2023 年 2 月 16 日

Stripe、クレジットカード不正使用の増加に伴い、不正対策 AI「Radar」の機能を向上

2022 年、クレジットカード不正使用による被害額が過去最高を記録

「カードテスティング」攻撃への対策が急務に

デジタルコマースの普及に伴い、新しいタイプの詐欺犯罪が世界中で増加しています。オンライン決済を導入している企業は、この問題によってビジネスが停滞しないよう、リスクを理解し解決策を講じておく必要があります。

日本においても同様で、日本クレジット協会が発表した速報データによると、2022 年にクレジットカードの不正使用による被害額が過去最高を記録しており、2021 年の 330 億円から大幅に増加し、1 年間で推定 400 億円の被害が出ると見積もられています。日本政府も、e コマースの普及を促進するために、この問題に取り組んでおり、経済産業省が委託する専門家委員会が 2 月に発表した報告書では、犯罪の手口が巧妙化していることが指摘されています。

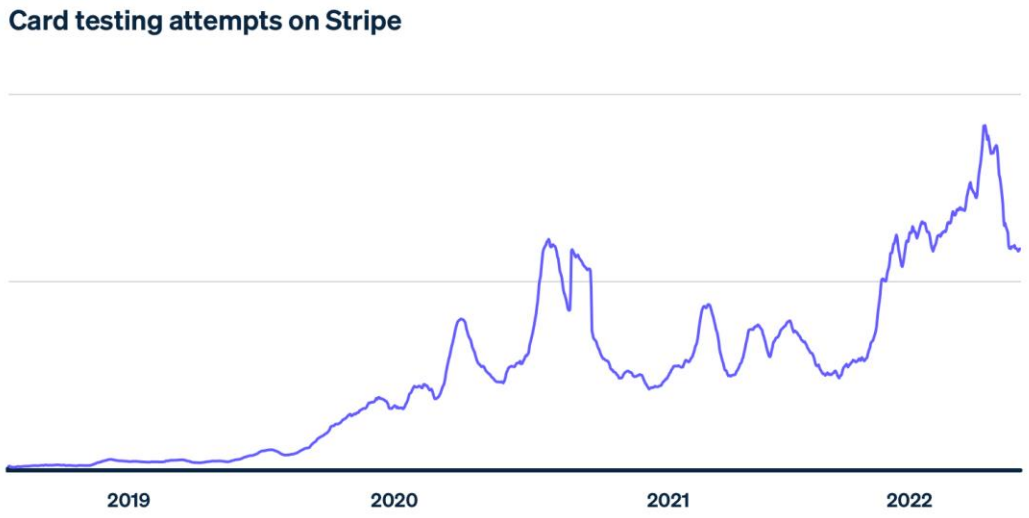
更なる大きな懸念は、インターネット決済の成長と共に、クレジットカードの不正使用も複雑に進化し続けてしまっているということです。Stripe の調査によると、過去 2 年間に日本で発生したオンライン決済上の詐欺事件の 94 %は、カードのデータのみを不正に使用する「カード番号盗用」によるものとなっています。これは、もはや物理的にクレジットカードを入手しなくても詐欺が実施できてしまうことを意味しています。

グローバルで事業を展開している Stripe は、様々な国や地域で発生している不正使用例を網羅しているため、他の主要市場で発生し、日本でも利用される手口も把握しています。直近で急増しているのが、「カードテスティング」攻撃です。

2022 年の 2 月から 8 月にかけて、Stripe はこのような不正使用が急増している状況を追跡調査したところ、加盟店で数百万件の少額またはゼロドルで取引が行われていたことを確認しました。これらの「カードテスティング」攻撃によって、犯罪者は盗んだクレジットカードがまだ使える状態であり、ビジネスに損害を与えることができることを確認しています。Stripe Radar (Stripe の不正防止ソリューション) は、この時期、ピーク時には 1 日あたり 2,000 万件を超える「カードテスティング」の試みを阻止していました。

ここ数年、より多くのビジネスのオンライン化が進むにつれて「カードテスティング」が急増しています。多くのビジネスオーナーは e コマースの複雑な仕組みに慣れていないため、悪質業者からの被害を受けやすい状態にあります。その結果、「カードテスティング」の試みは、2019 年以降急増し、100 倍以上になっています。

#####



盗難カードの検証

これらの攻撃は、盗んだクレジットカードから、個人情報等の価値のあるデータを引き出すプロセスにおいても重要な役割を果たします。悪質業者がクレジットカード情報リストを入手しても、それだけではどのカードが有効であるのか分かりません。取り消されたカードもあれば、有効期限が切れたものもあるため、リストに載っているクレジットカードが実際に価値があるのか分かりづらい状況にあります。

そこで登場するのが、カードテスティングを実施する「カードテスター」です。

Radar のプロダクトリーダーであるウィル・メグソン (Will Megson) 氏は、「一般的に詐欺は、最終的にお金を稼ぐために、バリューチェーンでさまざまなことをするプレーヤーがいるエコシステムです」と述べています。

カードテスターは、リストに登録されている各カードで自動的に少額の支払いを試みたり、有効な支払いソースとしてサイトに保存したりするプログラムを作成します。使用または保存に成功したカードは、他の悪質業者に売却すること

ができ、その業者はそのカードを使って高額な買い物をしたり、偽造カードを作成したりすることができるようになります。

加盟店に及ぼす損害

大量のカードテスティングは、不正行為を助長する以外に、ベンダーやプラットフォームにとっても問題です。ベンダーは、決済取引ごとにネットワーク料金を支払っています。この手数料は、1 回ごとの取引ではわずかなものですが、あるサイトが突然何千、何百万ものカードテストに利用されるようになると、その額は膨大になります。小さな商店は、ほんの数時間でカードテストのために破産してしまうこともあり得ます。

しかも、その被害は序章に過ぎないことが多く、チャージバックは、紛争費用、解決費用、インターチェンジ費用、そして解決に要する時間など、多くの費用やリソースを加盟店に負担させることになります。その結果、カードネットワークは、Visa 不正使用モニタリングプログラムや Mastercard EFM プログラム (不正使用が異常に高い加盟店のコンプライアンスプログラム) などのハイリスクカテゴリーに加盟店を分類し、処理手数料や加盟店準備金の増額を求めることができます。

「これらのプログラムは保護策を提供する一方で、懲罰的な意味合いもあります」とメグソンは述べています。

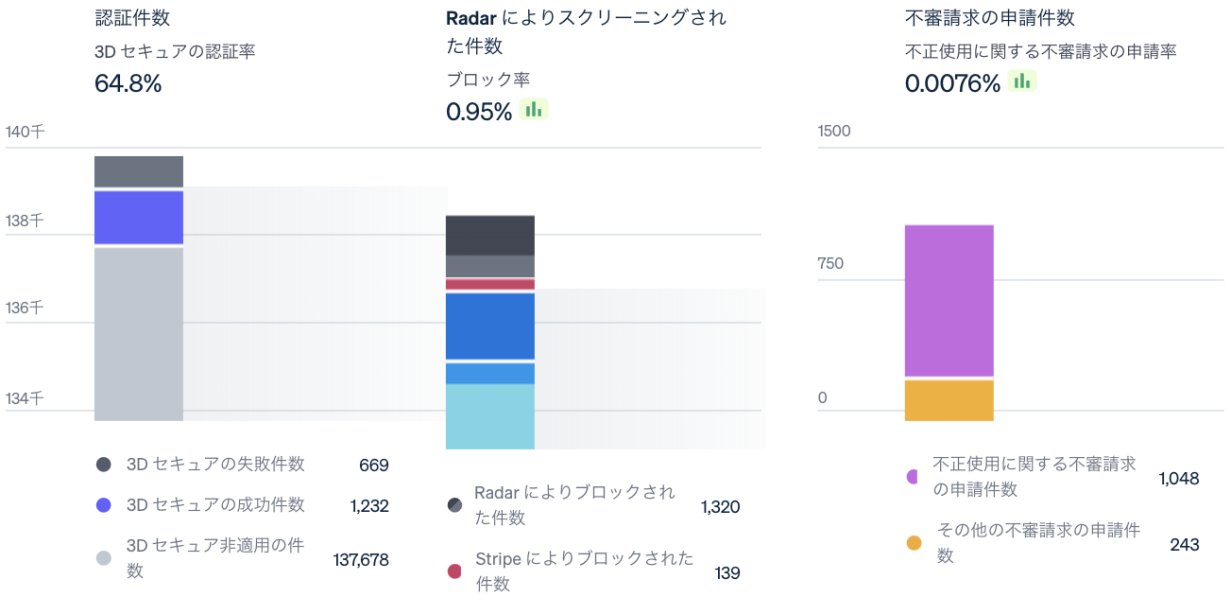
Radar による不正防止

幸いなことに、Radar を導入するだけで、企業は 自社のリソースや労力をかけずにこれらの攻撃を防ぐことができます。

カードテストの急増に対応するため、Stripe のエンジニアは Stripe ネットワークから Radar へのデータフローを効率化してプロセスを加速させたほか、決済取引単位のカードテスト機械学習モデルを新たに構築しました。また、新たに API が短時間に処理するリクエストの数に上限を設定するレートリミッターを数十個導入しました。この対応だけで、2022 年に約 4,000 万件のカードテスティング取引を防止することができました。

stripe

不正使用とリスク



より多くの攻撃を阻止するために

2022 年の結果は上々です。今年に入ってから、Radar はさらに 4 億件の不正取引を阻止し、不正取引と誤認される割合を増やすことなく、通過するカードテスティングの件数を半減させました。

「不正取引の多発により、決済処理ができなくなる寸前まで追い込まれました。そこで Radar を導入することで、プログラムで不正使用に対処し、さらにカードテスターに対抗するきめ細かい方法を確立できました」と、AdBlock 社の CEO、マット・メイヤー(Matt Maier) 氏は述べています。

Stripe は、機械学習のイノベーションと「カードテスティング」に対抗するという実際の経験から得た教訓を組み合わせることで、Radar への開発投資を続けています。「カードテスティング」をはじめとする不正や詐欺犯罪の進化に伴い、Radar も進化していきます。

#####

Stripe について

Stripe は、企業向けの経済的インフラストラクチャを構築する会社です。スタートアップから世界的な大企業まで、数百万におよぶ企業が Stripe を導入して支払いを受け取り、収益を成長させ、新たなビジネス機会を加速させています。サンフランシスコとダブリンに本社を持つ Stripe は、インターネットの GDP を拡大させることを使命に掲げています。

詳しくは https://stripe.com/jp をご覧ください。