

مقالة رأي وتحليل

التاريخ التحريري: ٢٢ سبتمبر ٢٠٢٦

الجدّة التي اشتبه بها نظام مكافحة الاحتيال

حين أغلق الحذر باب الحساب

رتّبت أميلي أمورها قبل أن تحتاج إلى من يرتّبها لها. منحت حفيديها توكيلًا يسمح لهما بالتصرف في شؤونها إذا فقدت أهليتها الذهنية. ثم فتحت يومًا باب حسابها فلم يفتح: بطاقتها لا تعمل، والدخول الإلكتروني مغلق. لم تكن فاقدة الأهلية، وكانت لا تزال تستخدم الحساب بانتظام. لكن البنك سجل التوكيل وغيّر صلاحيات الوصول من غير أسئلة إضافية كان يمكن أن تكشف الحقيقة البسيطة التي غابت عن الإجراء: صاحبة المال موجودة، وتفهم، وتريد أن تتصرف في مالها. ألغت التوكيل وأرسلت ما يثبت ذلك؛ فعاد القيد القانوني سريعًا إلى موضعه، ولم يعد باب الحساب معه. استغرق استرداد البطاقة والوصول الإلكتروني أسابيع. ولأن حركتها محدودة، صارت تستقل سيارة أجرة إلى الفرع كي تسحب خمسين جنيهًا نقدًا في كل مرة. وانتهت الشكوى أمام جهة المظالم المالية البريطانية بإلزام البنك بمصاريف انتقالها وتعويض قدره 350 جنيهًا عن المشقة والتأخير.1

هذه حالة حقيقية لجدّة تضررت من نظام حماية الصلاحيات، وليست، على وجه الدقة، حالة أعلن فيها نموذج ذكاء اصطناعي أنها محتالة. لا ينبغي ادعاء ذلك. لكنها تصلح مدخلًا إلى سؤال أوسع: كيف يتحول إجراء وُضع لحماية المال إلى عائق يمنع صاحبه من الوصول إليه؟ وفي سجل آخر للجهة نفسها امرأة تدعى فيرا انتقلت إلى دار رعاية بعد إصابتها بالخرف، وكانت ابنتها جوان تدفع فواتيرها بتوكيل قانوني. حاولت جوان إجراء تحويل كبير، فاعترضه نظام كشف الاحتيال في البنك لأنه غير مألوف، ثم اقتنع الموظفون بأنه حقيقي. غير أن الاعتراض كشف أن الابنة تستخدم بيانات دخول أمها، خلافًا

لشروط البنك. كان إيقاف مشاركة بيانات الدخول مشروعًا في نظر جهة المظالم، لكن البنك لم يساعد الوكيلة على استخدام البديل المتاح من هاتفها. انتهى الأمر بمساعدة عملية وتعويض قدره 200 جنيه. هنا، هذه المرة، دخل نظام كشف الاحتيال صراحة في القصة، ولم تكن مشكلته الوحيدة دقة الاشتباه، بل ما حدث بعد زواله.2

في الثامن والعشرين من يونيو 2025 حاول عميل لبنك HSBC، حجبت جهة المظالم البريطانية اسمه واكتفت بالحرف M، أن يحوّل 400 جنيه إلى صديق من تطبيق البنك. علّق نظام مكافحة الاحتيال العملية وأرسل رسالة تطلب الاتصال. اتصل الرجل، ولم تنجح وسيلة التحقق من صوته. اتصل مرة ثانية ونجح التحقق؛ وأخبره موظف بأن التحويل سيُطلق، بينما كان الموظف الأول قد شرع بالفعل في حجب الحساب. لم يعرف الموظف الثاني ما يحدث في المسار الموازي. في اليوم التالي فشل العميل في الدخول إلى التطبيق، وطُلب منه الحضور شخصيًا. وفي الثلاثين من يونيو ترك نصف يوم عمله وذهب إلى الفرع، بعدما كان قد أرسل المال إلى صديقه بطريقة أخرى. لم تقل جهة المظالم إن مجرد الاشتباه كان خطأ، بل رأت أن إجراءات التحقق والحجب الأولي معقولة، وأن الخطأ الذي يستدعي التعويض هو إخباره بأن المال سيُرسل مع أن ذلك لم يعد ممكنًا. وأقرت تعويضًا قدره 200 جنيه.3

هذه التفاصيل البيروقراطية أصدق من حكاية سهلة عن بنك شرير وخوارزمية غبية. لم يُحجب المال لأن آلة «اتهمت» صاحبه قانونًا بالاحتيال، ولم تحكم جهة المظالم بأن كل خطوة كانت ظالمة. وقع الضرر في المسافة بين أنظمة صحيحة جزئيًا: محرك يلتقط الشذوذ، ووسيلة تحقق صوتي، وموظف يغيّر حالة الحساب، وآخر لا يرى التغيير، وتطبيق لا يفسر لصاحبه ما جرى. كان يمكن لكل مكوّن أن يجتاز اختباره المنفرد بدرجة ممتازة، وأن تبقى الرحلة كلها سيئة. هنا تكمن المفارقة: قد ينجح نظام كشف الاحتيال في رفع الراية، بينما تخفق المؤسسة في إنزالها بعد أن يُحسم الاشتباه. وإذا قيس النجاح عند لحظة الإنذار، فأين تُسجل الساعات التي يظل فيها صاحب الحساب واقفًا تحته؟

الأرقام الكبيرة والمعدل الصغير

المصارف محقة في أصل استعمال أنظمة الكشف. فالاحتيال ليس هامشًا يسيرًا يمكن تركه لموظف لطيف يتفرغ لكل معاملة. ذكر تقرير UK Finance المنشور في مايو 2025 أن المؤسسات البريطانية منعت، بحسب بيانات القطاع، احتيالًا غير مصرّح به بقيمة 1.45 مليار جنيه خلال 2024، بينما بلغت خسائر الاحتيال غير المصرّح به المبلغ عنها 722 مليون جنيه عبر 3.13 ملايين حالة مؤكدة. وخسر العملاء والمؤسسات كذلك 450.7 مليون جنيه في احتيال التحويلات التي يوافق صاحب الحساب على إرسالها تحت الخداع. هذه أرقام خطيرة، لكنها ليست اختبارًا مقارنًا يثبت أن كل عملية أُوقفت كانت تستحق الإيقاف، ولا تكشف كم تحويلًا مشروعًا تأخر، وكم شخصًا اضطر إلى إثبات براءته العملية من اشتباه آلي.5

ولأن الأرقام كبيرة يغري ذلك المؤسسات بمقياس واحد: «كم جريمة التقطنا؟». هنا يبدأ الانحراف الرياضي الهادئ. فلنفترض مليون معاملة، بينها ألف معاملة احتيالية بالفعل. أي إن الاحتيال يمثل عُشر الواحد في المئة من عدد المعاملات. ولنفترض، في تجربة حسابية لا تصف بنكًا معينًا، أن نموذجًا يلتقط تسعين في المئة من الاحتيال، لكنه يرفع إنذارًا خاطئًا على واحد في المئة من المعاملات السليمة. سيكشف النموذج 900 حالة احتيال، وهو إنجاز يبدو ساحقًا على شريحة عرض. لكنه سيعترض كذلك 9,990 معاملة مشروعة. سيصبح أمام موظفي التحقق 10,890 إنذارًا، لا يزيد الصحيح منها

على نحو 8.26 في المئة. مقابل كل إنذار احتيال صحيح هناك أكثر من أحد عشر إنذارًا لمعاملة سليمة. ليست النتيجة أن النموذج عديم القيمة؛ بل أن «التقاط تسعين في المئة من الشر» يخبرنا بأقل مما نظن عن الحياة اليومية التي سيمر بها الناس.7

هذا هو أثر معدل الأساس (Base Rate) في الظواهر النادرة. يسهل على المرء أن يقرأ حساسية الكشف (Recall) فيتوهم أنها احتمال صحة أي إنذار، مع أن الاحتمال الثاني هو دقة الإنذارات الإيجابية (Precision)، ويتوقف أيضًا على انتشار الاحتيال بين المعاملات. ويمكن للبنك أن يرفع الحساسية بتخفيض عتبة الإنذار، فيكتشف محاولات إضافية، لكنه قد يرسل آلافًا أخرى من العملاء الحقيقيين إلى طوابير المراجعة. وإذا رفع العتبة عاد بعض المحتالين إلى العبور. في العلوم الإحصائية هذه مفاضلة مألوفة بين الإيجابيات الكاذبة (False Positives) والسلبيات الكاذبة (False Negatives). وفي البنك لا تبقى المفاضلة على الورق: تتحول إلى فاتورة لم تُدفع، وعامل غاب عن دوامه، وممرضة لم تصلها أجرتها، ورجل يحاول إقناع هاتفه بأن صوته لا يزال صوته.

لكن علينا أن نمنع الحساب نفسه من الكذب. فالنسب التي وضعتها للمليون معاملة افتراضية محضة، وليست معدل احتيال عالميًا ولا قياسًا لمدى جودة HSBC. كما أن كلمة «إيجابية كاذبة» تحتاج تعريفًا دقيقًا: قد تكون المعاملة مشروعة بعد التحقيق، ومع ذلك كان إيقافها المؤقت معقولًا في ضوء ما كان معلومًا عند لحظة القرار. التقييم الصحيح لا يسأل فقط هل ظهر خطر في النهاية، بل هل كانت درجة الاشتباه، ومقدار التدخل، ومدة الانتظار، والبدائل المعروضة، متناسبة مع الخطر الذي أمكن معرفته آنذاك. لا يجوز استعمال المعرفة اللاحقة لإدانة كل احتياط سابق؛ ولا يجوز، في المقابل، استعمال ضرورة الاحتياط تبريرًا لكل تأخير لاحق.

ليس كل احتيال هو الاحتيال نفسه

يجري جزء من هذا الخلط بسبب كلمة «الاحتيال» نفسها. فهناك معاملة يجريها مهاجم سرق بيانات البطاقة أو سيطر على وسيلة التوثيق، وهناك تحويل يأمر به صاحب الحساب الحقيقي لأنه صُدّق قصة احتيالية. في الأولى قد يكون اختلاف الجهاز والموقع وطريقة الاستعمال علامة ذات قيمة. وفي الثانية قد يكون الهاتف صحيحًا، والبصمة صحيحة، وصاحب المال حاضرًا بوعيه الكامل؛ الخلل في القصة التي دفعته إلى إصدار الأمر. أشار التقرير المشترك للهيئة المصرفية الأوروبية والبنك المركزي الأوروبي في ديسمبر 2025 إلى أن المصادقة القوية ظلت فعالة ضد أنواع من الاحتيال صُممت لمكافحتها، وأن المحتالين صاروا يستدرجون أصحاب الحسابات إلى توثيق معاملات احتيالية بأنفسهم. وأورد التقرير 4.2 مليارات يورو من احتيال المدفوعات المبلّغ عنه في المنطقة الاقتصادية الأوروبية سنة 2024. هذا مبلغ من القيمة، لا نسبة من عدد المدفوعات، فلا يصح خلطه بالمثال الحسابي السابق.6

إذا قاس البنك خطر المعاملة باعتباره مسألة «هل يحمل الدافع هاتفه الأصلي؟» فقد يحسن الإجابة عن السؤال القديم فيما يتحرك الاحتيال إلى سؤال آخر: «لماذا يدفع؟ ولمن؟ وبناءً على أي رواية؟». وثّقت UK Finance أن محتالين يستدرجون الناس إلى تسليم رموز المرور لمرة واحدة، وأن الاحتيال في التحويلات المصرح بها ما زال مرتبطًا بقنوات تواصل خارج البنك. هذا لا يعني أن التحقق من الجهاز بلا جدوى، وإنما يعني أن خصمًا يتعلم سيحاول دفع الإنسان إلى تنفيذ الخطوات

الصحيحة نيابةً عنه. في لغة التعلم الآلي يحدث انجراف مفهومي (Concept Drift): تتغير العلاقة بين الأنماط التي تعلمها النموذج وبين الاحتيال الفعلي. وقد يتغير كذلك سلوك العملاء الأبرياء عند السفر أو التقاعد أو المرض أو الانتقال إلى بلد آخر. عندها يصبح الغريب من حيث الإحصاء عادياً من حيث الحياة.568

ما لا تتعلمه الخوارزمية من المنع

البحث العلمي في هذا المجال تجاوز منذ زمن فكرة مقارنة خوارزميات بحسب الدقة الإجمالية وحدها. في دراسة أصلية نشرها أندريا دال بوزولو وزملاؤه في مؤتمر IEEE عام 2015، وصف الباحثون واقع أنظمة الاحتيال التي ترى سيولًا من المعاملات، ولا تستطيع فرق التحقيق فحص إلا مجموعة صغيرة من الإنذارات الأعلى خطورة. والمعلومة المبكرة تأتي من محقق يتواصل مع العميل، بينما تصل علامات التأكيد المتأخرة بعد أيام عندما يبلغ العملاء عن عمليات لم يأذنوا بها. ليست العينتان متماثلتين: ما يراه المحقق اختاره النظام القديم أصلًا لأنه ظنه خطراً، أما بقية المعاملات فلا تخضع لنمط الاختيار نفسه. لذلك اختبر الفريق معالجة تعليقات المحققين وعلامات التأكيد المتأخرة بصورة منفصلة ثم جمع نتائجها، ووجد تحسناً في دقة التنبيهات ضمن بيئة الدراسة.7

ثم نشر الفريق دراسة لاحقة في دورية IEEE عام 2018 تناولت أكثر من 75 مليون معاملة بطاقة حقيقية خلال ثلاث سنوات، موضحًا أثر عدم توازن الفئات وانجراف الأنماط في تقييم النظام وتحديثه. لا نستطيع أخذ هذه البيانات وإعلان أن كل بنك معاصر يملك النسب نفسها، ولا أن النموذج الذي نجح في سوق وبطاقات وفترة زمنية سينجح بالدرجة نفسها في بلد آخر. لكن النتيجة المنهجية شديدة الأهمية: عينة تدريب نظيفة بعد الحدث ليست مرآة أمينة لقرار يُتخذ في ثوان تحت نقص المعلومات. والتفوق في اختبار تاريخي لا يحسم سلوك النظام حين يتعلم المحتالون منه، وحين يغيّر العملاء عاداتهم، وحين تتأخر حقيقة العمليات شهوراً عن إشارات الاشتباه.8

توجد مشكلة أعمق أسميها «عمى المعاملة الممنوعة». لو رفض النظام تحويلًا قبل إرساله، فلن يشاهد ما كان سيحدث لو سمح بمروره. هل كان سيصل إلى محتال ثم يختفي؟ أم إلى صاحب عقار ينتظر الإيجار؟ في الحالة الأولى يبدو المنع نجاحًا، وفي الثانية يظهر خسارة خدمة. لكن السجل قد لا يحمل الحقيقة المقابلة أصلًا، وقد تسجّل بعض الأنظمة العملية الممنوعة كحادثة احتيال «تم منعها» بسبب قاعدة الاشتباه ذاتها، إذا لم تكن هناك عملية تحقق مستقلة. إذا استُعمل هذا الوسم لاحقًا لتدريب نموذج جديد، فمن الممكن أن يتعلم النموذج تصديق أحكامه القديمة. هذه ليست تهمة موجهة إلى مؤسسة بعينها، بل مشكلة استدلال سببي: القرار غيّر ما يمكن ملاحظته، فلا تكفي البيانات الناتجة عنه لإثبات أن القرار كان مصيبًا.

وتزداد المشكلة حين يُتخذ إجراء مختلف بحسب الخطر. فالمعاملات العالية الدرجة تخضع لمراجعة بشرية مكثفة، والمنخفضة تمر بلا سؤال، والوسطى قد تُرسل إلى توثيق إضافي. عندئذ يصبح اختيار العينة نفسه نتيجة للنموذج، وينشأ تحيز اختيار (Selection Bias). إذا درّبت الخوارزمية التالية على الحالات التي وصل إليها المحققون فقط، فقد تبدو لها الحياة كلها محفوفة بالاحتيال. وإذا اعتبرت كل معاملة لم يُبلغ عنها احتيالًا بعد أسبوع معاملة سليمة، فقد تفوتها ضحايا يتأخر

اكتشافهم، أو من لا يعرفون كيف يعترضون. الحل ليس إلزام البشر بمراجعة كل شيء، بل إنشاء آليات قياس محدودة ومضبوطة، وعينات تحقق يمكن تقييمها بوضوح، وتسجيل درجات اليقين وزمن ظهور الحقيقة ومصدرها. المحقق هنا ليس زرًا تجميليًا اسمه «مراجعة بشرية»؛ إنه أداة لإنتاج معرفة أفضل مما تتيحه الدرجة وحدها.

من احتمال إلى قرار

ومن هنا يتضح لماذا لا تكفي مطالبة النموذج برفع الدقة. فالخوارزمية قد تعطي تقديرًا احتماليًا يحتاج أولًا إلى معايرة (Calibration)، بحيث لا تعني درجة 0.8 مجرد ترتيب متقدم على الدرجة 0.6، بل تتسق، قدر الإمكان وعلى عينات مناسبة، مع الاحتمال الفعلي للحالة. بعد ذلك يأتي قرار آخر لا تنتجه المعايرة وحدها: ماذا نفعل عند احتمال معين؟ إذا كان البنك أمام عملية قيمتها كبيرة إلى مستفيد حديث الظهور، فقد يكون من المعقول أن يطلب تحققًا إضافيًا حتى إن كان احتمال الاحتيال متواضعًا. أما إذا كانت المعاملة فاتورة دواء مستحقة وفشلها يسبب ضررًا فوريًا، فلا يكفي أن نقول إنها غير معتادة. ينبغي النظر إلى كلفة إيقافها وإمكان التثبت منها على نحو أقل إضرارًا.

في أبسط صيغة لعلم القرار، نقارن كلفة السماح المتوقعة، وهي احتمال الاحتيال مضروبًا في الضرر المترتب عليه، بكلفة المنع المتوقعة، وهي احتمال سلامة المعاملة مضروبًا في الضرر الذي يسببه منعها، مع إضافة كلفة التدخل وما يبقى من خطر بعده. والواقع أعقد: البنك قد يعوّض خسارة ولا يعوّض أخرى، ووقف المعاملة قد يحمي العميل من خداع لا يدركه بعد، وأحيانًا يتطلب القانون اتخاذ تدابير لا يجوز اختزالها إلى معادلة ربح. لكن هذا التعقيد حجة لتوسيع ما نحسبه، لا لاستبعاد تكلفة العميل من المعادلة. وقدمت بحوث متخصصة في التعلم الحساس للكلفة (Cost-Sensitive Learning) عتبات تختلف باختلاف تكلفة الخطأ في كل تحويل، بدل افتراض أن خطأ كل معاملة يساوي خطأ الأخرى.9

المبدأ الأهم هنا أن قابلية التراجع عن قرار الحماية (Reversibility) خاصية أمنية وليست مجرد لمسة لطيفة في تجربة المستخدم. قد يطلب البنك وقف تحويل لساعة كي يتصل بصاحبه على قناة موثوقة، وهذا احتياط قابل للحسم. لكن حين يتحول الوقف إلى تجميد حساب كامل، ثم إلى حجز وصول رقمي، ثم إلى رسالة هاتفية لا تصل إلى موظف، تكون المؤسسة قد نقلت المعاملة من منطقة المخاطرة المالية إلى منطقة مصادرة الوقت والقدرة على التصرف. وقد وثق مكتب الحماية المالية للمستهلك الأمريكي (CFPB) في تقرير رقابي صدر في يوليو 2024 حالات مؤسسات جمّدت حسابات بسبب نشاط مشتبه فيه، ولم تبلغ بعض العملاء، أو لم تخبرهم كيف يعيدون تفعيل الحساب، بل إن بعضها أسقط أو حجب معظم المكالمات الواردة من الأرقام المرتبطة بالحسابات المجمدة. أمضى بعض المستهلكين أسابيع أو أشهر من دون وصول إلى أموالهم؛ واعتبر الفاحصون بعض هذه الممارسات غير عادلة.4

المثير هنا أن الجهة التي تملك القدرة على حجب الرقم في نظام الهاتف ربما كانت تظن أنها تمنع محتالًا من استعمال قناة خدمة بديلة. لكنها حجبت، في الوقت نفسه، القناة التي يحتاجها الشخص الحقيقي كي ينفي الاشتباه. بتعبير آخر، تحولت أداة الإنقاذ إلى باب لا يُفتح إلا لمن لم يحتج إليها. وإذا كان العميل يستطيع معرفة أن حسابه مجمد، لكنه لا يستطيع الوصول إلى شخص يخبره كيف يفك التجميد، فقد صار النظام حلقة مغلقة: يُمنع الوصول بسبب اشتباه، ويُمنع الاعتراض بسبب المنع. لا يحتاج مثل هذا الخلل إلى ذكاء اصطناعي متقدم كي يحدث، لكنه يتضاعف أثرًا حين توزع الأنظمة الآلية القيود في أجزاء عدة من المؤسسة من دون سجل موحد يبيّن حالة القرار ومن المسؤول عن إنهائه.

هناك، مع ذلك، حجة قوية في الجانب الآخر لا يجوز التغاضي عنها. فقد يعترف العميل بأن المعاملة خرجت منه، ويصر على أنها سليمة، مع أنه واقع تحت ضغط محتال يملي عليه ما يقول. نشرت جهة المظالم البريطانية حالة لشخص يدعى إيفان كانت معاملاته الكبيرة تمر عبر أصدقاء لمساعدة طرف آخر، واعتقد البنك أن الظروف تشير إلى احتمال تعرضه للخداع أو الإكراه. قيد البنك بعض التحويلات، مع إبقاء سبل أخرى للوصول إلى النقد وسداد التزاماته، ولم تر جهة المظالم أن التصرف يستوجب تأييد الشكوى، لكنها شددت على أهمية المراجعة الدورية للقيود. هذه الحالة تذكير بأن شهادة صاحب الحساب عن صحة الضغط على زر الإرسال لا تحسم تلقائيًا سلامة الغرض الذي دفعه إليه.10

ولهذا لا أحب الاستعارة السهلة التي تجعل موظف مكافحة الاحتيال حارسًا فضوليًا يفتعل المتاعب. قد يكون ذلك الموظف آخر من يحول دون فقدان مدخرات عمر كامل. المشكل الحقيقي يبدأ عندما نخلط ثلاث دعاوى: «لدينا سبب لطرح سؤال»، و«لدينا سبب لتأخير قرار»، و«لدينا سبب لسلب العميل كل خياراته حتى إشعار آخر». الأولى قد تكون مستندة إلى بيانات قوية، والثانية تحتاج إجراءً محددًا، والثالثة تتطلب مبررًا أعلى وضمانات أقوى. لا تقفز مؤسسة تحترم عملاءها من احتمال على شاشة إلى عقوبة عملية مفتوحة. وفي الاحتيال القائم على التلاعب النفسي يجب أن يكون التحقق حوارًا قادرًا على اكتشاف الضغوط، لا أسئلة آلية يسهل على المجرم تلقين ضحيته إجاباتها.

الضرر لا يتوزع بالتساوي

وإذا عدنا إلى أميلي وجدنا أن كبار السن ليسوا فئة «عالية الخطر» على معنى واحد. ربما تزداد احتمالات استغلال بعضهم ماليًا، وربما ترتفع كلفة خطأ المنع عليهم أيضًا. من لا يملك سيارة أو لا يعرف كلمات المرور المعقدة أو يتعامل مع البنك بواسطة وكيل قانوني قد يحتاج حماية إضافية من جهة، ومسار خدمة أيسر من جهة أخرى. أما القاعدة التي تعامل «انخفاض الحركة الرقمية» بوصفه نقصًا في الموثوقية، فتستطيع أن تقلب المساواة الحسابية إلى انحياز خدمي. الإنسان الذي لا يسافر ولا يحول أموالًا عادةً قد يصبح محل اشتباه كبير حين يضطر إلى دفع مصروف علاج واحد. وإذا رفضنا هذه المعاملة ثم طالبناه بالحضور بنفسه إلى الفرع، فقد جعلنا حاجته الاستثنائية دليلًا ضده وسببًا لتعذّر تبرئتها.

والحديث عن الضرر غير المتكافئ لا يعني أن النموذج يملك بالضرورة متغيرًا اسمه «العمر» أو «الإعاقة». يمكن أن تنشأ الفروق من عناصر تبدو محايدة: الجهاز المستخدم، والقدرة على تلقي رمز بسرعة، واللغة، وساعات الاتصال، وإمكان الذهاب إلى الفرع، ووجود وكيل معتمد. لا تكفي مساواة معدلات الإيجابيات الكاذبة بين مجموعتين لإثبات عدالة التجربة إذا كانت إحدى المجموعتين تسترد حسابها في خمس دقائق، والأخرى في خمسة أيام. وبعض الفئات لا تظهر في البيانات أصلًا لأنها هجرت الخدمة بعد الإخفاق. لذلك يصبح قياس زمن رفع القيد، وكلفة الوصول إلى قناة اعتراض، والنجاح في حل الحالات ذات الاحتياجات الخاصة، جزءًا من اختبار الأمن نفسه. فالدفاع الذي يصدّ المهاجم ويعجز عن تمييز صاحب الحق بعد أن يحضر إليه ليس دفاعًا مكتملًا.

اختبار كلفة المنع

أقترح لذلك تجربة مؤسسية قابلة للتفنيد أسميها «اختبار كلفة المنع». ليس معيارًا تنظيميًا قائمًا ولا دراسة منفذة، بل إطار بحثي تستطيع مؤسسة مصرفية أو جهة إشرافية تقييمه ثم تعديله. يبدأ الاختبار بعينة ممثلة من القرارات، لا من الإنذارات العالية وحدها. لكل معاملة تُسجّل درجة الخطر عند القرار، ونوع الشبهة، والإجراء الفعلي، والبدائل المتاحة، وساعة بدء القيد وانتهائه، ووسيلة حسمه، ونتيجته النهائية بدرجة يقين معروفة. ثم تُحسب الخسائر التي يُرجح أن المنع حال دون وقوعها وفق منهج معلن، إلى جانب الضرر الذي تسبب به المنع في المعاملات المشروعة، وساعات عمل العملاء والموظفين، والرسوم والغرامات المباشرة، وفروق القدرة على استعادة الخدمة. لا ينبغي تحويل المعاناة كلها قسرًا إلى مبلغ مالي واحد، لكن لا يجوز أيضًا أن تظل بلا تمثيل في لوحة القرار.

ويحتاج الاختبار إلى أربعة أنواع من التجارب لا يقدمها الرسم البياني المعتاد. الأولى إعادة تشغيل قرارات على سجلات تاريخية مع مراعاة ما كان معلومًا وقتها، وتوثيق البيانات التي لم تكن معروفة. والثانية اختبارات تدخّل في بيئة آمنة أو على عينات مدروسة، بحيث نقارن إنذارًا يطلب توثيقًا خفيفًا بإنذار يحجز معاملة، مع مراقبة ضرر العميل ومخاطر السماح. والثالثة محاكاة خصم متكيّف يحاول نقل احتياله من سرقة بيانات الدخول إلى خداع صاحب الحساب أو تعديل قيمة الحوالة وتوقيتها. والرابعة اختبارات للأشخاص الذين لا تنجح معهم القناة الرقمية الأولى، بمن فيهم وكلاء قانونيون وأصحاب إعاقات ومستخدمون لا يملكون جهازًا حديثًا. لا يصلح الادعاء بنجاح «اختبار كلفة المنع» قبل تحديد العينات ومنهج اختيارها وحقوق العملاء والتأثيرات الجانبية، ولا ينبغي إجراء تجارب تعرض مالًا حقيقيًا للخطر من دون ضوابط وموافقات مناسبة.

لو أردنا لوحة قياس مختصرة لوجدنا فيها أرقامًا نادرًا ما يجمعها تقرير واحد: قيمة الاحتيال المؤكد الذي مُنع، ومعدل الإنذار الصحيح في أعلى مجموعة تُرسل للمراجعة، ونسبة العمليات المشروعة التي احتاجت تدخلًا، والزمن الوسيط وزمن الشريحة الأبطأ لاستعادة القدرة على الدفع، ونسبة القيود التي رُفعت عند أول اتصال موثوق، ونسبة الحالات التي أُغلقت من غير قرار بشري واضح، وفرق زمن التعافي بين فئات المستخدمين، وحجم الاحتيال الذي مر رغم الضوابط. ومن المفيد قياس المعاملات التي غادرها العملاء قبل استكمال التحقق، لكن لا يجوز اعتبارها احتيالًا ممنوعًا أو عملية سليمة بلا دليل إضافي. المؤشر ليس عدد الرايات الحمراء على الشاشة؛ بل مجموع الخطر الذي أُزيل والحقوق التي ظلت متاحة، تحت تعريف يمكن تدقيقه.

حين تتغير هندسة البنك

وقد يفضي هذا المنطق إلى تغيير هندسة البنك نفسها. بدل أن يخرج «الرفض» من محرك واحد إلى عشرات القنوات، يكون لكل تدخل سجل حالة موحد يوضح لماذا فُرض، ومدة صلاحيته، وما الدليل المطلوب لإعادة التقييم، ومَن يملك رفعه، وما الذي يظل مسموحًا للعميل أثناء المراجعة. إذا أثبت صاحب الحساب هويته عبر قناة موثوقة، ينبغي أن تنتقل النتيجة إلى كل المسارات المعنية من غير أن يظل موظف ثانٍ يعده بإرسال تحويل أعاده موظف أول إلى قائمة التعليق. وإذا تغيرت

ظروف الاحتيال أثناء الانتظار، تجري إعادة تقييم واعية لا تمديدًا آليًا إلى ما لا نهاية. ويستطيع البنك أن يفصل بين منع معاملة بعينها وبين شل الحساب كاملًا عندما تسمح المخاطر والقواعد بذلك. هذا تصميم قابل للتحقق، لا مجرد وعد بأن الخط الساخن سيصبح أكثر تعاطفًا.

وأتوقع أن تظهر هنا صناعة تقنية أضيق وأكثر أصالة من اللافتة الفضفاضة «ذكاء اصطناعي يمنع الاحتيال». قيمة حقيقية قد تُبنى في أنظمة تقدير الضرر الفردي، ومحركات سياسات تتخذ تدابير متدرجة، وبنية لاختبار القرارات تحت انجراف الأنماط، وأنظمة تحقق تعيد استخدام نتيجة موثوقة عبر قنوات البنك، ومنصات تدقيق تكشف الفرق بين منع جريمة وبين منع نشاط مشروع. أما من يضع نموذجًا تصنيفيًا فوق بيانات قديمة ثم يتفاخر بنسبة كشف مرتفعة من غير أن يحسب كلفة الإنذار، فهو يبيع نصف علم القرار على أنه قرار كامل. وليس من الإنصاف أن نسمي الحل «ذكيًا» إذا عرف كيف يوقف الحوالة في خمسين جزءًا من الألف من الثانية، ثم احتاج ثلاثة أيام ليعرف أن صاحبها قد أثبت حقه فيها.

هذه الصناعة لا تلغي حدود المساءلة القانونية ولا تجعل كل عميل حكمًا نهائيًا على مخاطر معاملاته. قد تفرض قواعد مكافحة غسل الأموال أو أوامر الجهات المختصة قيودًا مختلفة عن تأخير دفع ناشئ من مؤشر احتيال، وقد تكون بعض المعلومات غير قابلة للإفصاح بسبب التحقيقات. كذلك تتغير حقوق الاعتراض والتعويض باختلاف الولاية وطبيعة الحساب والخدمة. لذلك لا يصلح اقتراح «ارفعوا كل حجز بعد مكالمة» سياسة عامة. ما يصلح هو شرط أضيق وأقوى: كل قيد ينبغي أن تكون له جهة مسؤولة، وأساس محدد، ودرجة تناسب، ومسار مشروع للمراجعة عندما تسمح القواعد، وأثر موثّق يمكن فحصه بعد انتهاء الحالة. الأمن الذي لا يستطيع أن يشرح أين انتهت سلطته معرض لأن يمد سلطته بقدر عجزه عن الشرح.

متى تنتهي سلطة التوقف

هذه القصص، على اختلاف أسبابها، تكشف أن الحدث المصرفي لا ينتهي عندما ينتج النموذج احتمالًا، ولا عندما يضغط الموظف زر الحجب، ولا عندما تظهر عبارة «لحمايتك» على شاشة التطبيق. ينتهي حين يُمنع الاحتيال حقًا، أو يُسمح بالتصرف المشروع، أو يتلقى العميل تفسيرًا ومسارًا صحيحًا للمراجعة ضمن الحدود المتاحة. كثير من الأنظمة يتعلم من معاملة احتيالية عبرت، وبعضها يتعلم من إنذار كاذب. لكن المؤسسة التي تريد بناء ثقة طويلة الأجل ينبغي أن تتعلم أيضًا من الساعة التي ضاعت بين الاثنين. فالمال الموجود في الحساب ليس وعدًا نظريًا بالملكية؛ قيمته العملية أن يستطيع صاحبه استعماله عندما يحتاج إليه، ما لم يوجد سبب مشروع ومتناسب يمنعه.

لهذا تبدو الجدّة في العنوان أوضح من كل مصفوفات التصنيف. هي لا تطلب من البنك أن يتخلى عن الحذر، ولا أن يصدق تلقائيًا كل من يقول «أنا صاحب الحساب». تطلب فقط ألا يجعل الحذر خاتمة القصة. خلف كل علامة خطر شخص قد يكون ضحية، أو متورطًا، أو صاحب حق خرج سلوكه هذه المرة عن متوسط بيانات الأمس؛ ولكل احتمال مسار مختلف. ليس أصعب ما في هندسة مكافحة الاحتيال أن نعلّم الآلة قول «توقف». الأصعب أن نبني مؤسسة تعرف متى تنتهي سلطة التوقف، وكيف تقول للشخص الصحيح، بعد تحققٍ مفهوم وسريع: «تفضل، هذا مالك».

المصادر والمراجع

[1] Financial Ombudsman Service, A bank account is blocked after grandchildren use power of attorney — دراسة حالة رسمية دون تاريخ نشر ظاهر؛ اطلع عليها 9 نوفمبر 2026.

[2] Financial Ombudsman Service, Power of attorney didn’t entitle Joanne to use her mum’s login — دراسة حالة رسمية دون تاريخ نشر ظاهر؛ اطلاع 9 نوفمبر 2026.

[3] Financial Ombudsman Service, Final Decision DRN-5921701 — واقعة 28–30 يونيو 2025؛ لم يثبت في ملف القرار المفتوح تاريخ إصدار محدد؛ اطلاع 9 نوفمبر 2026.

[4] US Consumer Financial Protection Bureau, Supervisory Highlights, Issue 34, §2.5.1 — يوليو 2024؛ ملاحظات الفحص تعود عمومًا إلى 2023.

[5] UK Finance, Annual Fraud Report 2025, press release — 28 مايو 2025، بيانات 2024.

[6] European Banking Authority & European Central Bank, Joint EBA–ECB Report on Payment Fraud — 15 ديسمبر 2025، بيانات 2024.

[7] Dal Pozzolo, Boracchi, Caelen, Alippi & Bontempi, Credit Card Fraud Detection and Concept-Drift Adaptation with Delayed Supervised Information — مؤتمر IEEE IJCNN 2015؛ نسخة البحث الأصلية من موقع مؤلف.

[8] Dal Pozzolo et al., Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy — نشر إلكتروني 14 سبتمبر 2017؛ في IEEE TNNLS، أغسطس 2018، 29(8).

[9] Höppner, Baesens, Verbeke & Verdonck, Instance-dependent Cost-sensitive Learning for Detecting Transfer Fraud — نُشر مبكرًا 2021، 2022، European Journal of Operational Research 297(1)، ص291–300.

[10] Financial Ombudsman Service, Evan’s bank blocked payments on his current account — دراسة حالة رسمية دون تاريخ نشر ظاهر؛ اطلاع 9 نوفمبر 2026.