FRAUD ATTEMPT NOTIFICATION

We have been notified that Visa has observed a sustained increase in enumeration attacks and account testing. It is imperative that all merchants use best practices to help protect the payment system against such attacks.

Most recently we have seen various gateway's "Hosted Payment Form" being utilized to test card numbers. While ALL merchants should address these fraud prevention measures, it is critical that those using any Hosted Payment Form *take immediate action* to prevent your account from being utilized to test cards.

Recommended actions are listed below:

FOR ALL MERCHANTS

- Have your Gateway provider add Velocity Filters for the number of times a card could be tried
- Add Velocity Filters for the number of times a single IP address can send transactions to them as well as any other controls that can prevent this type of activity.
- Set minimum transaction amounts that apply to your business ie if your business does not offer a product under $25 then your minimum transaction may be set at $30.
- If you do not sell Internationally, block transactions from all countries other than the US.
- Scan their systems for Malware & Spyware.

ADDITIONAL RECOMMENDATIONS FOR THOSE USING PAYMENT FORMS

- Add CAPTCHA to your website to ensure your check-out page prevents automated transaction initiation by bots or script.

Contact Information for common gateways are listed below.

- USA ePay at 866-872-3729
  - included the link we discussed for your reference: Fraud Center
- Authorize.net 877-447-3938
- NMI 800-617-4850

Visa Guidance to Guard Against Enumeration Attacks and Account Testing Schemes