Why we need the Virtual Credit Card (VCC).

Recently there have been some questions raised as to why we as a Group we need to have and maintain the Virtual Credit Card system currently in place.

The reason why booking.com can't transfer consumer credit card information to properties is due to the fact the receiving computer is not PCI compliant. Booking.com is compliant, sends credit card details to UseROSS which is compliant, then sends credit card information to our motels which are not compliant.

Recently one of our member's computers was destroyed by a virus which may have caused a recent credit card breach. Consumer credit cards have been stolen from the ARRA network and have been used illegally.

The VISA and MasterCard via the National Bank have asked us to rectify the situation. This is the reason for the virtual card. Trustwave | SMART SECURITY ON DEMAND www.trustwave.com has been engaged by the Bank to ensure that we are PCI compliant.

The below extracts from the Payment Card Industry (PCI) Security Standards Council's website: https://www.pcisecuritystandards.org/merchants/ help explain why the Virtual Credit Card (VCC) has been set up for ARRA Accommodation Group Members.

This is where you will find what you need to know about the PCI Security Standards. You can also find out why and how to become compliant with PCI Security Standards, and how to make use of the information and services the Council offers to merchants worldwide.

From the world's largest corporations to small Internet stores, compliance with the PCI Data Security Standard (PCI DSS) is vital for all merchants who accept credit cards, online or offline, because nothing is more important than keeping your customer's payment card data secure. The size of your business will determine the specific compliance requirements that must be met. Note that enforcement of merchant compliance is managed by the individual payment brands and not by the Council – the same is true for non-compliance penalties.

The Council is here to help merchants through maintaining and enhancing the PCI Security Standards, providing education and training about protecting payment card data with the PCI Security Standards, and by serving as a forum for engaging with the industry on developing these standards. Our **FAQs** hold a wealth of information – to save yourself time, be sure to check there first when you have specific questions.

What is the Payment Card Industry (PCI) Data Security Standard (DSS)?

The PCI Data Security Standard represents a common set of industry tools and measurements to help ensure the safe handling of sensitive information. Initially created by aligning Visa's Account Information Security (AIS)/Cardholder Information Security (CISP) programs with MasterCard's Site Data Protection (SDP) program, the standard provides an actionable framework for developing a robust account data security process - including preventing, detecting and reacting to security incidents. The updated version, version 1.1, developed by the founding members of the PCI Security Standards Council, became effective with the launch of the PCI Security Standards Council.

Why Comply with PCI Security Standards? Why should you, as a merchant, comply with the PCI Security Standards?

At first glance, especially if you are a smaller organization, it may seem like a lot of effort, and confusing to boot. But not only is compliance becoming increasingly important, it may not be the headache you expected. Compliance with data security standards can bring major benefits to businesses of all sizes, while failure to comply can have serious and long-term negative consequences. Here are some reasons why.

- Compliance with the PCI DSS means that your systems are secure, and customers can trust you with their sensitive payment card information:
    - Trust means your customers have confidence in doing business with you
    - Confident customers are more likely to be repeat customers, and to recommend you to others
- Compliance improves your reputation with acquirers and payment brands -- the partners you need in order to do business
  Compliance is an ongoing process, not a one-time event. It helps prevent security breaches and theft of payment card data, not just today, but in the future:
    - As data compromise becomes ever more sophisticated, it becomes ever more difficult for an individual merchant to stay ahead of the threats
    - The PCI Security Standards Council is constantly working to monitor threats and improve the industry's means of dealing with them, through enhancements to PCI Security Standards and by the training of security professionals
    - When you stay compliant, you are part of the solution – a united, global response to fighting payment card data compromise
- Compliance has indirect benefits as well:
    - Through your efforts to comply with PCI Security Standards, you'll likely be better prepared to comply with other regulations as they come along, such as HIPAA, SOX, etc.
    - You'll have a basis for a corporate security strategy
    - You will likely identify ways to improve the efficiency of your IT infrastructure
- But if you are **not** compliant, it could be disastrous:
    - Compromised data negatively affects consumers, merchants, and financial institutions
    - Just one incident can severely damage your reputation and your ability to conduct business effectively, far into the future
    - Account data breaches can lead to catastrophic loss of sales, relationships and standing in your community, and depressed share price if yours is a public company
    - Possible negative consequences also include:

        - Lawsuits
        - Insurance claims
        - Cancelled accounts
        - Payment card issuer fines
        - Government fines

You've worked hard to build your business – make sure you secure your success by securing your customers' payment card data. Your customers depend on you to keep their information safe – repay their trust with compliance to the PCI Security Standards.

How to Be Compliant - Getting Started with PCI Data Security Standard Compliance

PCI Security Standards are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The Council is responsible for managing the security standards, while compliance with the PCI Security Standards is enforced by the payment card brands. The standards apply to all organisations that store, process or transmit cardholder data – with guidance for software developers and manufacturers of applications and devices used in those transactions. **If you are a merchant that accepts payment cards, you are required to be compliant with the PCI Data Security Standard.**