stripe

オンライン不正行為の現状

序章

このレポートでは、オンラインにおけるカード不正使用の現状を包括的に解説します。Stripe では、数百万社が Stripe 上で試みた数十億件におよぶ決済取引を 2 年間にわたって分析しました。また、Milltown Partners 社 (focaldata 社と提携) と共同で、世界各地 (オーストラリア、カナダ、フランス、ドイツ、日本、オランダ、シンガポール、イギリス、アメリカ) の 9 業種のビジネスリーダー 2,500 人以上を対象に調査を実施しました。

これらの調査結果と Stripe 独自の分析結果を組み合わせることで、過去 1 年間で最も顕著な不正使用の傾向が浮き彫りになりました。たとえば、2020 年には商品に関する不審請求の申請が増加しました。また、経常収益型のビジネスは、不正使用が財務に与える影響を深刻に捉えています。このレポートでは、移り変わる不正使用への対処方法や、明らかになったデータをもとにしたビジネスのヒントをご紹介します。レポートの最後には、不正使用の動向予測に基づく 4 つの包括的なベストプラクティスも示しています。

このレポートは次の 4 つのセクションに分かれています。

- 不正使用が増加した理由
- 地域および企業規模による不正使用の違い
- 不正使用がビジネスに与える影響
- 不正使用の動向予測

エグゼクティブサマリー

- グローバルビジネスリーダーの 64% が、パンデミックの発生以来、ビジネスにおける不正使用対策が難しくなっていると回答しました。その原因の一端は、不正使用の種類や全体的な件数が増加していることにあると考えられます。
- パンデミックの発生当初、商品に関する不審請求の申請が一時的に 156% 増加し、「商品が届かない」「商品に不満がある」などの申請コードが使用されていました。Stripe では、サプライチェーンの混乱によって売り手が注文への対応に数週間、あるいは数カ月もの期間を要したため、顧客がチャージバックを要求したと見ています。
- さらに、40% 以上の企業がカードテスティング攻撃の試みを受けていたことも判明しました。パンデミックの間には、数千におよぶ新しい E-コマースビジネスが誕生し、それが不正使用者にとっての新たな機会につながったと Stripe では考えています。
- 世界各地で不正使用が増加しており、なかでも中南米の企業は特に不正使用の攻撃を受け、その状況は現在も続いています。中南米のビジネスでの不正使用率は北米のビジネスに比べて 97%、アジア太平洋地域のビジネスよりも 222% 高いことが確認されました。これには、現地で運用されている決済インフラなど、地域固有のさまざまな要因が考えられます。
- 不正使用への対処に最も苦労しているのは、経常収益型の企業、特に B2C 企業です。B2C サブスクリプションビジネスの 75% 以上が、昨年は、手作業による審査の負担が増大した、不正使用への対処により多くのリソースを割かなければならなかった、などと回答しています。これらの企業の消費者向けビジネスは高いブランド力を持っているため、その商品は容易に転売できます。結果として、不正使用者の標的にされやすくなります。
- 不正使用によるビジネスへの影響は、財務上の損失を上回ります。Stripe 分析によると、ビジネスがより多くの不正使用を防ごうとすればするほど、正当な支払いもブロックしてしまう可能性が高まり、決済コンバージョン率が低下します。このような誤検出を減らすために、疑わしい取引を手動で審査することもできますが、それによって追加のオーバーヘッドが発生します。
- Stripe では、事業者が次の 4 つの方法でこれらの傾向に適応することになると予測しています。1) 3D セキュアなどによる認証を有効活用する。2) 豊富なデータソースに基づいて、より迅速で的確な判断を下す。3) カード発行会社とビジネスがより緊密に連携し、不審請求の申請を効率化し、誤った支払い拒否を減らす。4) 顧客が好む支払い方法の移り変わりにともなって変化する不正使用の状況に対応できるようにする。

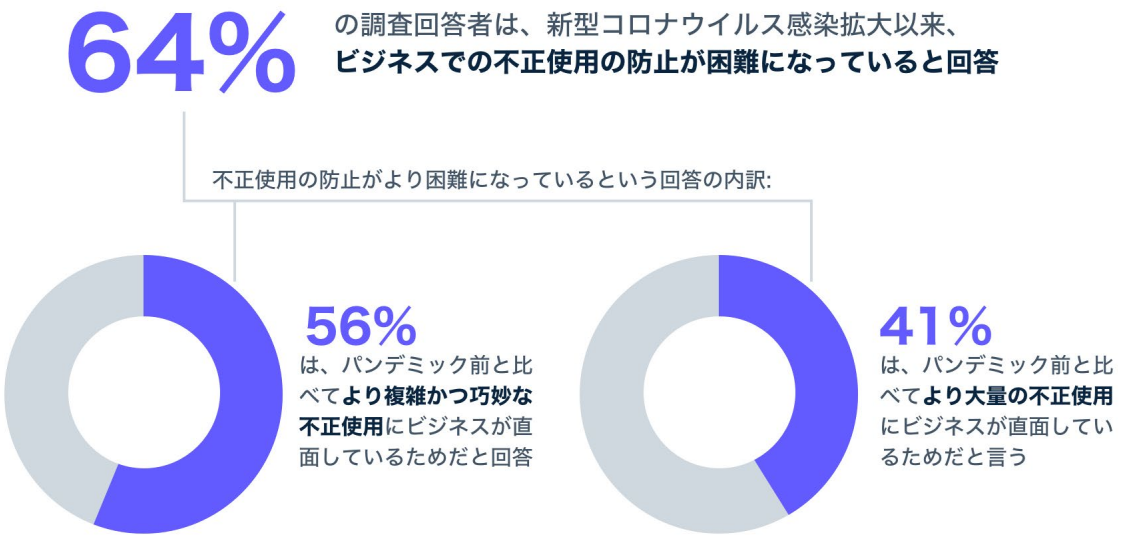
不正使用が増加した理由

新型コロナウイルスは、E-コマースに歴史的な成長をもたらしました。Stripe を導入している企業が 2021 年に処理した決済は 6,400 億ドルを超え、前年度から 60% 増加しました。これらの決済は、急成長中のビジネスグループによるものです。昨年は、毎日 1,400 社もの新しい企業が Stripe に加わりました。この歴史的な成長、なかでも新規ビジネスの増加は、不正使用者により多くの機会を与えることになりました。

新規ビジネスの多くは、初めてビジネスを行うため、不正使用に対処するためのツールやリソースを十分に準備できておらず、また不正使用を防止する戦略を立てることよりも、ビジネスを立ち上げて利益を得ることに重点を置いていました。しかし、これらの課題は新規ビジネスだけのものではありません。既存のビジネスでもパンデミック前と比較して、不正使用のタイプが複雑化したり、不正使用の件数が増大したりしたことにより、不正使用を防止することが困難になっています。

一方で、不正使用者の手口はますます巧妙化しています。彼らは、ビジネスを攻撃する新しい方法を見つけ、しばしばグループを組織し、他の不正使用者とつながって、「ベストプラクティス」を共有します。

> “ オンラインストアでの買い物客が増えるにつれて、不正使用による決済額が増加しました。すべての取引を手作業で審査するのは難しく、リソースも十分ではなかったため、一部のみを調査しました。
>
> - シンガポールの E-コマース企業の不正対策専門家



Stripe では、商品に関する不審請求の申請とカードテスティング攻撃の増加について具体的に調べました。

商品に関する不審請求の申請が 2019 年から 2020 年で倍増

Stripe 分析によると、2020 年 3 月から 5 月にかけて、不正使用関連以外の理由コード (「商品が届かない」「商品に不満がある」など) による申請が発生した決済取引は、2019 年の 2 倍以上にのぼりました。Stripe では、サプライチェーンの混乱によって売り手が注文への対応に数週間、あるいは数カ月もの期間を要したため、顧客がより多くのチャージバックを要求したと見ています。

一見すると商品に関する不審請求の申請率が最も低いのは中南米ですが、その原因はカード発行会社の行動にあると思われます。メキシコでは、世界合計の 7 倍もの不審請求の申請が、理由コードを付けずに報告されていると考えられます。ブラジルでは、不審請求の申請が不正使用として報告される確率が 50% 高くなっています。

商品に関する不審請求の申請を防止するためのベストプラクティス

- ☐ 明快で、透明性が確立されており、妥当な返品ポリシーを設定します。たとえば、返品期間の開始を商品の出荷時ではなく受領時にします。
- ☐ クレジットカードの明細書表記に、直接自社の社名を挿入します。
- ☐ 正式な不審請求の申請プロセスを策定します。
- ☐ 支払い処理の前に、顧客に通知します。サブスクリプションビジネスの場合は、顧客が次回の支払いについて少なくとも 1 回は通知を受け取るようにします。
- ☐ E-コマースビジネスの場合は、注文品の配送時に顧客のサインを求めます。

40% 以上のビジネスがカードテスティング攻撃の試みの標的に

カードテスティングは、盗難カードの情報が有効で買い物に使用できるかどうかを確かめるために行われます。不正使用者は盗難クレジットカードの情報を購入し、それらのカードを使って認証や購入処理を行い、どのカードが現在も有効であるかを判断します。

パンデミックの発生から 1 年間で、カードテスティング攻撃の試みを受けたビジネスの割合は 40% 急増しました。この傾向は新規と既存のどちらのビジネスでも確認されました。ただし、新規参入 (Stripe への登録後 90 日以内) のビジネスは、カードテスティングされた企業のなかで通常より大きな割合を占めています。

カードテスティング攻撃は、さまざまな形でビジネスに悪影響を与えます。カードテスティング攻撃が引き起こす大量の取引は、支払い処理のコストやダウンタイムのリスクを増大させます (ビジネスがトラフィックの増加に対処できなければ、その Web サイトは機能停止に陥ります)。さらに、カードテスティング攻撃が成功すると、世界の金融エコシステムが損害を被ります。ビジネスでは盗難カードによる支払いを処理する可能性が高まり、その結果、不審請求の申請が増加します。金融エコシステムへのリスクを理由に、カードテスティング攻撃を許したことに対して事業者がカード発行会社やカードネットワークからペナルティを科される場合もあります。

2021 年 11 月から実施された別の **Stripe 分析**では、カードテスティング攻撃によって募金事業が非常に大きな影響を受け、カードテスティング攻撃全体の 11% を占めることがわかりました。なぜでしょうか？多くの募金活動では、寄贈者 (この場合は不正使用者) が $1.00 や $5.00 といった少額を寄付することができます。少額であれば、明細書を見たカード保有者本人に気づかれにくくなります。さらに、募金事業の多くは不正対策チームが小規模で、取引を阻止するためのリソースが不足しています。募金事業 (およびカードテスティングされたビジネス) は金銭的損失を被るだけでなく、カードテスティング攻撃を許したことで銀行からペナルティを科されます。

カードテスティング攻撃を防止するためのベストプラクティス

- ☐ ペイメントプロバイダーの組み込みを最適化します。カードテスティング攻撃を緩和するために、多数のペイメントプロバイダーがさまざまな制御を実施しますが、成功するかどうかは、連携の質やプロバイダーに送信するシグナルに左右されます。一般的に、連携によって提供されるデータが多いほど、カードテスティングを防止できる確率は高くなります。
- ☐ API キーを安全に保管します。秘密の API キーを使用すると、支払いの作成や返金処理などの API コールをアカウントに代わって作成できます。秘密の API キーを他のパスワードと同じように取り扱い、それを必要とするユーザーのみにアクセスを許可します。
- ☐ 決済フローで CAPTCHA を有効にし、正当な顧客とカードテスティングボットを区別します。
- ☐ レート制限を設定し、受信トラフィックと送信トラフィックの量を制御します。たとえば、カードテスティング攻撃者が新規顧客にカードを関連付けて、そのカードの有効性を確認している場合は、1 日に 1 つの IP アドレスから受け入れる新規顧客数を制限します。
- ☐ 顧客が支払いを行う際にアカウントへのログインを要求することを検討します。

地域や国、企業規模による不正使用の違い

不正使用対策の重要性は世界共通です。Stripe が調査したビジネスリーダーの 90% は、E-コマースでの不正使用を防止することが自社のビジネスにとって重要であると回答しました。しかし、不正使用の方法は業種や企業の所在地によって微妙に違いがあり、複雑な様相を呈しています。

地域および国別の不正使用

Stripe の決済額データの大半は、北米でのビジネスを対象としています。そのため、このセクションの分析では、北米を他地域のベースラインとして使用しています。

すべてのオンラインビジネスは不正使用に対処する必要があります。しかし Stripe 分析によると、中南米のビジネスでの不正使用率が著しく増加していました。

Stripe のデータによれば、調査期間中に中南米のカード不正使用率が世界最高を記録しました。これは北米と比較して97%、アジア太平洋地域と比較すると 222% 高いものでした。地域的な決済インフラを運用している、あるいはクレジットカードの利用頻度が低いことから、カード会社で使用される不正使用対策モデル

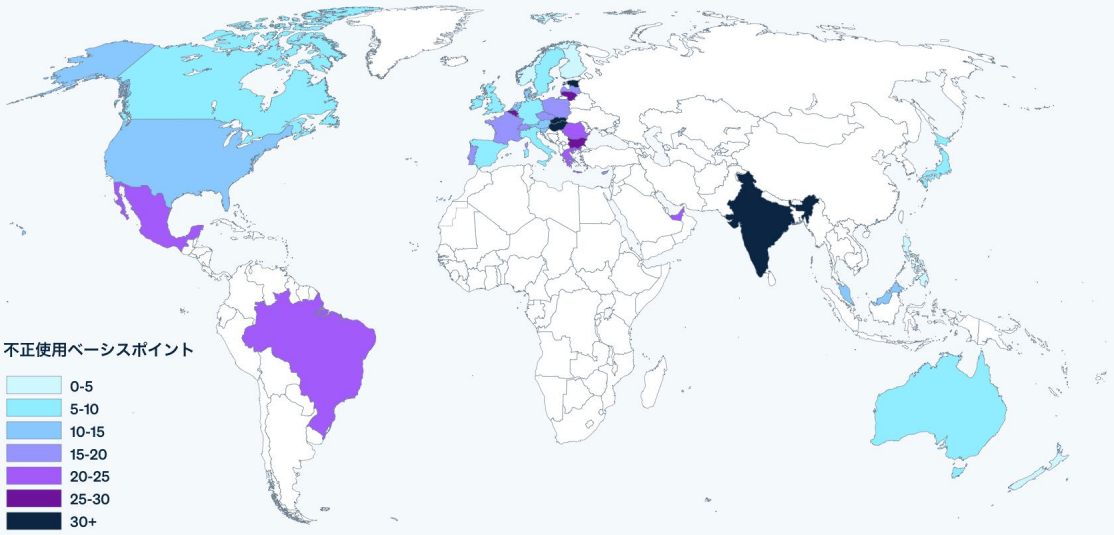
が他の地域に比べて不十分であると考えられます。また、不審請求の申請プロセスの規則はカード保有者に非常に脆弱となる原因になっています。こうした地理的な要因に加えて、市場ではますますオンライン化が進んでおり (Stripe を例にとってみても、Stripe を導入して中南米で事業を開始した新規企業は 2021 年に **518%** 増加しました)、不正使用者にさらに多くの攻撃機会を与えています。

ヨーロッパ、中東、アフリカでのビジネスは、北米に比べると不正使用率が非常に低く、これは決済フローで 2 段階認証を使用することを義務付けた、**強力な顧客認証 (SCA)** の効果を反映したものと思われます。

国によっても大きな差が見られました。たとえば、フランスの不正使用率はドイツのほぼ 2 倍、シンガポールではアジア太平洋地域全体の半分でした。このように国によって不正使用率にばらつきがあるため、グローバルビジネスの不正使用対策は一層難しくなっています。つまり、不正使用対策において、すべてに対応できる万能のアプローチは存在しないということです。

Stripe Radar による国レベルの不正使用率

Rader は機械学習を用い、あらゆる業種でのオンライン不正使用を検出・ブロックします。



推奨事項

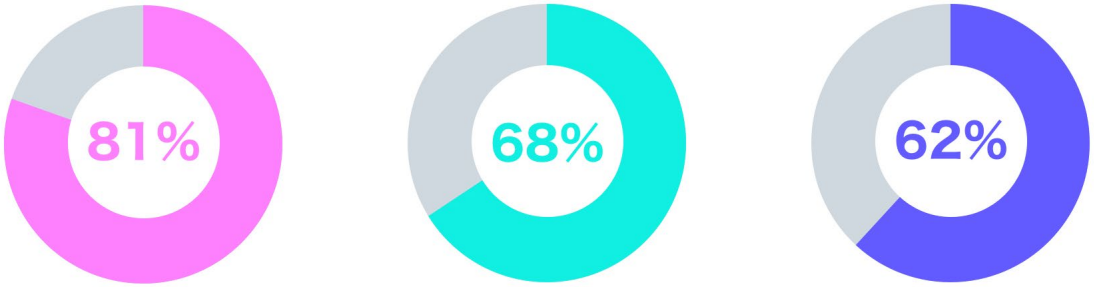
十分なキャパシティがある場合は、顧客の行動、市場動向、事業を行う各国の規制を分析し、自社に仕掛けられる可能性が最も高い不正使用攻撃とそのベクトルをよく理解しておくことをお勧めします。しかし、ビジネスの規模が拡大すると、業務が急速に複雑化して管理しきれなくなる場合があります。そこで、高度で自動化された不正使用対策ツールの活用が重要になってきます。

企業規模およびビジネスモデル別の不正使用

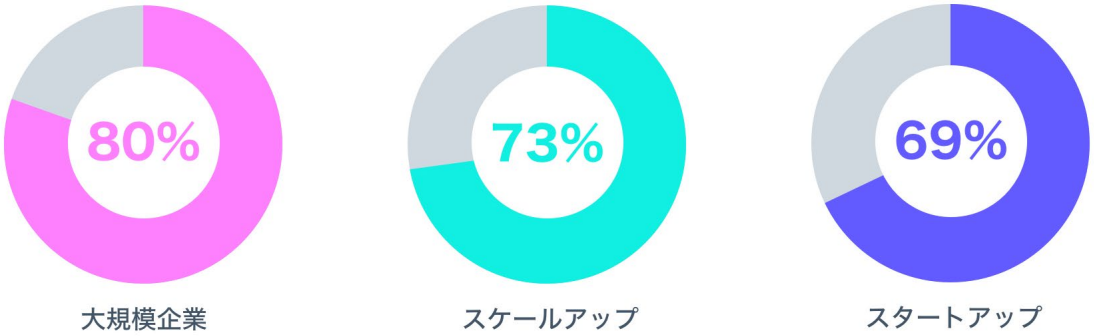
ビジネスリーダーたちは、企業の規模やビジネスモデルによって不正使用のリスクが異なることを理解しています。たとえば Stripe の調査によると、規模の拡大に伴って不正使用防止の重要性が増し、当然、大企業は中小企業に比べて、不正使用防止戦略に投じるリソースをより多く所有しています。しかし、不正使用を防止するのはリソースだけではありません。私たちの調査では、大規模な不正対策チームを擁するビジネスリーダーの方が、不正使用対策で運用上の問題に直面する確率が高く、不正使用による損失も高額に上っています。

このような傾向を、小規模ビジネスはチャンスと捉えることもできます。成長過程にあるビジネスは、規模が小さい今のうちに不正使用に対する綿密な戦略を策定しておけば、問題が起こったときに素早く対応できるからです。ただし、不正使用対策に時間やリソースを割くとビジネスの成長が滞る場合があるため、小規模なビジネスでは慎重に妥協点を見極める必要があります。

E-コマースでの不正使用を非常に重大なものと捉える傾向が強いのは、より規模の大きい企業のリーダーである。



昨年よりも今年は不正防止により多くのリソースを割くようになると予想する傾向が強いのは、より規模の大きいビジネスのリーダーである。



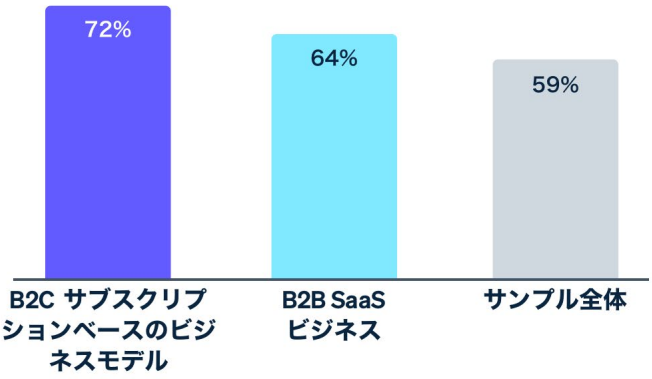
大規模企業: 年間収益が $6,000 万超。
スケールアップ: 年間収益が $200 万〜 $6,000 万。
スタートアップ: 年間収益が $200 万未満。

私たちは企業を次のように分類し、ビジネスモデルに基づく結果分析も行いました。

- SaaS (サービスとしてのソフトウェア)
- B2C サブスクリプション
- マーケットプレイスとプラットフォーム
- E-コマース

分析の結果、不正使用の財務的影響を最も懸念しているのは、経常利益型のビジネスであることがわかりました。調査対象の他のビジネスモデルと比べると、経常利益型ビジネスの不正対策担当者は、不正使用による金銭的損失をより深刻に心配しています。また、2021 年には不正使用による損失の収益に占める割合がパンデミック前よりも増加すると考える傾向がありました。このような懸念は、ビジネスモデルに起因するものかもしれません。これらのビジネスでは一定のスケジュールに沿って (毎月、四半期ごと、など) 収益を上げており、過去 1 年間に不正使用率の増加を経験したことから、自社のビジネスが成長する限りその傾向が続くと考えているようです。

経常収益ビジネスでは、不正使用による損失額 (2022 年) が前年よりも増えるのではないかと懸念する傾向が強い。



特に B2C サブスクリプションビジネスは、不正使用による運用上の負担に苦しんでいます。これらの企業からは、「2021 年に手作業の審査件数が増加した」「不正使用対策に振り向けるリソースを増やした」「不正使用対策のために投資や拡張計画を延期せざるを得なかった」などの回答が寄せられました。

私たちは B2C ビジネスでの不正使用が増加した理由を、これらのビジネスには家庭用ブランドが多いため、盗難にあった商品やサービスを不正使用者が転売 (たとえば盗難クレジットカードでデジタルサブスクリプションを購入し、それをより低価格で販売) しやすいからだと考えています。

不正使用がビジネスに与える影響

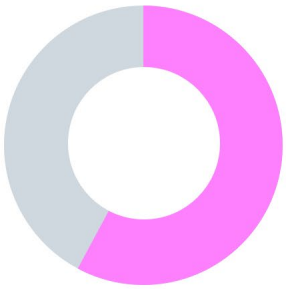
不正使用は高額のコストを伴います。実際、調査回答者の 59% が、今年は昨年より多くの収益が不正使用によって失われると予測しています。

ビジネスは不正使用に伴う不審請求の申請と、不正防止対策の両方によって損失を被ります。たとえば、不審請求の申請が認められると、元の取引額を超える金額を支払わなければなりません。多くの場合、カードが不正使用されると不審請求が申請され、チャージバック手数料 (カード会社がカード支払いを差し戻す際の費用) と高額のネットワーク手数料が発生します。

しかし、損失はそれだけに留まりません。私たちの調査で、不正使用によるビジネスへの影響は、単なる財務的損失を上回ることがわかりました。多くの企業は不正対策チームを拡充したり、製品やエンジニアリングのリソースを余分な作業や操作への対処に振り向けたりするなど、中核となる製品から貴重なリソースを移動させています。

不正使用によるビジネスへの影響は、財務上の損失に留まらない。

72%
のグローバルビジネスリーダーが、**生産やエンジニアリングのリソースを不正使用対策に充てざるを得ない**と回答



58%
のグローバルビジネスリーダーが、**不正使用により拡張計画や投資を延期せざるを得ない**と回答

決済コンバージョン率の低下

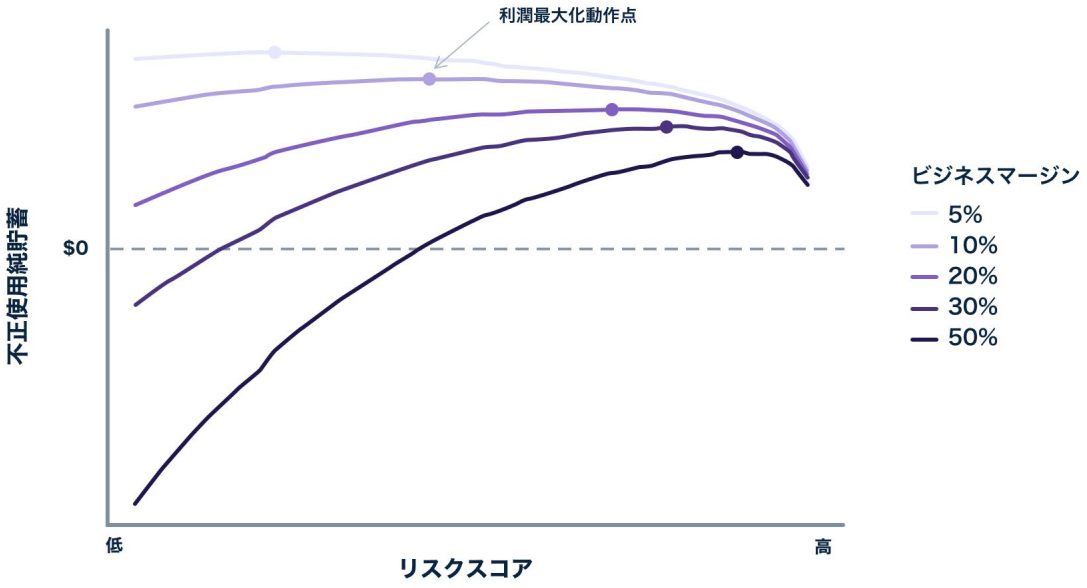
Stripe 分析では、ビジネスがより多くの不正使用を防ごうとすればするほど、正当な支払いもブロックしてしまう可能性が高まることがわかりました。

誤検出、すなわち誤った支払い拒否とは、正当な顧客が買い物をしようとしてもそれを阻止される状態です。誤った支払い拒否は、総利益と評判の両面で企業に打撃を与えます。事実、**顧客の 33%** は、誤って支払いを拒否された企業でもう一度買い物をする気にはならないと回答しています。

> “ たった 1 回の不正使用であっても、深刻なトラブルを引き起こし、追加的なセキュリティ審査によって正当な買い手を逃してしまう可能性があります。
>
> - カナダの SaaS 企業の不正対策担当者

不審請求の申請を防止することと、ブロックされる正当な顧客の数を減らすことは、トレードオフの関係にあります。阻止する不正使用の数を増やそうとすると、ブロックされる正当な顧客も増加します。一方、誤ってブロックされる正当な顧客の数を減らそうとすると、多くの場合、不正使用を見落とす可能性が高まります。トレードオフの状態は、使用する不正使用対策ソリューションによっても異なります。利用している不正使用対策ソリューションが静的で、改善のために継続的にリソースを投入していない場合は、常にこの状態に対処しなければなりません。一方、不正使用のベクトルに基づいてソリューションのモデルが絶えず順応し変化していれば、トレードオフの問題は緩和されます。

不審請求申請の回避と、正当な支払いのブロックとのトレードオフを考慮して、支払いをブロックするしきい値を選択すると、利益を最大化することができます。回避できる不正使用のコストと、ブロックされる正当な利益の差が最も大きいとき、利益は最大になります。



リスクスコアは、Radar を使用して取引をブロックするしきい値です (デフォルト設定では、リスクスコアが 75 を超えると取引がブロックされます)。

不正使用純貯蓄は、回避できる不正使用のコストの総額から、ブロックされる正当な利益を差し引いた値です。

利潤最大化動作点は、不正な取引のブロックと正当な取引のブロックのバランスが最適化され、不正使用純貯蓄が最大になるポイントです。

このグラフの見方: x 軸上のリスクしきい値が増加すると、取引が不正使用である可能性が高くなります。リスクしきい値が高いほど、ブロックする取引が少なくなります。ブロックする取引を増やすと、不正使用純貯蓄は増加します。ただし、正当な取引をブロックする確率も高まります。

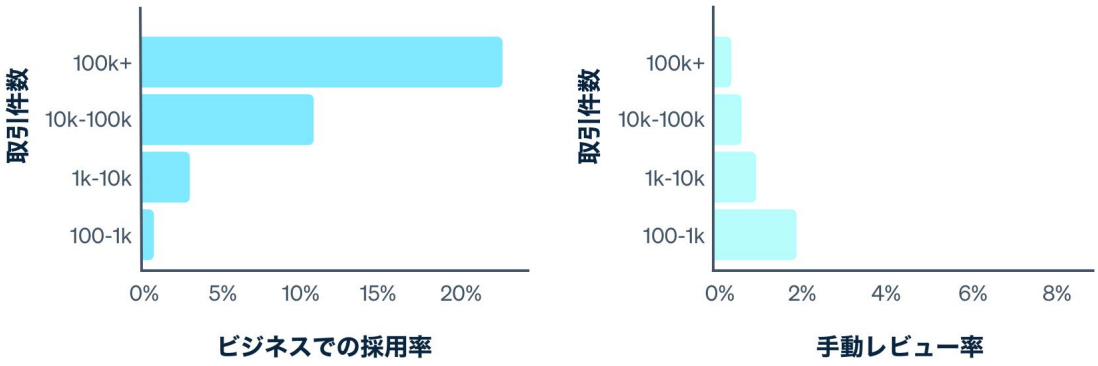
不正使用の防止と正当な取引のブロックとのトレードオフは、取引の利幅によって異なります。たとえば、グラフの紺色の線で示した高利幅 (50%) で取引を行うビジネスでは、個々の正当な取引の価値が (低利幅のビジネスなどと比較して) 非常に高いため、より多くの取引が許可され、リスクしきい値が高くなります。

ビジネスのマージン、グロースプロフィール、およびその他の要因に基づいて、このトレードオフに対処する必要があります。マージンの小さいビジネス、たとえば、食品のオンライン販売であれば、不正使用取引のコストを、何百件もの商品取引によって埋め合わせることが必要になる可能性があり、個々の検出漏れは非常にコストの高いものになります。このプロフィールを持つビジネスでは、潜在的な不正使用を防ごうとした場合に、幅広い対象に目を向ける方向に傾くことが考えられます。一方、マージンの大きいビジネス、仮に SaaS ビジネスであれば、逆のことが言えます。正当な顧客が 1 社ブロックされることによる収入減は、不正使用増加のコストを上回る可能性があります。また、どうやって不正使用率をある程度まで最適化するかは、ビジネス側で選択できることにも注目することが重要です。不正使用が一定のレベルに達すれば、カードネットワーク側では手数料や罰金を課すことになるでしょう。

作業にかかる余分な時間

誤検出を減らすためには、注意が促された支払いを手動でレビューして、本当に不正使用なのかどうかを確認するという手もあります。これは非常に多くの人手を要することです。取引の詳細や顧客履歴など、さまざまな要因に基づいてリスクを評価する不正使用分析チームが必要になります。

> 対処のためにリソースを振り向けなければならないのは不本意ですが、そうしなければ手に負えなくなると感じています。
>
> - オーストラリアの SaaS 企業で働く、不正使用に関する専門家



昨年の取引数別に見た、手動レビューを利用している Stripe ビジネスの比率 (ビジネスでの採用率) と、手動でレビューされた取引の平均比率 (手動レビュー率) - 記載されている数字はバケットの上限

大企業ほど手動レビューを取り入れる傾向が強いものの、規模が大きくなればなるほど、レビュー対象とする取引件数は少ないという結果になっています。たとえば、昨年 10 万件以上の取引件数があったビジネスの 20% 以上は手動レビューを利用していますが、レビュー対象となったのは合計取引数の 1% 未満です。大規模ビジネスでは、取引を手動でレビューするためのリソースを擁していますが、より危険度の高い取引用としてそれらを確保しています。

作業にかかる余分な時間を削減するための推奨事項

- ☐ 専任の不正対策チームがない小規模ビジネスの場合、チャージバック保証ソリューション (チャージバックコストの負担をサードパーティーが保証するソリューション) が特に役立ちます。
- ☐ 中規模〜大規模 E-コマースビジネスの場合、追加のエンジニアリングリソースを必要とせずに不正使用対策を大規模に展開するためには、機械学習ソリューションが役立ちます。
- ☐ 大企業の場合、大抵、手頃なポイントソリューション (CAPTCHA やカードのスキャンをサポートする特定のツールなど) を、不正使用対策ソフトウェアと連携させて、あるいは独自の不正使用の予測モデルへの入力として利用しています。

不正使用の動向予測

不正使用は徐々に進化しており、2021 年も例外ではありませんでした。事実、昨年の不正使用者の手口はさらに一層巧妙になり、新しい方法でオンラインビジネスを標的としました。このレポートでは数多くの課題を取り上げていますが、これは、皆さんのビジネスにとってどのような意味を持つでしょうか。現在の不正使用を取り巻く状況には、以下の 4 つの道筋で適応すべきだと Stripe は確信しています。

1. 3DS などの追加認証がより大きな役割を果たすようになる

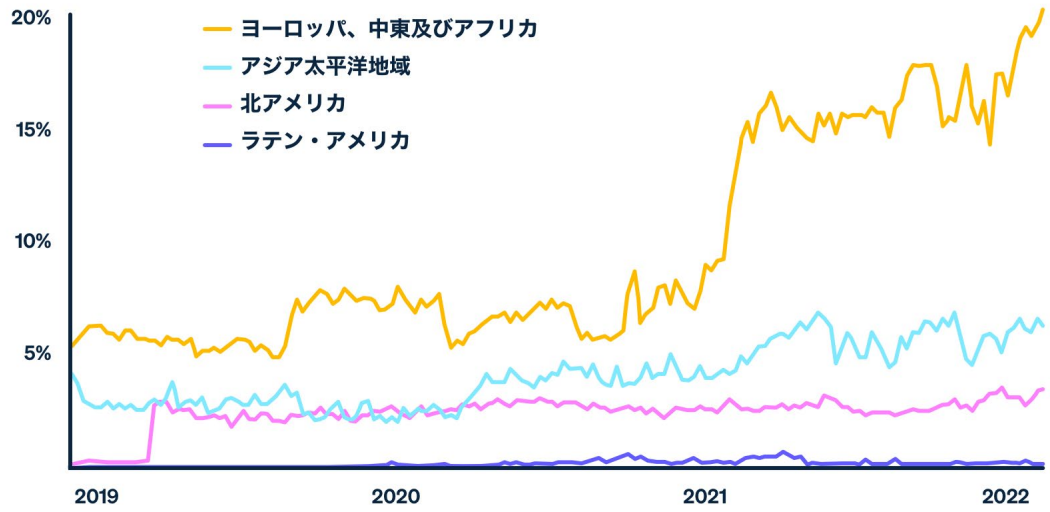
疑わしい取引であると考えられる場合に、顧客に「チャレンジ」を発行する (テキスト経由で送信されるワンタイムコードの入力を求めるなど) ことで、より確信を持って取引をブロック、あるいは許可できるようになります。

追加認証には、次のようなさまざまな形態があります。

- 支払いの際に 2 段階認証を行うように顧客に要求する **3DS**。これは、ヨーロッパの**強力な顧客認証** (SCA) 要件を満たすために使用される主要なクレジットカード認証方式であり、ビジネスが SCA に**免除**をリクエストするための重要なメカニズムです。
- 政府発行の ID をスキャンして本人であることを実証するよう顧客に求めるなどの、**本人確認**。
- 取引時点で物理カードを顧客が所有していることを確認するためのカードスキャン。
- ゆがんだイメージの中の一連の数字や文字を書き写すといった、簡単なパズルを解くよう、Web サイトへの訪問者に要求する **CAPTCHA ツール**。

追加認証はすでに普及しています。たとえば、3DS のアクティビティについて、2021 年における Stripe 上での取引を分析したところ、全体的に 3DS の採用が増えており、北米以外での採用が最も好調に推移していることがわかりました。予想どおり、3DS の採用が最も増えているのはヨーロッパのビジネスでした (これは、昨年、ヨーロッパの対象国のほぼすべてで SCA 要件が完全に施行された結果です)。SCA のような規制を取り入れる動きはヨーロッパ以外でも高まっており、インドで最も急速に拡大しています。

地域別に見た、支払いに関する 3DS 対応範囲の時間的推移



実験により、3DS を呼び出すしきい値を下げると、不正使用に関する不審請求の申請率が 74% 減少することがわかりました。加えて、即座に支払いをブロックする場合と比べて、3DS を利用することで、大多数の決済が成功します (全リスクレベルで 67%、比較的高いリスクレベルでは 5%)。ただし、3DS のパフォーマンスはカード発行会社によって異なります。

今後は、追加認証の利用は増えると予想しています。追加認証が適用される取引量が増え、とりわけ支払いプロセスの負担を軽減する追加認証など、多岐に渡る種類の追加認証が利用されるようになるでしょう。

追加認証を利用する際のヒント

- ☐ 現在はブロックしている取引を、コンバージョンを増加させる追加認証に置き換えて、正当な支払いがブロックされないようにします。
- ☐ 追加認証によりユーザーにとっては負担が増えることになり、コンバージョンにマイナスの影響を与えかねません。正当な顧客に悪影響を与えないように、追加認証をどのように実行するか、慎重に最適化し、テストします。
- ☐ 介在ごとに、それぞれ成功率は異なり、不正使用に対する影響も異なります。たとえば、セキュリティキーは不正使用者を阻止する上では極めて効果的ですが、コンバージョンを著しく損ないます。顧客が実行しているアクションの危険性や、リスク / コンバージョンの許容度に基づいて、適切な追加認証を選択してください。
- ☐ 追加認証は、顧客が支払いを完了するまでの過程で最も論理的に意味を成す場所で実行します (顧客がカード情報を追加するタイミングで物理カードのスキャンを要求するなど)。

2. 豊富なデータソースをもとに、より迅速で的確な判断を下す

かつて不正使用対策は人手に頼る部分が多く、アナリストチームが取引をひとつひとつレビューする必要がありました。今日では、大多数のビジネスが、必要なときには手動レビューも行いますが、ある程度の機械学習モデルと自動化を利用して、大きな規模で不正使用に対処しています (この混合型のアプローチは、業界やビジネスモデルによって異なります)。機械学習モデルは、正当な取引と、不正使用の可能性がある取引を識別する方法を学習しますが、一部には自主トレーニング機能を備えたものもあり、より拡張性や効率性の高いモデルとなります。

かつて機械学習モデルは、不正使用に対処するための先端技術と見なされていましたが、今では最低限必要なものになっています。事実、機械学習の機能だけでは、絶え間なく進化する不正使用のリスクを緩和するには、不十分です。アンケートの回答者も同意見です。レビュープロセスのほとんどを自動化している回答者の半数以上が、直面する不正使用の種類と量があまりにも急速に進化しているため、ビジネスがついていけないと答えています。

> “ 金融的な不正使用が発生する状況は、徐々に、より多様で複雑なものになっています。新しい不正使用のパターンや発生状況に絶えず適応していく必要があります。
>
> - ドイツのプロフェッショナルサービス会社で働く、不正使用に関する専門家

不正使用管理の進化における次のフェーズは、不正使用の予測モデルに情報を提供するためのより豊富なデータに焦点を当てることだと考えています。今日、この情報を収集するためのツールや技術は利用可能ですが、サイロ化された異種システム内にあることがほとんどです。たとえば、本人確認と生体認証のそれぞれ別のツールを持っている場合があります。将来的には、ビジネスはより優れたテクノロジーと統合を活用してこれらの情報を 1 カ所に集約し、不正使用の予測モデルをより効率的にするための全体的なアプローチを提供することができるようになると私たちは予測しています。

行動、生体認証、電話番号、電子メールアドレスに関連する豊富なサードパーティーデータ、活用されていないカード発行会社の豊富なデータ、ソーシャルネットワークプラットフォームなどを含め、顧客の購入プロセス全体から関連データを見ることにより、不正使用検出の精度は新たなレベルに到達します。

このレベルのデータは不正使用の予測モデルを改善する上で非常に有益である一方、この情報を収集して保存する際には、データセキュリティやプライバシーに関する世界の法規則に準拠するよう、注意を払う必要があります。

3. カード発行会社とビジネスが協力体制を強化して、不審請求の申請を効率化し、誤った支払い拒否を減らす

顧客がサイトでの購入を済ませると、その支払いの詳細情報をペイメントプロバイダーが取得し、カードネットワーク (Visa、Mastercard、銀聯 [UnionPay] など) を通じて、カード発行会社に支払いリクエストとして送信します。**オーソリフェーズ**で取引を承認または拒否する際の最終的な意思決定者は、Chase や Citi、および Barclays などのカード発行会社です。このカード発行会社は、オーソリ中に受け取った、かなり限定的なシグナルに基づいて、不正使用のリスクを計算します。

その一方で、ビジネスには、顧客のメールアドレスや請求先住所など、顧客および取引に関する豊富なデータがあります。このデータを、カード発行会社がすでに持っている情報と組み合わせると、結果として、より高い割合で取引が承認される可能性があります。

オーソリ率の向上と不正使用率の改善は双方にとってメリットがあります。カード発行会社にとっては、不正使用による損失の低減、運用コストの削減、誤った支払い拒否に関する顧客からの問い合わせが減ることによる取引量の増加につながります。同時に、ビジネスにとっては、決済のコンバージョン率の向上と、顧客維持の改善につながります。しかし、ほとんどのビジネスはまだこのデータをカード発行会社と共有していないため、情報の非対称性につながり、2021 年には **4,430 億米ドル**の誤った支払い拒否を招いています。

現在では、Capital One の **Enhanced Decisioning Data API** や **Amex の Enhanced Authorization API** といったカード発行会社の拡張オーソリ API の構築への投資にともなって状況に変化が見られます。オーソリが 1 パーセント上がると数百万ドルが動く大規模ビジネスでも、データ連携の重要性を理解し、カード発行会社との連携に投資し始めています。それでも、技術的なキャパシティのない、決済額もそれほど大きくない他の何百万ものビジネスが、カード発行会社とのカスタムメイドの連携の ROI を正当化できるかといえば、そこには格差があります。こうしたビジネスにとっては、Stripe やその他のペイメントプロバイダーが、その規模や、カード発行会社との組み込みのパートナーシップを活用することで、この交換の促進に役立つと期待しています。

4. 顧客が好む支払い方法は今後も移り変わり、不正使用の状況も変化する

後払い、デジタルウォレット、カードにカード番号が印字されていない仮想通貨カード (**Gemini クレジットカード**) などの支払い方法が存在感を高めています。特に、後払いサービスの利用者の増加は顕著です。後払いサービスは、**アメリカの顧客の半数以上**が利用しており、2020 年には**インド**と**イギリス**で最も急成長を遂げた支払い方法でもあります。

オンライン取引に使用されるあらゆる支払い方法は、多少なりとも不正使用のリスクがあり、カード以外の方法もそれは同じです。たとえば、後払いのような支払い方法は、不正取引のリスクは比較的小さいですが、新しい口座詐欺 (きちんと保護されていない可能性のあるユーザー登録フローの中で不正使用者が新しい ID を作成して不正口座を開く) や、アカウントの乗っ取り (悪意のある第三者が、ある顧客のアカウント認証情報にアクセスし、その顧客の支払い情報を使用して不正購入を行う) の影響を受ける可能性が高くなります。

しかし、顧客ライフサイクルの早い時期に不正使用防止戦略に焦点を当てることで、これらのリスクを緩和できます。取引そのものに焦点を当てるのではなく、顧客がたどる購入プロセスの早い時期に不正使用のアクティビティをスクリーニングすることで、顧客 (つまり不正使用者) が購入を行う前に評価を行うことができます。たとえば、ユーザー登録時に顧客の ID を確認し、重複するアカウントがないかチェックし、ログイン時に本人確認のための対策 (2 段階認証など) を実施します。

Stripe によるサポート

Stripe は、完全に統合された決済製品スイートであり、オンライン販売および対面販売の小売業者、サブスクリプションビジネス、ソフトウェアプラットフォームおよびマーケットプレイス、そしてこれらの中間にあるすべてのビジネスの決済体験を向上させます。不正使用の防止から本人確認まで、何百万ものビジネスが Stripe を利用して以下のことを実現しています。

決済体験を最適化

- **支払い時に詳細な関連情報を収集:** 顧客が支払う際に**詳細な関連情報の提供**を求めると、顧客の正当性の確認がスムーズになります。たとえば、顧客の名前とメールアドレスは必ず収集するようにしましょう。この追加情報を **Stripe Radar** に渡すことで、機械学習による不正検出の精度が高まるとともに、不審請求の申請時にさらなる証拠として提出できます。
- **他の決済手段を検討する:** 望ましい**決済手段**のセットを用意すると、顧客に柔軟性を提供できるとともに、不正使用のリスクを軽減できます。Apple Pay や Google Pay などのデジタルウォレットの場合、支払いを完了するためには追加の顧客確認 (生体認証、SMS、パスコードなど) が必要で、不審請求の申請率の低減につながります。同様に、ほとんどの口座引き落とし (資金を顧客の銀行口座から直接引き出す) では、顧客に同意書への同意、またはアカウント所有権の確認を要求します。これにより、さらにセキュリティ層が追加され、不審請求の申請の可能性が低減します。

決済時の不正使用の防止

- **機械学習による不正使用検知の利用:** 「もし x が発生したら y を行う」という論法で動作するルールベースの不正使用検知は、決して現代のインターネットビジネスのために設計されたものではなく、収益の減少を招きかねません。適応型機械学習を搭載した Stripe Radar は、あらゆる取引を評価し、リスクスコアを割り当てた後、不正使用のリスクに基づいて取引をブロックまたは許可するアルゴリズムを備えています。Radar のアルゴリズムは、変化する不正使用パターンや企業独自のビジネスに迅速に適応します。

- **カード発行会社とのパートナーシップを通じた不正使用の防止とオーソリの向上:** Stripe のカード発行会社とのパートナーシップにより、可能な場合には厳選されたリスクデータを共有することで、カード発行会社が正当な取引は許可し、不正な取引はブロックできるようにします。カード発行会社との連携により、カード保有者とビジネスの双方にとって価値が生まれます。つまり、顧客側はより安心してショッピングを楽しむことができ、ビジネス側は、不正使用に関する不審請求を増やすことなく、より多くの取引について承認を得ることができます。

- **2 段階認証の動的な適用:** Stripe Checkout では、**ヨーロッパの SCA 要件**に対処し、カード保有者のカード会社から要求があった場合や、不正使用が疑われる場合に、3DS などの認証を動的に適用することができます。Stripe Checkout は、入力済みの SAQ A を使用した、最も簡単な PCI 検証方法にも対応しています。カードテスティング攻撃が疑われる場合にのみ CAPTCHA を実行して、不正使用を防止します。

チームで不正使用に対応

- **不正使用をカスタマイズするためのルールを作成:** Radar for Teams を使用して、受け取った支払いの処理、疑わしい取引のブロック、あるいは疑わしい取引の**レビュー**をどのように行うかを管理するための、カスタムの**ルール**を作成できます。たとえば、手動レビューを実行するのに必要なリスクスコアを下げることや、初めて取引する顧客からの大量注文をレビューすることなどが可能です。また、Radar for Teams は、特定の支払いの**リスクに関するインサイト**も提供します。これにより、高いリスクスコアの原因となっている最も重要な要因を把握できます。この情報を使用して、よりターゲットを絞った追加ルールを作成できます。

- **高リスクの支払いの手動レビュー:** Radar for Teams には、もう 1 つの**レビュー**プロセスが含まれています。このプロセスを使用すると、特定の支払いに対して注意を促すことができます (ただし、この支払いは処理され、クレジットカードに請求されます)。一般に、Radar for Teams は大規模組織によって使用されますが、支払いを手動でレビューする機能は、(小規模ビジネスにおいて手動レビューが特に役立つことがわかっていますが) 会社の規模に関係なく有益です。疑わしい支払いを手動でレビューすることは、不審請求の申請が発生する前に、より正確な対策を講じる上で役立ちます。たとえば、レビュー中に不安に思った支払いがある場合は、顧客に電話やメールで連絡を取ることができます。あるいは、不正使用が疑われる支払いがある場合は、返金することができます。

不正使用防止に関するさらなるヒント

- **不正使用の傾向に関するより深いインサイトへのアクセス:** Stripe Sigma を活用すると、定義済みの SQL クエリやカスタムクエリを使用して、ダッシュボード内で Stripe データを迅速に分析できます。なぜ顧客が不審請求の申請をするのかといったものから、不審請求の申請に異議を唱える割合まで、複雑なビジネス上の疑問への答えが見つかります。また、Stripe Data Pipeline を使用して、最新の Stripe データをお使いのデータウェアハウス (Snowflake や Amazon Redshift) に送信することもできます。これにより、Stripe の不正使用リスクスコアを他の不正使用データと簡単に組み合わせて、より詳細な不正使用レポートを引き出すことができます。
- **世界規模での顧客の確認:** Stripe Identity なら、プログラムを使用して世界中のユーザーの身元確認ができるため、正当な顧客の負荷を最小限に抑えながら、不正使用者からの攻撃を減らすことができます。
- **コンバージョンを最適化して、より多くの売上を回収:** Stripe Card Image Verification は、誤ってブロックされる取引の数を減らすのに役立ちます。高リスクの可能性がある取引をブロックするのではなく、ユーザーにカードをスキャンして画像として提出するよう求めることで、ユーザーがそのカードを実際に所有していることを裏付ける機会となります (2022 年に導入)。

Stripe Radar を活用した不正使用対策について、詳しくは、**営業チームに問い合わせるか、こちらから登録**してご確認ください。

その他のリソース

不正使用への対処やビジネスの保護に役立つ資料を多数ご用意しています。

- **オンライン決済の概要**
- **不正使用防止のベストプラクティス**
- **機械学習を用いた不正行為検出の基礎**
- **Radar for Teams: ルールの基本**
- **Stripe Radar について**
- **パワフルな不正使用対策ツール**

調査について

2019 年から 2021 年にかけて数百万社で試行された数十億回の決済取引を分析しました。それらの決済取引およびビジネス全体を対象に、不審請求の申請とその理由、Stripe の機械学習モデルによる予測、3DS の使用状況、およびビジネスにおける手動レビューのアクティビティを調べました。国レベルでの不正使用率については、2021 年の支払い件数が 1 万件に満たない国は、取引件数が少なすぎて信頼性の高い不正使用率を計算できないため、分析から除外しました。

2022 年初頭に、さらに Milltown Partners 社 (データプロバイダーの focaldata 社と提携) と共同で、世界各国 (オーストラリア、カナダ、フランス、ドイツ、日本、オランダ、シンガポール、イギリス、アメリカ) における 9 業種で、少なくとも 10% の収益をオンライン販売で得ていると見積もるビジネスリーダー 2,500 人以上を対象に調査を実施しました。