PCI-DSS Compliance in Rackspace Hybrid Cloud

Written by Mahesh Gande,
Senior Solutions Manager

Francis Ofungwu,
Product Manager for Rackspace Security Solutions

Jarret Raim,
Rackspace Cloud Security Product Manager

Lizetta Staplefoote,
Online Content Strategist

Table of Contents

1. Introduction

Meeting Payment Card Industry – Data Security Standards (PCI-DSS) can be a complex and costly exercise for the average e-commerce merchant. This may explain why 96% of 2011 breach victims were not compliant as of their last assessment or had never been validated.[1]

There is no one-size-fits-all approach to achieving and maintaining compliance. Merchants without the expertise to execute an effective compliance program should seek guidance from external partners to supplement their knowledge gaps and infrastructure deficiencies.

2. The 12 Requirements of PCI-DSS Compliance

PCI-DSS is a set of comprehensive requirements for enhancing payment account data security. The standard was developed by the PCI-DSS Security Standards Council, which includes American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa to help facilitate the broad adoption of consistent data security measures on a global basis.

PCI-DSS compliance is broken down into 12 steps across six categories of protection:

1. BUILD AND MAINTAIN A SECURE NETWORK

- **Requirement 1:** Install and maintain a firewall configuration to protect cardholder data.

Establishes firewall and router configuration standards that mandate testing, testing procedures, and a review of configuration rule sets every six months.

- **Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters.

Addresses password hygiene with respect to vendor-supplied passwords that if combined with hacker tools able to show all of your networked devices can make you a sitting duck for unauthorized entry.

Common Default Passwords You Need to Change: access, admin, anonymous, database, guest, manager, root, sysadmin, user

2. PROTECT CARDHOLDER DATA

- **Requirement 3:** Protect stored cardholder data

Defines storage, encryption, and retention of cardholder data and authentication data for required business uses. Also covers the documentation and protection of the keys used to encrypt cardholder data.

	Cardholder Data	Authentication Data
Includes	• Primary Account Number (PAN) • Cardholder Name • Service Code • Expiration Date	• Full Magnetic Stripe Data • CAV2/CVC2/CVV2/CID • PIN/PIN Block
Retention	Purge based on your documented data retention policy	Never

- **Requirement 4:** Encrypt transmission of cardholder data across open, public networks

Refers to the implementation of strong cryptography and security protocols such as SSL/TLS, SSH or IPSec to safeguard sensitive cardholder data during transmission over open, public networks (Internet and mobile). Additionally, wireless networks transmitting cardholder data or connected to the cardholder data environment must use industry best practices to implement strong encryption for authentication and transmission.

82% of breached operations were not compliant with PCI-DSS standards for protection of stored data[2]

3. MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

- **Requirement 5:** Use and regularly update anti-virus software or programs

Any system potentially affected by malware must be protected by anti-virus software that is current, actively running, and generating audit logs.

- **Requirement 6:** Develop and maintain secure systems and applications

Application code must adhere to secure coding guidelines including reviewing custom application and third-party code to identify vulnerabilities.

4. IMPLEMENT STRONG ACCESS CONTROL MEASURES

- **Requirement 7:** Limit access to system component and cardholder data to only those individuals whose job requires such access

To protect critical data from access by unauthorized personnel inside and outside of the business, systems and documented processes must exist to restrict access to cardholder data using role-based access controls (RBAC) set to "deny all" unless access to cardholder data and systems is specifically granted.

- **Requirement 8:** Assign a unique ID

Any user granted access to cardholder data must have a unique identification so that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. This requirement also includes provisions around using two-factor authentication via token and storage of user passwords.

- **Requirement 9:** Restrict physical access to cardholder data

To safeguard against physical media containing cardholder data being removed or compromised, areas where devices, data, systems, or hardcopies of cardholder data must be restricted from general access. This applies to both electronic systems for all online merchants and paper receipts and POS systems for brick and mortal establishments.

5. REGULARLY MONITOR AND TEST NETWORK

- **Requirement 10:** Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical for effective forensics and vulnerability management. Logs should record specific actions and create an audit trail including at a minimum: user identification, type of event, date and time, success or failure indication, origination of event, and identity or name of affected data, system component or resource. These logs should be reviewed daily and audit trails retained for at least a year.

- **Requirement 11:** Regularly test security systems and processes

Run internal and external network vulnerability scans at least quarterly and after any significant change in the network or infrastructure, application upgrade or modification. After passing the initial compliance scan, merchants must pass four more consecutive quarterly scans by an Approved Scanning Vendor (ASV) as a requirement for compliance. This provision also includes the use of up-to-date network intrusion detection systems (IDS) and file integrity monitoring tools to check for and alert to system compromise or unauthorized modification of critical files.

Only 6% of breached organizations report having regular security systems testing and processes.[3]

6.MAINTAIN AN INFORMATION SECURITY POLICY

- **Requirement 12:** Maintain a policy that addresses information security for all personnel

Establish, publish, update, and disseminate a security policy that addresses compliance requirements. This policy should include an annual review process for identifying vulnerabilities and formally assessing risks. Defined usage policies for employee screening, remote access, wireless, removable electronic media, laptops, tablets, handheld devices, email and internet are also required.

3. Who Needs PCI-DSS Compliance?

If your business meets either of these criteria, you should have a PCI-DSS strategy in place:

- Do you store, process, or transmit Cardholder data*?
- Do you provide services to merchants who process, store, or transmit Cardholder data*?

*Refers to PAN (Primary Account Number) plus cardholder name, expiration date, service code

UNDERSTANDING PCI-DSS MERCHANT LEVELS AND VALIDATION TYPES

The process and frequency of validating compliance with these 12 steps is determined by your merchant level and security assessment types below:

	Level 1	Level 2	Level 3	Level 4
Criteria	Over 6 million transactions processed per year	1 million to 6 million transactions processed per year	20,000 to 1 million transactions processed per year	Less than 20,000 transactions processed per year
Validation	Annual on-site review by an internal auditor and a network scan by an approved scanning vendor (ASV).	Annual completion of a Self-Assessment Questionnaire (SAQ) and a network scan with an ASV.	Annual completion of an SAQ and a network scan with an ASV.	Annual completion of an SAQ and a network scan with an ASV.[4]

This is an example of VISA card brand classifications. Other industry standards exist.

Your validation type determines which SAQ you need to complete.

Type	Description
A	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants.
B	Imprint-only merchants with no electronic cardholder data storage, or standalone, dial- out terminal merchants with no electronic cardholder data storage
C-VT	Merchants using only web-based virtual terminals, no electronic cardholder data storage
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage
D	All other merchants not included in descriptions for SAQ types A through C above, and all service providers defined by a payment brand as eligible to complete an SAQ.[5]

This is an example of VISA card brand classifications. Other industry standards exist.

WHY IS COMPLIANCE IMPORTANT?

Non-compliance to PCI-DSS could lead to:

- Loss of reputation
- Increased costs for accepting credit card transactions
- Substantial fines associated with security breaches and non-compliance

Should a breach occur as a result of non-compliance, there are discovery and containment costs for investigating the incident, remediation expenses, and attorney and legal fees in addition to:

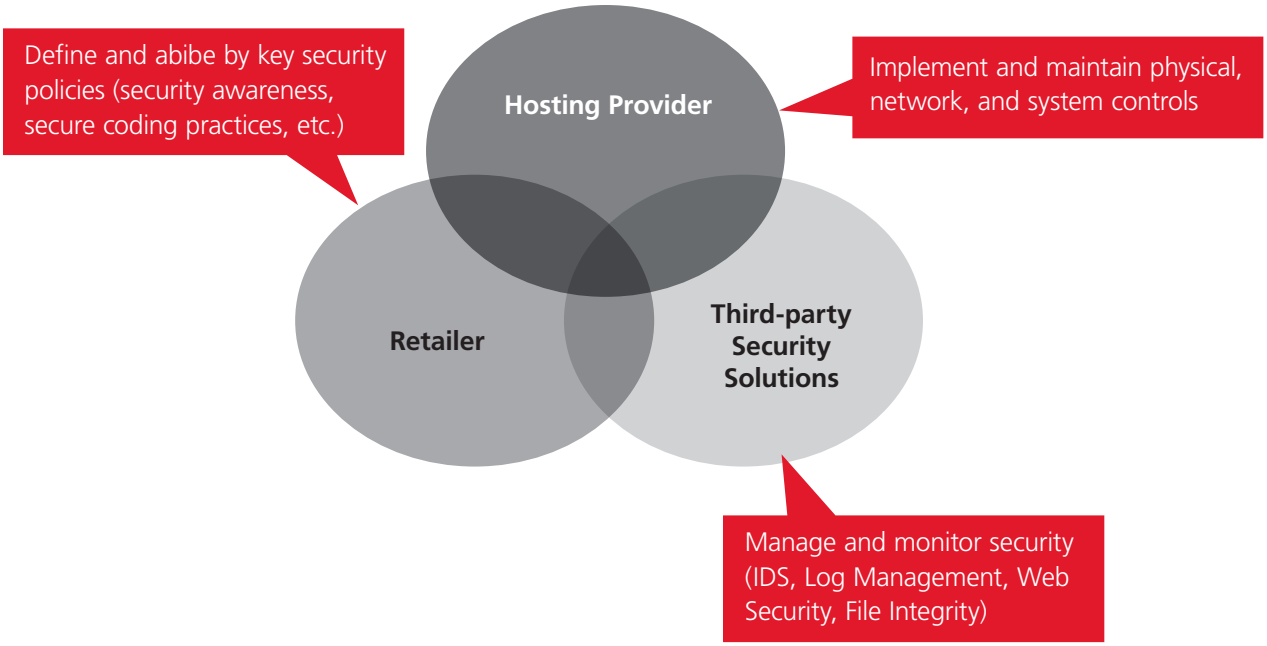
- Loss of customer confidence
- Lost sales and revenue
- Brand degradation or drop in public stock value
- Fines and penalties for non-compliance with PCI-DSS
- Termination of the ability to accept payment cards
- Fraud losses
- Cost of reissuing new payment cards
- Dispute resolution costs
- Cost of legal settlements or judgments

Don't Become A Statistic	
Strong authentication (VPN and 2-factor) mitigated 4 out of the top 5 hacking methods	Top 5 hacking methods: • **Exploitation of default or guessable credentials** • **Use of stolen log in credentials** • **Brute force and dictionary attacks** • Exploitation of backdoor and control channel • **Exploitation of insufficient authentication**
75% of victims were targets of opportunity[6]	Most victims of cyber attacks are 'targets of opportunity' (as opposed to victims of attacks aimed specifically for them)
78% of attacks were not highly difficult	21% of attacks examined in 2012 were deemed to be sophisticated, 4x as many as in 2011
94% of all data compromised involved servers	Server compromises increased significantly in 2011, up 18% compared to 2010
66% of breaches took months or more to discover/22% take months to contain	Most victims are unaware they have been compromised for months due to lack of detection tools or inconsistent auditing processes.
69% of incidents were discovered by a third party	
97% of breaches were avoidable through simple or intermediate controls	Most (97%) breaches are avoidable by utilizing simple or intermediate controls that customers should consider as more than just PCI-DSS controls, but as a good prescriptive standard for security.
96% of victims subject to PCI-DSS had not achieved compliance	

PARTNERING FOR PCI-DSS COMPLIANCE

Because of the complexity and necessity of maintaining PCI-DSS, many merchants opt to enlist solutions partners to provide the tools needed to build compliant infrastructure elements.

Even with partners involved, PCI-DSS compliance is a dual responsibility shared by you and your provider. Hosting with a provider that offers PCI-DSS-compliant infrastructure doesn't automatically make you compliant. For example, a simple coding mistake can still leave a business open to an exploit even with strong hosting and security partners. As you can see below, each entity bears responsibility:



4. Achieving PCI-DSS Compliance

QUESTIONS TO ASK:

1. **Has your bank contacted you about PCI-DSS or stipulated a date when they require compliance?**

   Why this is important: May determine how aggressive your compliance timeline needs to be.

2. **Have you contacted your Acquirer about PCI-DSS compliance?**

   Why this is important: The Acquirer is typically responsible for merchant compliance

3. **What payment brand compliance program (AMEX, Discover, JCB, MasterCard, Visa) will you subscribe to?**

   Why this is important: Each payment brand has it's own validation requirements

4. **What Self Assessment Questionnaire will you complete?**

   Why this is important: Seek assistance from a Qualified Security Advisor (QSA) to determine which PCI-DSS Data Security Standard **Self-Assessment questionnaire** fits your business processes.

5. **Are you a Service Provider, Merchant, or both?**

   Why this is important: To determine which validation requirements apply to your business.

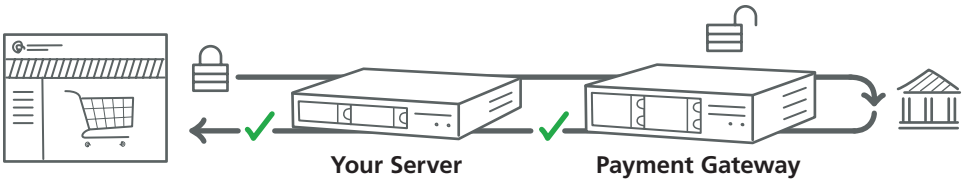
6. **Do you have the in-house resources to drive compliance?**

   Why this is important: To identify gaps and assess where partnerships bring the most value.

OPTIONS AVAILABLE:

The cornerstone of PCI-DSS is data protection. Your company policies and credit card transaction volume, along with other business factors not discussed here, should guide where you decide to store this data and how you protect it. Options to explore:

- Store credit card data at a provider offering PCI-DSS-compliant infrastructure.
- Store credit card information using a third-party payment gateway transmitting data server side using APIs. They collect the data and send it encrypted to your servers.



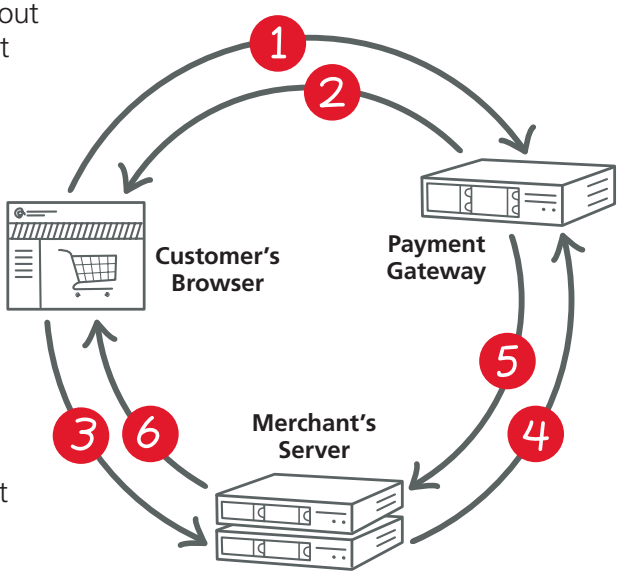
How it Works:

1. Upon the customer's request to checkout, a form is displayed to your customer to collect the required payment information. When the customer submits the form, the data is encrypted and then sent to your servers.
2. Using a client library, a server-to-server (S2S) call to payment gateway is made to complete the processing of the transaction.
3. The payment gateway processes the transaction and returns a response to your server.
4. This response can be used to display relevant data to the customer in the browser, such as the status of the transaction.

- Store credit card information using a third-party payment gateway transmitting data from the client browser before reaching your server.

How it Works:

1. Upon the customer's request to checkout, a form is displayed to your customer to collect the required payment information. When the customer submits the form, the data is posted directly to the payment gateway over an SSL connection.
2. The payment gateway then stores the data. Because the payment gateway redirects the customer back to your site without displaying any content, the customer never knows that they've even left your site.
3. The customer's browser requests the redirected URL from your site. The query string for the request URL contains a token that identifies the stored data from Step 1.
4. Using the client library, you make a server-to-server (S2S) call to payment gateway is made to complete the processing of the request. This step confirms that if the customer doesn't complete the redirect back to your site, the payment gateway will not complete the transaction.
5. After receiving the confirmation request, the payment gateway will run the transaction and send a response.



rackspace
the open cloud company

DECIDING BETWEEN STORING DATA IN-HOUSE OR USING PAYMENT GATEWAY

Compare the cost of using a third-party payment gateway with the cost of storing credit card information in your data center or a provider's data center. Compare these calculations to guide your decision:

- Calculate the cost of additional products/services required to store credit card data in-house per month. Rackspace can help you create sample configurations and provide estimates about cost.
- Calculate the cost of using a third-party payment gateway per month = number of transactions * cost of transaction charged by payment gateway + online revenue * % of revenue to be paid to payment gateway vendor.

If you find storing data on-site is more expensive than the gateway, consider moving to a gateway. If using the payment gateway is more expensive or a third party gateway is incompatible with other company policies, consider storing data in a PCI-DSS-compliant data center on dedicated servers.

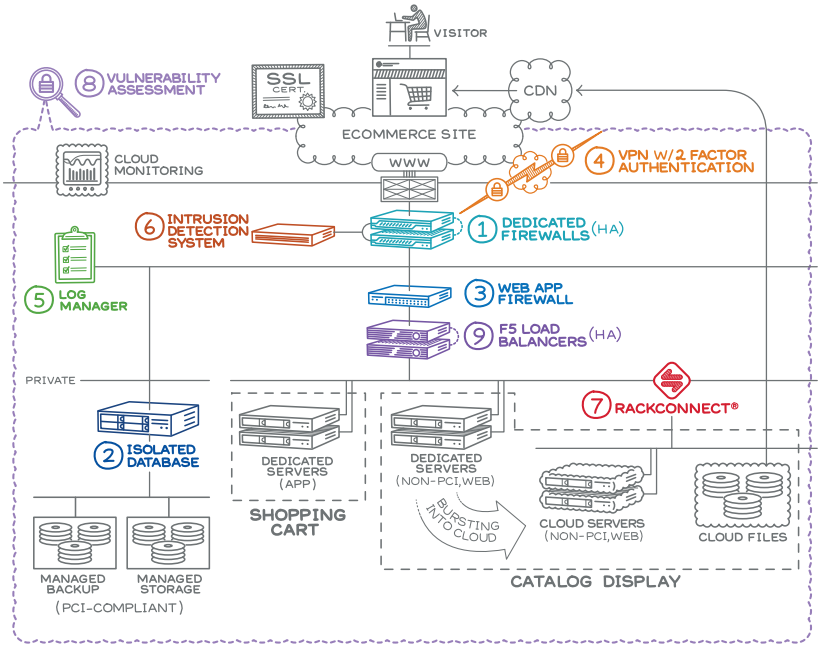
DECIDING BETWEEN TRANSMITTING DATA FROM THE SERVER OR BROWSER

Using APIs from client browsers excludes your server infrastructure from the scope of PCI-DSS compliance as all sensitive data is transmitted between the user and the payment gateway.

When you choose to transmit credit card information from the server side using third party payment gateway APIs, your server infrastructure becomes part of PCI-DSS compliance since sensitive data crosses your infrastructure.

PCI-DSS COMPLIANT SOLUTION FOR RACKSPACE DEDICATED HOSTING

Example of PCI-DSS-compliant reference architecture without a payment gateway:



rackspace
the open cloud company

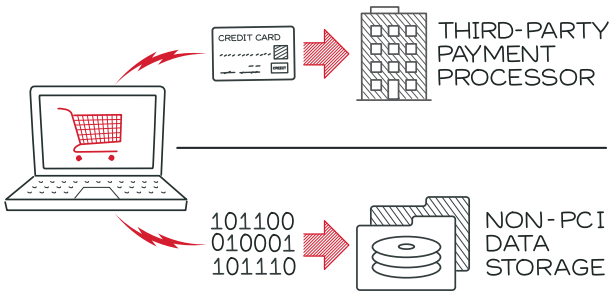
Use this table to align your PCI-DSS compliance needs with Rackspace services:

PCI–DSS Requirements	Rackspace Product/Service
Install and maintain a firewall configuration to protect cardholder data.	**Managed Firewall**: Rackspace Managed Firewalls provide the highest level of security earning ICSA Firewall and IPsec certification and Common Criteria EAL4 evaluation status. Working with a Rackspace Security Engineer you establish and are the sole owner of the set of rules that defines unwanted traffic. Based on this set of rules, information that is sent to your server is inspected and then filtered.
Do not use vendor-supplied defaults for system passwords and other security parameters.	**Vulnerability Assessment Services**: Alert Logic's Threat Manger is cloud-powered vulnerability assessment and intrusion detection service to defend and protect systems against internal and external threats.
Protect stored cardholder data.	Not applicable
Encrypt transmission of cardholder data across open, public networks	**SSL Certificates**: Installation and renewal service for six certificates from the two leading and most trusted names in the industry, VeriSign® and thawte™. Extended Validation (EV), organization validated (OV) and domain validated (DV) SSL certificates available.
Use and regularly update anti-virus software or programs.	**Managed Anti-virus**: Fully managed anti-virus solution offers proactive, sustained protection against viruses, worms, Trojans, spyware and other malware for Windows or Linux servers. Features Behavioral Genotype Protection TM for zero-day protection by proactively identifying malicious code on file servers and deleting it before it executes or reaches endpoint computers on your network.
Develop and maintain secure systems and applications.	**Web Application Firewall (WAF)**: Leverages industry-leading SecureSphere® & ThreatRadar technology from Imperva, the leader in web application security. The Rackspace WAF Service is fully supported by our Professional Services Team who deploys, tunes, profiles, troubleshoots and manages your device. Service also includes re-tuning your web application firewall as you make changes to your application.
Restrict access to cardholder data by business need-to-know.	**Managed Active Directory**: Rackspace Managed Servers with Intensive® Proactive Support include customized Active Directory management services.
Assign a unique ID to each person with computer access	**Two-factor Authentication**: Backed by industry-leading RSA SecurID technology, with a 20-year history of outstanding performance and innovation and a team of Rackspace CCSP- and RSA-certified professionals to fully manage your dedicated RSA SecurID appliance and tokens. Each RSA Authenticator token automatically generates a unique password every 60 seconds. Two-factor authentication using a unique PIN and the authenticator token password offers a more reliable level of user authentication than reusable passwords alone.
Restrict physical access to cardholder data	**Data Center Security**: Rackspace data centers are PCI-DSS and Safe Harbor compliant in addition to having SSAE16 Type II, SOC1, SOC2 (Security and Availability Only), and SOC3 audits on file for all data center facilities. Specific policies exist to both prevent unauthorized physical access, damage, and interference to our organization's premises and information and to confirm that only approved users are granted access to appropriate systems and resources.

PCI–DSS Requirements	Rackspace Product/Service
Track and monitor all access to network resources and cardholder data.	**Log Management**: The Alert Logic Log Manager™ automatically aggregates, normalizes, and stores log data from your environment to simplify log searches, forensic analysis, and report creation through real-time or scheduled analysis. LogReview, a service enhancement to Log Manager, provides daily event log monitoring and review by a team of Alert Logic security professionals.
Regularly test security systems and processes	**Threat Management**: The Alert Logic Threat Management™ system monitors your Rackspace environment, detecting external and internal threats. When it detects an incident, Alert Logic's ActiveWatch service provides expert guidance from its security operations center (SOC), staffed round the clock by Alert Logic security analysts. Integrated vulnerability scanning helps you identify possible points of entry and correct them, and assists you with meeting regulatory compliance requirements.
Maintain a policy that addresses information security for all personnel	Not applicable (Policy Management)

PCI-DSS-COMPLIANT SOLUTIONS FOR RACKSPACE CLOUD HOSTING

When you host your environment with Rackspace, you may also sign up with a separate payment processor to provide tokenization—replacing credit card data with meaningless numbers or "tokens." When you accept a payment, non-PCI-DSS data routes to your Rackspace-hosted environment, while the tokenized credit card data routes to your payment processor.



Since your customers' credit card data does not route to your Rackspace hosted infrastructure—only the payment processor—your Rackspace environment stays out of the scope of your PCI-DSS requirements.

Check out **Rackspace Cloud Tools partners** for Rackspace-recommended payment gateway services:

Stripe: A simple, developer-friendly way to accept payments online. Stripe handles custom payment forms, storing cards, subscriptions, and direct payouts.

- Best fit: Developers building payment applications using APIs
- Pricing: 2.9% + 30¢ per successful charge*

Learn More

Braintree: Braintree is a full-stack payments platform for mobile apps and websites. The service provides merchant account, payment gateway, recurring billing and credit card storage including one-touch payments to mobile SDKs and foreign currency acceptance.

Braintree

- Best fit for: Developers building payment applications using APIs
- Pricing: 2.9% + 30¢ per successful charge*

Learn more

rackspace
the open cloud company

PayPal: With more than 123 million active accounts in 190 markets and 25 currencies around the world, PayPal enables global commerce via mobile devices and in store. Service features automatic fraud screening, Seller Protection Policy, and the BillMeLater® financing option.

- Best fit for: Handling international currencies
- Pricing: 2.9% + 30¢ per successful charge*

Learn more

*pricing and features noted as of writing of this paper

Conclusion

A key step to a successful compliance program is the establishment of continuous management of the people, processes and technology. It is a common misconception for many small and large organizations that investing solely in technologies will solve their security and compliance requirements. Technologies like firewalls, Intrusion Detection Systems (IDS) and log management appliances are only as effective as the people and processes in place to install and manage them.

This is a lesson that Transport for London (TFL), responsible for managing transport services across England's capital city, learned while trying to achieve PCI-DSS compliance for its travel payment system. Their system was handling up to 40,000 visits per day with over 2.5 million registered users. Being a 24-hour business, 365 days of the year, they couldn't risk a breach or other outage disrupting operations. They turned to Rackspace for the pieces of the puzzle they needed to become fully compliant. "It is probably true to say that without the considerable amount of help from Rackspace we could not have passed the exceptionally stringent PCI-DSS audit. Rackspace certainly went above and beyond their remit to ensure that everything was perfect for us," says Aingaran Somaskandarajah, Technical Lead, Oyster Card.

Let Rackspace be your trusted partner in the PCI-DSS journey. We can help you navigate the maze with infrastructure and solution requirements to help reduce the scope and complexity of your compliance efforts. **Contact us today to discuss your needs or explore PCI-DSS-Compliance services now.**

References:

1 http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

2 http://www.verizonenterprise.com/DBIR/2013/

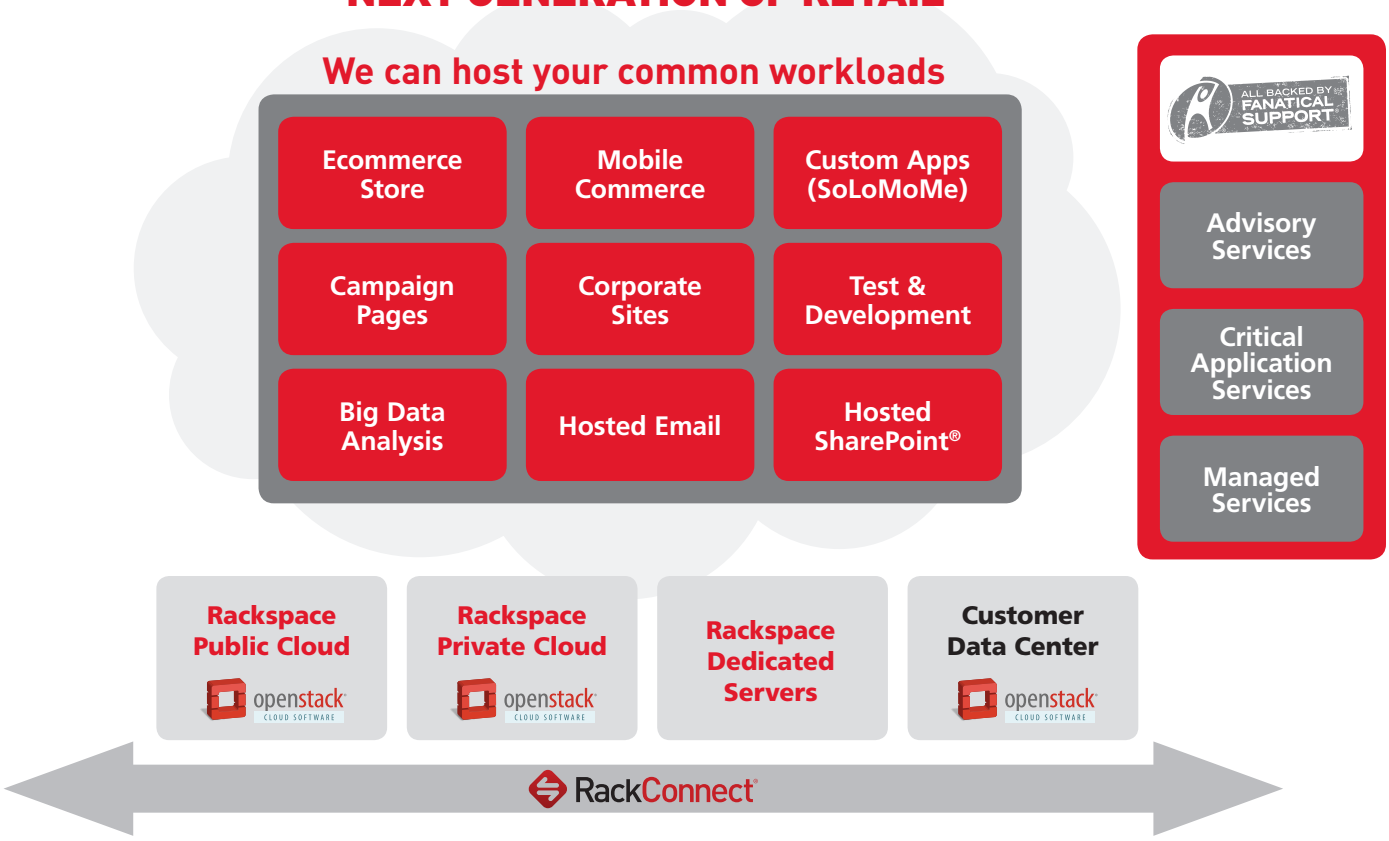
3 http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

4 https://www.pcisecuritystandards.org/merchants/self_assessment_form.php

5 https://www.pcisecuritystandards.org/merchants/self_assessment_form.php

6 http://www.verizonenterprise.com/DBIR/2013/

ENABLING YOUR JOURNEY TO THE NEXT GENERATION OF RETAIL



rackspace® the open cloud company

About Rackspace

Rackspace® Hosting (NYSE: RAX) is the open cloud company, delivering open technologies and powering hundreds of thousands of customers worldwide. Rackspace provides its renowned **Fanatical Support®** across a broad portfolio of IT products, including Public Cloud, Private Cloud, Hybrid Hosting and Dedicated Hosting. The company offers choice, flexibility and freedom from vendor lock in.

GLOBAL OFFICES

Headquarters Rackspace, Inc.
1 Fanatical Place | Windcrest, Texas 78218 | 1-800-961-2888 | Intl: +1 210 312 4700
www.**rackspace**.com

UK Office
Rackspace Ltd.
5 Millington Road
Hyde Park Hayes
Middlesex, UB3 4AZ
Phone: 0800-988-0100
Intl: +44 (0)20 8734 2600
www.rackspace.co.uk

Benelux Office
Rackspace Benelux B.V.
Teleportboulevard 110
1043 EJ Amsterdam
Phone: 00800 8899 00 33
Intl: +31 (0)20 753 32 01
www.rackspace.nl

Hong Kong Office
9/F, Cambridge House, Taikoo Place
979 King's Road,
Quarry Bay, Hong Kong
Sales: +852 3752 6465
Support +852 3752 6464
www.rackspace.com.hk

Australia Office
Level 4, 210 George Street,
Sydney, NSW 2000
Phone: 1-800-722577
www.rackspace.com.au

rackspace
the open cloud company