшая заблокировать номер в телефонной системе, вероятно, пыталась помешать мошеннику воспользоваться запасным каналом поддержки. Но тем же действием она перекрыла настоящий канал, нужный законному владельцу, чтобы снять подозрение. Спасательный инструмент превратился в дверь, которая открывается лишь тем, кому спасение не понадобилось. Клиент может знать, что счёт заморожен, и не иметь доступа к человеку, способному объяснить разморозку. Получается замкнутый круг: доступ закрыт из-за подозрения, а возражение недоступно из-за закрытого доступа. Для такого сбоя не нужен передовой искусственный интеллект. Но вред умножается, когда автоматические системы распределяют ограничения по разным частям учреждения без единого журнала, показывающего состояние решения и ответственного за его завершение.

Есть, однако, сильный довод с другой стороны. Клиент может признать, что сам дал распоряжение, и настаивать на его законности, находясь под давлением мошенника, который диктует ответы. Британский омбудсмен опубликовал дело Эвана: крупные переводы проходили через друзей ради помощи третьему лицу, а банк счёл обстоятельства возможным признаком обмана или принуждения. Он ограничил часть переводов, сохранив другие способы получить наличные и исполнить обязательства. Омбудсмен не поддержал жалобу, но подчеркнул необходимость регулярно пересматривать ограничения. Этот случай напоминает: утверждение владельца о том, что кнопку нажал он, ещё не доказывает безопасность цели, ради которой её нажали.10

Поэтому мне не нравится удобная метафора, превращающая антифрод-специалиста в назойливого сторожа. Возможно, именно он последним стоит между человеком и потерей накоплений за всю жизнь. Настоящая проблема начинается, когда мы смешиваем три утверждения: «есть повод задать вопрос», «есть повод задержать решение» и «есть повод до дальнейшего уведомления лишить клиента всех вариантов». Первое может опираться на сильные данные, второе требует определённой процедуры, третье — более высокого обоснования и более прочных гарантий. Уважающая клиентов организация не прыгает от вероятности на экране к бессрочному практическому наказанию. При мошенничестве с психологической манипуляцией проверка должна быть разговором, способным заметить давление, а не набором автоматических вопросов, ответы на которые преступник легко продиктует жертве.

Вред распределяется неравномерно

История Эмили показывает: пожилые люди не составляют одну однозначно «высокорисковую» группу. Одни могут чаще сталкиваться с финансовой эксплуатацией, но и цена ошибочной блокировки для них может быть выше. Человеку без машины, со сложностями при работе с паролями или действующему через законного представителя порой нужны и дополнительная защита, и более доступный путь обслуживания. Правило, принимающее низкую цифровую активность за недостаток надёжности, превращает арифметическое равенство в сервисное неравенство. Тот, кто обычно не путешествует и не переводит деньги, становится особенно подозрительным в день, когда ему понадобилось оплатить единственное лечение. Отклонив платёж и потребовав личной явки, мы делаем исключительную нужду одновременно уликой против человека и причиной, по которой он не может оправдаться.

Неравный вред не означает, что у модели обязательно есть переменная «возраст» или «инвалидность». Различия возникают из нейтральных на вид деталей: устройства, способности быстро получить код, языка, часов работы поддержки, возможности добраться до отделения, наличия доверенного представителя. Равная доля ложных срабатываний в двух группах ещё не доказывает справедливость опыта, если одна восстанавливает счёт за пять минут, другая — за пять дней. Некоторые группы вообще исчезают из данных, потому что после неудачи уходят из сервиса. Поэтому время снятия ограничения, стоимость доступа к каналу обжалования и успешность решения случаев с особыми потребностями входят в проверку самой безопасности. Защита, отражающая нападающего, но не узнающая явившегося владельца права, остаётся незавершённой.

Тест цены блокировки

Поэтому я предлагаю опровержимый институциональный эксперимент — «тест цены блокировки». Это не действующий регуляторный стандарт и не проведённое исследование, а рамка, которую банк или надзорный орган может оценить и изменить. Тест начинается с репрезентативной выборки решений, а не только самых громких сигналов. Для каждой операции фиксируются оценка риска в момент решения, вид подозрения, фактическая мера, доступные альтернативы, время начала и окончания ограничения, способ разрешения и окончательный исход с известной степенью уверенности. Затем по раскрытой методике оцениваются потери, вероятно предотвращённые блокировкой, и одновременно вред от остановки законных операций, часы клиентов и сотрудников, прямые сборы и штрафы, различия в возможности восстановить услугу. Не всякое страдание следует насильно переводить в одну денежную сумму. Но нельзя оставлять его вовсе невидимым на панели решений.

Тесту нужны четыре вида эксперимента, которых нет на обычном графике. Первый — повтор решений на исторических журналах с учётом только сведений, доступных тогда, и явной записью неизвестного. Второй — безопасные интервенционные испытания или тщательно подобранные выборки: сравнивать сигнал с лёгкой дополнительной проверкой и сигнал с остановкой операции, наблюдая вред клиенту и риск разрешения. Третий — симуляция адаптивного противника, который переносит атаку с кражи данных входа на обман владельца либо меняет сумму и время перевода. Четвёртый — испытания для тех, у кого не срабатывает первый цифровой канал: законных представителей, людей с инвалидностью и пользователей без современного устройства. Нельзя объявлять тест успешным до описания выборок, способа отбора, прав клиента и побочных эффектов; нельзя подвергать реальные деньги риску без надлежащих ограничений и согласований.

Короткая панель такого теста собрала бы показатели, редко встречающиеся в одном отчёте: стоимость подтверждённого предотвращённого мошенничества; точность сигналов в верхней группе, направляемой на проверку; долю законных операций, потребовавших вмешательства; медианное время и время самой медленной группы до восстановления возможности платить; долю ограничений, снятых при первом надёжном контакте; долю дел, закрытых без ясного человеческого решения; разницу во времени восстановления между группами пользователей; объём мошенничества, прошедшего сквозь меры. Полезно считать операции, от которых клиент отказался до завершения проверки, но без дополнительного доказательства нельзя записывать их ни в предотвращённое мошенничество, ни в законные. Показатель — не число красных флажков, а сумма устранённого риска и сохранённых прав по определению, которое можно проверить.

Когда меняется архитектура банка

Эта логика способна изменить саму архитектуру банка. Вместо того чтобы один движок распространял «отказ» по десяткам каналов, каждое вмешательство получает единый журнал состояния: почему оно введено, сколько действует, какое доказательство требуется для пересмотра, кто вправе его снять и что клиенту разрешено во время проверки. Если владелец подтвердил личность надёжным каналом, результат должен дойти до всех связанных процессов, чтобы второй сотрудник не обещал провести перевод, который первый уже поместил в очередь ожидания. При изменении обстоятельств риска следует осмысленный пересмотр, а не автоматическое продление до бесконечности. Когда риск и правила позволяют, можно отделить остановку одной операции от паралича всего счёта. Это проверяемая конструкция, а не обещание сделать горячую линию человечнее.

Здесь может возникнуть технологическая отрасль — более узкая и честная, чем вывеска «ИИ предотвращает мошенничество». Ценность есть в системах индивидуальной оценки вреда, движках политики с градуированными мерами, инфраструктуре проверки решений при дрейфе паттернов, аутентификации, переносящей достоверный результат между банковскими каналами, и аудите, различающем предотвращённое преступление и предотвращённую законную активность. Тот, кто кладёт классификатор поверх старых данных и хвалится высокой полнотой, не считая цену сигнала, продаёт половину науки о решениях как целое решение. Нечестно называть систему «умной», если она останавливает перевод за пятьдесят микросекунд, а затем три дня выясняет, что владелец уже доказал своё право на него.

Такая отрасль не отменяет правовую подотчётность и не делает клиента окончательным судьёй риска собственной операции. Правила против отмывания денег или распоряжения органов могут требовать иных ограничений, чем задержка платежа из-за антифрод-сигнала; часть сведений нельзя раскрывать во время расследования. Права на обжалование и возмещение зависят от юрисдикции, вида счёта и услуги. Поэтому правило «снимайте всякую блокировку после звонка» не годится как общая политика. Годится более узкое и сильное требование: у каждого ограничения должны быть ответственный, конкретное основание, соразмерность, законный путь пересмотра там, где он допустим, и документированный эффект, доступный последующей проверке. Безопасность, не умеющая объяснить, где закончилась её власть, рискует продлевать эту власть ровно настолько, насколько не умеет объяснять.

Когда заканчивается власть остановки

Все эти истории, при разных причинах, показывают: банковское событие не заканчивается, когда модель выдаёт вероятность, сотрудник нажимает кнопку блокировки или приложение пишет «для вашей защиты». Оно заканчивается, когда мошенничество действительно предотвращено, законное действие разрешено либо клиент получил объяснение и рабочий путь пересмотра в допустимых пределах. Многие системы учатся на пропущенной мошеннической операции, некоторые — на ложном сигнале. Учреждение, желающее долгого доверия, должно учиться и на часе, потерянном между ними. Деньги на счёте — не теоретическое обещание собственности. Их практическая ценность в том, что владелец может воспользоваться ими, когда они нужны, если нет законной и соразмерной причины помешать.

Поэтому бабушка из заголовка яснее всех матриц классификации. Она не просит банк отказаться от осторожности и автоматически верить каждому, кто говорит: «Это мой счёт». Она просит лишь не превращать осторожность в финал истории. За каждым сигналом — человек: возможно, жертва; возможно, участник; возможно, законный владелец, чьё поведение сегодня вышло за среднее вчерашних данных. Каждому

варианту нужен свой путь. Труднее всего в борьбе с мошенничеством не научить машину говорить «стоп». Труднее построить учреждение, которое знает, когда власть остановки закончилась и как после понятной быстрой проверки сказать нужному человеку: «Вот ваши деньги».

Источники и литература

[1] Financial Ombudsman Service, A bank account is blocked after grandchildren use power of attorney — официальное исследование случая без видимой даты публикации; дата обращения: 9 ноября 2026 года.

[2] Financial Ombudsman Service, Power of attorney didn’t entitle Joanne to use her mum’s login — официальное исследование случая без видимой даты публикации; дата обращения: 9 ноября 2026 года.

[3] Financial Ombudsman Service, Final Decision DRN-5921701 — события 28–30 июня 2025 года; точная дата решения в доступном деле не установлена; дата обращения: 9 ноября 2026 года.

[4] US Consumer Financial Protection Bureau, Supervisory Highlights, Issue 34, §2.5.1 — июль 2024 года; надзорные наблюдения в целом относятся к 2023 году.

[5] UK Finance, Annual Fraud Report 2025, press release — 28 мая 2025 года, данные за 2024 год.

[6] European Banking Authority & European Central Bank, Joint EBA–ECB Report on Payment Fraud — 15 декабря 2025 года, данные за 2024 год.

[7] Dal Pozzolo, Boracchi, Caelen, Alippi & Bontempi, Credit Card Fraud Detection and Concept-Drift Adaptation with Delayed Supervised Information — конференция IEEE IJCNN 2015; оригинальная версия с сайта автора.

[8] Dal Pozzolo et al., Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy — онлайн-публикация 14 сентября 2017 года; IEEE TNNLS, август 2018 года, 29(8).

[9] Höppner, Baesens, Verbeke & Verdonck, Instance-dependent Cost-sensitive Learning for Detecting Transfer Fraud — ранняя публикация 2021 года; European Journal of Operational Research 297(1), 2022, с. 291–300.

[10] Financial Ombudsman Service, Evan’s bank blocked payments on his current account — официальное исследование случая без видимой даты публикации; дата обращения: 9 ноября 2026 года.