

Important NEWS from C&K SYSTEMS and RADIANT SYSTEMS regarding PCI Compliance.

Dear Business Owner or Manager,

We have a duty to inform you of your obligations under the mandatory PCI PA-DSS requirements that are for all businesses that accept credit cards.

This brochure is intended to act as a guide and explain the requirements that businesses must meet in order to protect against liability in the event of a credit card security breach.

It also outlines the steps we are proactively taking as your service provider to protect your customers information from hackers and dishonesty.

The time to act is NOW!, it is only a matter of time before your business will be impacted.



C&K Systems, Inc.

648 Independence Parkway, Suite 400, Chesapeake, VA 23320

Tel. : 888-476-7911. Fax : 757-482-6440. Email : sales@cksystem.com Web : <http://www.cksystem.com>

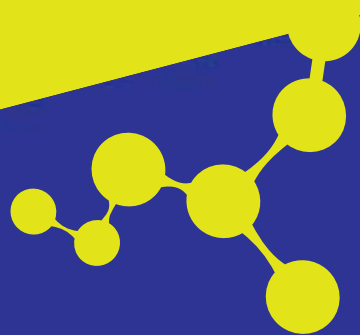


C&K Systems is taking a serious stance on PCI compliance. Our ultimate goal is to protect your data from prying eyes. To accomplish this, our mission is two-fold: we must first ensure that we meet all the necessary standards as a service provider, and then we need to work with you, the merchant, to ensure that you too have fulfilled your annual PCI requirements.

To address the first half of our mission, C&K Systems has partnered with Coalfire Systems to help us achieve certification as a PCI Compliant Level 1 Service Provider--the highest level of security classification in the industry. This certification will allow C&K to securely host ecomm, Counterpoint, and other applications.

Our relationship with Coalfire will also enable us to offer a group of comprehensive services to help you meet and maintain your PCI security requirements and limit your exposure. We can assist with the completion of security questionnaires that banks are requiring; and we can provide complete security risk assessments, audits, vulnerability scanning and penetration testing for your business.

Additionally, we are implementing new procedures for delivering support that meet PCI standards. We have recently secured "Logmein Rescue", a remote-access application that logs all the activity of our technicians whenever they access a client's system to provide support. Logmein Rescue also requires that the customer grant specific access to our techs. This process prevents random logins and also eliminates the need for technicians to know any of your passwords.



Contact your C&K Systems
Account Executive for details



The second half of our mission is to help you, our customer, meet your requirements. Simply running a PCI-compliant application such as CounterPoint does not automatically mean that you have met your obligations. Therefore, we intend to provide education by way of newsletters, webinars, and personal phone calls. Its imperative that you understand not only the steps required to achieve compliancy, but also the ramifications of ignoring PCI-DSS. Banks and card payment services are increasing enforcement and are assessing stiff penalties on small and large businesses alike. These measures have drastically increased since late last year.

Your obligation as a merchant to meet these requirements not only protects your customers' information, but also protects your systems and data from hackers, data thieves, viruses, malware and dishonesty.

Call us today and talk with a PCI security expert on how we can help.

The Pain of Non-compliance

Small merchants with on-site credit card processing who are hacked and have not put PCI standards in place can be fined \$20 to \$30 for each stolen card number (up to \$500,000). If the breach is large, they may also be required to undergo a forensic audit (the cost of which starts at \$15,000), be subject to more stringent standards than other stores of their size and may be sued. In addition to the horrors of dealing with the original breach, this is enough to effectively wipe out any small merchant. Please watch this 11 minute video to see how any sized retailer is at risk: <http://www.youtube.com/watch?v=7W-k3R2N7Zk>



Stiff Requirements for On-site Credit Card Processing

For merchants who use on-site credit card processing, the requirements are extensive. They must answer 195 questions on Questionnaire C each year, and begin quarterly or monthly security scans of their store. They must also take active steps to fix any areas that are found to not be in compliance and specify dates by which their stores will be in compliance.

Questionnaire C is for merchants who use Point-of-Sale terminals connected to the Internet with a program such as Counterpoint.

These lengthy self-assessment questionnaires cover 12 security steps in great detail, including:

- ▶ Firewall and network testing
- ▶ Track and monitor all access to network resources and data.
- ▶ Use of secure encryption and passwords
- ▶ Quarterly scanning of all IP addresses connected to the internet
- ▶ Anti-virus, anti-spyware and anti-adware programs installed and updated
- ▶ Creation of a company Information Security Policy for employees, contractors and IT vendors
- ▶ Shredding, cross-cutting or pulping of paper documents that contain credit card information
- ▶ Secure storage of backups.
- ▶ PCI Compliancy Websites

<http://www.pciknowledgebase.com/> Knowledge base for PCI related questions.

<https://www.pcisecuritystandards.org/education/prioritized.shtml> Prioritizing high risk targets

<http://technet.microsoft.com/en-us/security/cc184923.aspx> Microsoft baseline Security Analyzer

<http://www.visa.com/dropthe data/> Best way to keep yourself safe, don't save the data

If any item on your questionnaire is not in compliance, you must specify a date that you expect to be in compliance, and explain what actions you plan to take to achieve compliance.

