Credit Card Fraud Prevention

Article Number
000087586

Information

Background

Millions of credit card numbers are stolen every year. They are then sold in bulk on the dark web. Anyone in possession of these stolen card numbers needs to determine which credit card numbers are still valid and can be used for fraudulent purposes.

An online giving form that doesn't require user authentication provides the means to verify if a stolen credit card number can still be used. Encompass isn't the only company that has the type of forms that can be used for this purpose, but there is a lot of activity in this area. Client forms not behind a login, primarily giving forms, regularly become targets of this card checking activity.

This type of fraudulent activity is evidenced by a series of small transactions - $1, $2 or $5 transactions are those most seen.

While this fraudulent activity is troubling, there is no data security attack or breach taking place. The fraudulent activity is simply card checking. While this is an issue that needs to be resolved, it is not a case of constituent profile or transactional / card data stored in the Encompass system being at risk as that information is stored in unconnected systems behind multiple hardened firewalls.

These card checking transaction activities are seen to occur at both low volumes, with a single person or small group checking cards one by one. These have always been addressed in a series of steps as outlined below.

In 2014, some clients started to report massive surges of this card checking activity with hundreds or thousands of transactions over a very small period of time. These were determined to be the result of bots, basically duplicating the automatic, software-driven transaction of the type used in the Encompass automated testing, to automatically attempt a large number of transactions very quickly.

In response to this bot-driven card checking, Encompass developed the Billing Form CAPTCHA was developed to defend against automated bots, as a human is required to read the CAPTCHA and input the random series of characters. The default mode of the CAPTCHA is to appear after 5 failed instances tied to any non-member ID session. Payment Gateway Admins in Encompass can set the default down incrementally to the point where it is enabled for all transactions (setting = 0).

Recently, some clients have reported an intermediate level of this card checking. More than a single person working alone, but also not at the volumes that occurred with the bots before the introduction of the CAPTCHA. This level of activity appears to be something along the lines of a large group of humans working together to check cards on a targeted form because the volume is higher than the single individual, but must also be humans as they are not thwarted by the CAPTCHA.

Order of Operations for Client Defense Against Card Checking Activity

1. **Most Important Step:** The most important and most effective step you can take is to increase the AVS (**Address Verification System**) settings in your payment gateway. AVS checks the numerical

components of the credit card billing information entered by the user.

It is our experience that the default AVS level for most, if not all, gateways are set to only verify that the card number and expiration date are correct. While Encompass is required to send all of the billing information on the credit card billing form for a particular payment gateway configuration, that is separate from whether a payment gateway actually verifies if that information matches what is on file for that particular credit card. With AVS, clients can increase that to verify that the zip code, phone number, and/or street address matches that associated with the card.

To increase your AVS settings, you will need to contact your payment gateway. Even a small adjustment like verifying the billing zip code is likely to help. People in possession of stolen card numbers have a list of credit card numbers to test, but they do not usually have the correct billing address information. By having the payment gateway verify the zip code, you stop them without making it difficult for legitimate donors. If the zip code does not stop the activity, then increase it to the phone number and the card billing street address.

Note regarding PayPal PayFlow Pro - The PayFlow Pro payment gateway requires the purchase of an additional fraud package in order to have AVS capability.

2. Set a minimum allowed payment of $5 or $10 for the donation amount on the form in Encompass. This will have no, or very limited, effect on legitimate users.

3. Set a minimum transaction amount with your payment gateway (not Encompass) so that transactions under that amount are declined. This will have no or very limited effect on legitimate users.

4. Set the CAPTCHA to always-on by changing the admin setting to 0 (zero). This is set to 5 invalid attempts by default. This will make the form somewhat more cumbersome for users, but also for individuals trying to check cards and will stop the bot-driven activity.

Caution on CVV2 verification - If you have enabled the Encompass recurring billing system (online giving scheduled or perpetual payments; membership scheduled payments or auto-renewal), and use a payment gateway other than IATS Payments, Elavon Converge (formerly Virtual Merchant), or CyberSource with tokenization enabled, then you should **not** set card verification on the CVV2 code as this will cause recurring transactions to fail. This is because PCI compliance forbids Encompass from storing the CVV2 so it is not available to be sent with the recurring transaction scheduled in Encompass. IATS Payments, Elavon Converge and CyberSource have custom capabilities that enable Encompass to send an initial transaction with CVV2 for verifying, but not have to send a CVV2 code for verifying with the subsequent recurring transactions.

Additional Options

There are additional options that are available to help you defend against this card checking activity. While it has been our experience that the steps above will stop the activity from occurring, these are other options that you can consider if there is pause or pushback on steps 1-4 described above.

1. Set the form to prompt users to create a non-member account. Providing this option is sometimes enough of a deterrent and the bad guys will move on to another site. You might even try this for a week or so and then set it back to allow direct access.

2. Clone the form to create a new version of it with a new URL. This can also cause them to move on to a different site if the link they used before no longer works.

3. Set the form to "logged in". This is very similar to option #1 but is more restrictive. You may only need to try this for a week or so and then set it back to allow direct access.

KB Product

Encompass

Last Modified Date

Fri Apr 11 19:31:57 GMT 2025

Title

Credit Card Fraud Prevention