Accelerating PCI Compliance
PCI Compliance for B2B Managed Services

March 8, 2016
What’s the Issue?
Credit Card Data Breaches are Expensive for Everyone

The Wall Street Journal

Cost of Replacing Credit Cards After Target Breach Estimated at $200 Million

By SAABIRA CHAUDHURI
Updated Feb. 18, 2014 5:58 p.m. ET

Costs associated with the recent security breach involving credit cards used at Target Corp. have topped $200 million for financial institutions, according to data collected by the Consumer Bankers Association and the Credit Union National Association.

Home Depot credit card security breach could cost $3B

Security firm BillGuard estimates 60 million accounts could be affected

PCI Compliance for Managed Services

- Firewall configuration employed
- No vendor-supplied defaults for system passwords
- Stored data protected by encryption using Oracle Transparent Data Encryption and encryption key management provided by Oracle Wallet
- In-flight transmission of cardholder data encrypted
  - PCI token to replace PAN
  - Other PCI data masked
- Regularly updated antivirus software
- Secure systems and applications
- All network access tracked and monitored
- Regular system and processes tests
How We Deliver Compliance

- Purchase Order with PCI
- HTTP/S SFTP
- GATEWAY
- PCI Data Tokenized
- PCI Data Tokenized processed through Trading Grid
- Tokenized data stored in an encrypted store
- Original data restored for delivery
- PCI
- HTTP/S SFTP
- GATEWAY
- Purchase Order with PCI
How We Deliver Compliance

Customer’s B2B Managed Services implementation never sees the original data!

1. Purchase Order with PCI
2. HTTP/S SFTP
3. GATEWAY
4. Tokenized data processed through Trading Grid
5. PCI Data Tokenized
6. ENCRYPTED STORE
7. Original Data Restored for Delivery
How We Deliver Compliance

- **Purchase Order with PCI**
- **HTTP/S SFTP**
- **GATEWAY**
- **OPENTEXT Trading Grid™**
  - Tokenized data processed through Trading Grid
- **TOKEN**
- **B2B MANAGED SERVICES**
- **CC# can be tokenized to 12 random digits + last 4 digits**
  - No map changes required!
- **PCI Data Tokenized**
- **ENCRYPTED STORE**
- **Original Data Restored for Delivery**
- **GATEWAY**
- **HTTP/S SFTP**
- **Purchase Order with PCI**
Key Benefits

**Ensure a secure network**
OpenText’s world-class data centers ensure networks, firewalls, and routers comply with PCI DSS standards, without investing in additional infrastructure.

**Encrypt transmission of cardholder data**
Safely transmit sensitive cardholder data with strong encryption for authentication and transmission.

**Protect cardholder data**
Render Primary Account Number (PAN) unreadable and easily mask other personally identifiable data with a PCI token.

**Maintain a vulnerability management program**
Protect against malicious attacks with regular updates to anti-virus software and the latest security patches.

**Implement strong access control standards**
OpenText manages access control with restricted system access, robust user security protocols and limited physical access to systems in the cardholder data environment.

**Track and monitor networks**
OpenText tracks and monitors access to network resources, regularly performs penetration testing, and maintains a strong information security policy.
Delivering Return-on-Investment

Reduce costs
Eliminate the need to invest in additional infrastructure, maintenance and personnel to support cardholder data protection in your B2B network

Minimize disruption
No modifications to existing file layouts or data maps are required to protect personally identifiable cardholder data elements

Limit PCI audit scope
Outsourcing cardholder data protection limits the number of PCI requirements for your organization

Keep current
OpenText manages software updates, implements annual encryption key changes and stays abreast of the latest revisions to PCI data security standards

Simplify complexity
OpenText Managed Services with PCI compliance is your single-source provider for B2B outsourcing combined with cardholder data security