Wind River
Payments

Payment Card Account Testing

E-Commerce or Compromised Gateway Credentials

Wind River has detected that your business's e-commerce website or gateway is being used for one of the following scenarios:

- Test stolen credit card numbers to see if they are active
- Guess the expiration date or other card parameters to see what works
- Systematically try different combinations of card numbers until one that works is found
- Compromised login credentials for your virtual terminal or payment gateway account

You may have already had a discussion with your Relationship Manager regarding this situation. The purpose of this document is to further clarify what is occurring and provide you with options to help mitigate it.

The scenarios above are all part of what the payment card industry calls card testing and enumeration attacks. Attackers use automation on unsuspecting ecommerce websites to run hundreds or even thousands of authorization attempts per hour -- depending on which scheme they are attempting.

This is a problem for several reasons:

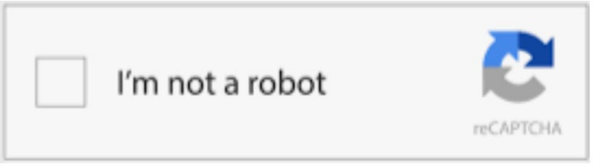
- You will be responsible for paying substantial authorization and transaction fees.
- There is a strong likelihood that you will be targeted for other financial fraud attempts.
- You can potentially be fined by the payment card brands (Visa, Mastercard) if the activity is not stopped in a timely manner.

Wind River has compiled a list of actions you can take to help thwart such fraudulent activity. Your Relationship Manager will work with you to answer any questions you may have about these steps and recommend the best solution for your business.

E-Commerce:

1. Implement ReCaptcha on your e-commerce site, a cost-free, anti-automation solution from Google. While more sophisticated attackers can subvert ReCaptcha , it's usually successful at stopping these types of attacks. We recommend using the most up-to-date version (V.3 at the time of this writing). Your web developer should be able to deploy this tool to your website.

2. Check with your web developer or 3rd party web host to see if they have any tools available that may help stop this type of activity. Note that blocking a single IP is not sophisticated enough as attackers can simply change their IP.



3. Our gateway partners have their own anti-fraud tools which may help, although they have cost. Configuration of these tools can be a little tricky. You'll want to ensure the settings you use stop card testing but do not impact legitimate sales. We have experience with these types of tools and are here to help.

4. Consider requiring users to register or login to make purchases. This puts a significant speedbump in the way of automation. You'll want to carefully consider this as you do not want to deter legitimate customers from purchasing on your ecommerce site.

5. The highest-level solution is to contract with a modern cloud-based fraud solution that can make a real-time determination whether a machine or person is inputting authorizations. This type of solution is effective at stopping other types of fraud as well. Wind River partners with such a solution, and we are happy to refer you to get more information and pricing.

6. In the most extreme cases, Wind River can turn off payments to stop all payment activity on your website. Don't worry, this is a last resort and is normally deployed only if all other options have been exhausted.

Gateway / Virtual Terminal Compromised Credentials:

Scenario: User credentials have been compromised and an attacker is using your merchant account to test stolen credit cards with your gateway provider.

1. If multi-factor authentication is an option, enable it. This allows the gateway to send you an out-of-channel verification during login attempts (e.g. receiving a code on your mobile device). Enabling multi-factor authentication is normally highly effective against an attacker being able to access your account.

2. Immediately change the login credentials for your gateway or virtual terminal login. If more than one employee has a login, change all while using strong credentials (password with 10 or more characters with upper- and lower-case letters, numbers, and special characters).

Try to determine which credentials may have been compromised based on login records. This may help you determine if other action is needed to help secure your computer network.

Please note that a username and password alone are often not strong enough in today's environment to secure an account, even if the password is strong. Multi-factor authentication is highly recommended.

Your Wind River Relationship Manager will be in close contact with you to help you through this process.