KenConsulting
情 報 ・ 通 信 ・ ビ ジ ネ ス
Webサイト http://www.kenconsul.com　　メール support@kenconsul.com　　携帯 070-5460-5495

オンラインクレジットカード詐欺を防ぐために

e-コマースサイトを運営している事業者が、クレジットカードを使った詐欺にどの様に対抗すべきかを以下にご説明します。顧客はコマースサイトで商品を購入する時にクレジットカード番号、有効期限、名義人名を入力し、事業者はそれが正当かどうかをチェックするのが一般的なスクリーニングプロセスですが、それだけでは高度な技術を持つ詐欺集団に対抗できるとは限りません。詐欺集団がクレジットカードを盗んで商品を購入した場合、正当なクレジットカードの所有者がその料金を支払い、事業者はその費用を払い戻すことになり、その金額が全額損失になります。2006年、世界では3,800万枚のクレジットカードが盗難にあい、その為の被害額は3,600億円に上っています。以下にご説明する対抗手段はどの様なコマースサイトでも有効です。

2 通りの手法があります。1つはソフトウエアを使って自動でトランザクションを全てスキャンし、スクリーニングする方法です。もう1つはマニュアルでトランザクションをチェックし、詐欺かどうかをチェックする方法です。どちらの手法も単独では完全ではありません。 自動化手法では合法的な購入を違法な購入として誤認することがあります。 マニュアルでは全てのトランザクションがチェックできれば理想的ですが、その為には時間、労力、費用、顧客の満足を犠牲にしなければなりません。

自動とマニュアルのチェックを組み合わせた手法、即ち、トランザクションを自動的にスクリーニングし、システムが詐欺の可能性が高いと判断したトランザクションだけをマニュアルでチェックすれば良い、という手法が可能です。これにより資金と時間を節約し、生産性を高め、詐欺に対して高い防御レベルが実現できます。

この様な自動化とマニュアルを組合せた手法を以下に詳しくご説明します。

自動チェック:

- IP アドレスの地理情報
- メールのドメイン
- 匿名のオープンプロクシ
- BIN(銀行識別コード)チェック

マニュアルチェック:

- カード所有者に電話する
- サイン(押印)によるファクスでの承認

関連情報:

- PayPal の取り扱いについて

自動チェック

KenConsulting
情報・通信・ビジネス
Webサイト http://www.kenconsul.com　メール support@kenconsul.com　携帯 070-5460-5495

IP アドレスの地理情報

顧客が言っている地名と顧客がアクセスしているコンピュータの地名が一致しない時詐欺の可能性が高いと言えます。 MaxMind サービスは顧客のクレジットカードが課金を行う場所と実際にサイトにアクセスしている場所が一致しているかどうかを調べることによりトランザクションが正当かどうかを判断できます。アクセスしているコンピュータの IP アドレス*を調べればその場所が分かります。勿論、その人は単に旅行中か、自分が仕事をしていないオフィスの住所を言っただけなのかも知れません。

メールのドメイン

詐欺師は自分の匿名性を維持する為に hotmail.com などの無料の電子メールプロバイダを使うので無料の電子メールを使った購入は詐欺の可能性が高いと言えます。 もちろん、多くの合法的な顧客も無料の電子メールを使います。 B2B の商取引の場合、ブラウザを使って「http://www」の後に取得したドメイン名をタイプし、その Web サイトのビジネスが合法的なものに見えるかどうか確かめることをお勧めします。 この手法はコンシューマ商品の購入には適用できません。

匿名のオープンプロクシ

詐欺師は、追及を回避する方法の 1 つとして匿名のオープンプロクシを使います。 スキーマスクが銀行強盗の正体を現実の世界で隠す様に、これらのプロクシはクライアントが本当に何所にいるかを隠します。 弊社は多数の不正な購入がオープンプロクシ経由で行われる(約 26%)ことに気づきました。オープンプロクシを使った購入は組織されたクレジットカード詐欺集団による可能性が高いと言えます。

一方、合法的な注文もオープンプロクシから来ます。 この様な注文は通常ユーザが知らない内にウイルスに感染し、スパマーやクレジットカードハッカーにハイジャックされた顧客のコンピュータからのものです。 弊社の経験では、合法的な購入の 4%がオープンプロクシから来ています。これはコンピューターウイルスが広く伝播している為です。 注文がオープンプロクシから来ていることを検知したら顧客に連絡してより多くの情報を得ることをお勧めします。openrbl.org で参照すればそのプロクシの IP アドレスがオープンプロクシリストにあるかどうか検証できます。

弊社の minFraud サービスは匿名のオープンプロクシを報告し、更にその IP アドレスがスパムソースとして報告されているかどうかをお知らせします。 弊社はスパムソースとして判明している IP アドレスから受けた不正な注文は、詐欺集団が関与している可能性が高いとしてブロックします。

BIN(銀行識別コード)チェック

多くの国際的なクレジットカードは住所による検証をサポートしていません。 銀行識別コード(BIN)をチェックすることにより、クレジットカードを発行している銀行がカード所有者が居住しているのと同じ国にあるかどうかを確かめられます。但し、合法的なユーザでも外国でクレジットカードを使うことがあることに注意してください。

クレジットカード上に印刷してある銀行名とその顧客サービス用の電話番号を教えるよう顧客に頼むこともできます。 この情報を弊社のデータベース中の BIN に関する情報と一致するかどうか照合します。 この手法を使って顧客がクレジットカードを現実に持っていることが検証できます。詐欺師が何らかの方法で BIN 名と電話番号リストを入手していないなら、になりますが。

Manual Checks マニュアルチェック

カード所有者に電話する

これはカード所有者が購入を認めたかどうかを確認する非常に良い方法です。ただ、この手法はコマースサイトの販売業者にとって時間がかかるのが欠点です。 この手法は、まず注文確認用の電話番号を記入する様に注文用フォームを作ります。次に、コマースサイトの運用会社とクレジットカードの発行企業(またはどちらか)に電話して、顧客が教えた電話番号が正しいかどうか確認します。 カード所有者の正しい電話番号を得たらその番号に電話し、注文を認めるかどうかを尋ねます。 もし電話に出た相手がクレジットカードの所有者であり、注文を認めないなら、その人にクレジットカード会社に連絡してカードが盗まれたことを報告する様に提案してください。 この手法は一般的に高額の商品の購入や、自動チェックで高い詐欺スコアが戻ってきた場合に行うようお勧めします。 MaxMind の Telephone Verification サービスを使うとこの検証プロセスを自動化できます。

サイン(押印)によるファクスでの承認

これもカード所有者を検証する手法です。 この手法は顧客の手間が増えるのが欠点です。顧客は送った認証用のフォームに記入し、サイン(押印)し、クレジットカードの両面のコピーを付けてファックスで返送します。(フォームのサンプルはここをクリック)この手法は正当なカードの所有者が商品購入を認めた覚えがないと主張する場合に有効です。特に、ソフトウエアの様なデジタル商品の販売で「好意的な」返金を防ぐ最良の方法です。

関連情報

PayPal の取り扱いについて

多くの e-コマースサイトではクレジットカードも PayPal も受付けています。 PayPal による支払いはクレジットカードと同様に慎重に受け付けているのが一般的です。 PayPal は不渡りになることがありますし、更に、多くの PayPal アカウントがハイジャックされています。弊社はハイジャックさ

れたアカウントから逆に支払いを受けたことが少なくとも1回あります。 この場合弊社は幸運にも詐欺師が不正なクレジットカード購入に使ったのと同じ IP アドレスを使ったことに気づいたので、PayPal アカウント所有者に接触し、その人のアカウントがハイジャックされていることを知らせました。 一般的に言って hotmail や他の無料のメールアドレスを持っている PayPal アカウントは危険です。hotmail と PayPal アカウントの両方に同じパスワードを使うことがよくあるので、ハイジャック犯は PayPal アカウントと電子メールの両方にアクセスできることになるからです。

脚注

***** トランスペアレントなプロクシのために、HTTP ヘッダーHTTP_X_FORWARDED_FOR と HTTP_CLIENT_IP を調べてプロクシの背後にある IP アドレスを得てください。弊社の minFraud サービスは forwardedIP 入力フィールドを使ってその値をお渡しします。

最終更新日: 2005 年 1 月 28 日
ご質問、ご連絡は support@kenconsul.com までお願いします。