



Synxis PCI Compliance

Tuesday, April 15, 2008

Tom Murray
Vice President of Technology

SynXis PCI – Agenda

Company Overview

Why PCI - Drivers

Synxis PCI History

PCI Challenges

2008 Objectives

Lessons Learned

SynXis – Company Overview

History

- Founded 1996
- Provide **RedX** Distribution Management System via SaaS model
 - A Web-based Central Reservations System
- Year over year growth and a recognized industry innovator
- Acquired by Sabre Holdings in January 2005
- Approx. 8,000 properties in over 100 countries

Management

- Seasoned management team with impressive hospitality, operations, and technology backgrounds
- International organization with offices in USA, Europe, South America and Asia

SynXis Mission

“Energize and optimize hotel distribution and marketing”

Who is Sabre Holdings?

- The world leader in travel commerce, retail travel products and providing distribution and technology solutions for the travel industry.
- A privately held company recently acquired by Silver Lake Partners and Texas Pacific Group, private equity firms.

Businesses include:    

Quick Facts

- Headquartered in Southlake, Texas
- 9,000 employees in 52 countries
- \$80 billion of travel products and services sold through Sabre systems
- 2007 total revenue approximately 3 billion (USD)



lastminute.com

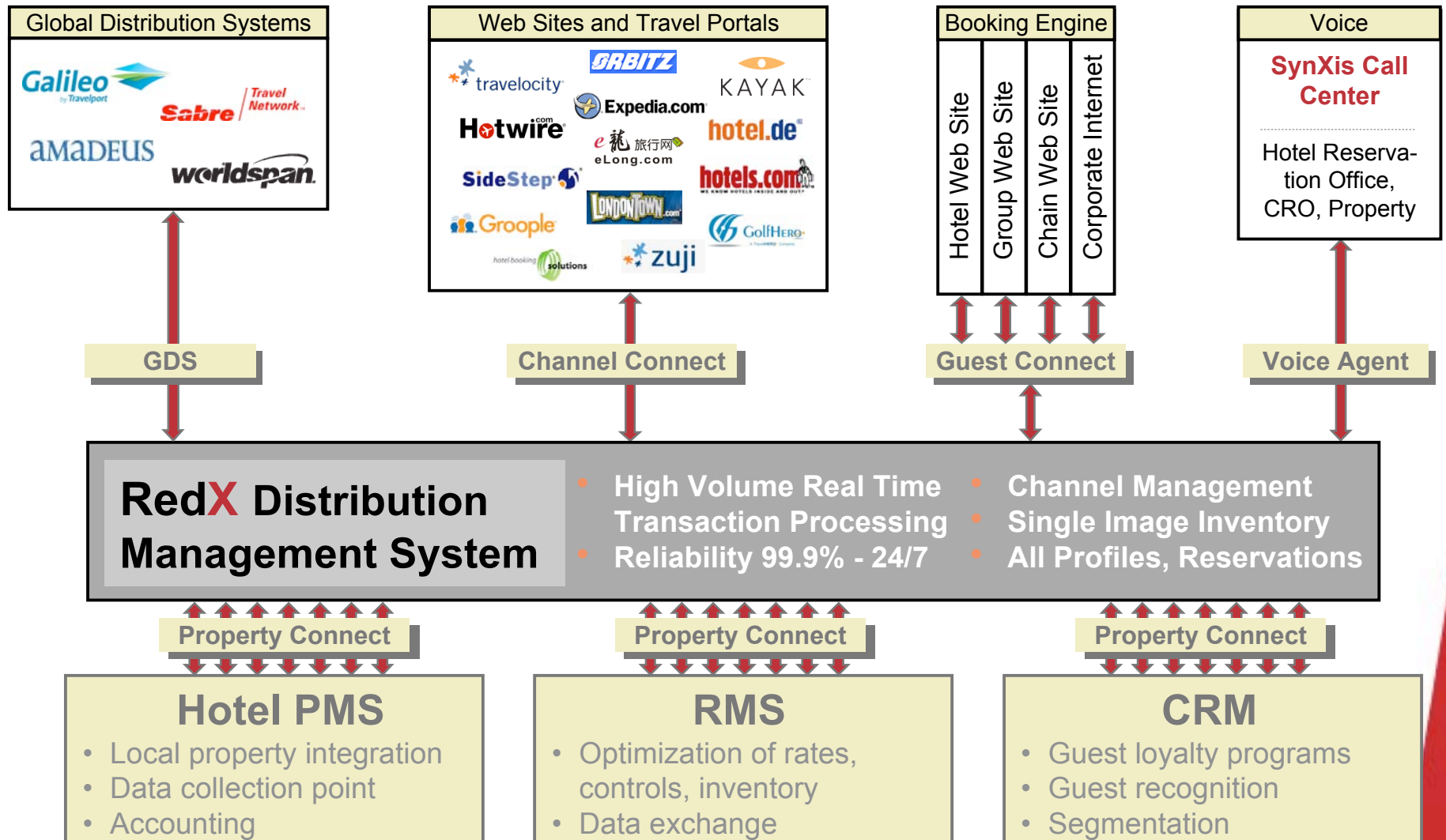
neXion



site 59



SynXis Distribution Landscape



SynXis' Customers



CONFIDENTIAL



MANDARIN ORIENTAL
THE HOTEL GROUP



The Sutton Place Hotels



SONESTA COLLECTION
HOTELS • RESORTS • CRUISES



SynXis – What is PCI?

Payment Card Industry (PCI) Data Security Standard
Requirements for protection of Payment Account Data Security
Standard Published by PCI Security Standards Council

- **VISA, MasterCard, Discover, American Express & Others...**

Twelve Requirement spanning;

- **Security Management**
- **Policies**
- **Procedures**
- **Network Architecture**
- **Software Design**
- **And other areas**

<https://www.pcisecuritystandards.org/index.htm>

http://usa.visa.com/merchants/risk_management/cisp.html

SynXis – Why PCI Compliance?

Customer Drivers

Growing Awareness of PCI

Pressure from Financial Institutions

Requiring Contractual Commitments for compliance

Internal Drivers

Protect Customer Data

Adherence to Best Practices in Network, Data and Application Security

Corporate Objective for Sabre Holdings

Payment Authorization in the Future

Competitive

SynXis PCI - History

Level 2 Service Provider per VISA CISP

Any service provider that is not in Level 1 and stores, processes, or transmits more than 1,000,000 VISA accounts/transactions annually.

- *We do 6,000,000+ bookings per year*
- *We do not process payments – but hold CVV for 48 hours*
- *Third Party Audit required*

PCI self-assessment in mid 2006

Third Party Audit started late 2006

Audit completed December 2007

**AMEX DSOP (Data Security Operating Procedure)
compliance certified in December, 2007**

**PCI Report On Compliance (ROC) accepted by VISA, January
2008**

SynXis PCI – Challenges

General

Interpretation of Standard

- **Contracted for Informal Review of self assessment and network environment**
 - Validated strategy for Gap Closure & compensating controls

Resources

Significant Effort and Impact across Technology organization

Network / Infrastructure

Mostly Minor – but time intensive

- **E.g. Firewall Rules to be most restrictive**

Quarterly Network Vulnerability Scanning

Process

Documentation, Formalization and Education

SynXis PCI – Challenges

Data

Enhanced Encryption of Sensitive Data

- **Upgraded to Triple DES Encryption in business layer**
- **24 Hour Purging of CVV**
- **Credit card details purged 60 days after departure**
- **Removal of Credit Card Information from all logs**
- **Masking of Credit Card Information in all reports**
- **Masking of Credit Card information on most pages**
 - Viewable via a single web page with explicit viewership
- **Implementation of encryption key management application**
 - Version Key management
 - Split master key

SynXis PCI – Challenges

Application

Identifying & Eliminating Application Vulnerabilities

- **Contracted a Third Party Application Vulnerability Scan to satisfy PCI – clean**
- **Third Party Scans for each new product release (4x annual) as an alternative to code reviews**
- **Developer Education on Open Web Application Security Project (OWASP) standards and best practices**

Third Party Connectivity

Reviewed all third party connectivity (OpenTravel, HTNG, other)

- **Over 60 different interfaces**

All communications via HTTPS – Satisfies PCI

No OpenTravel Schema or coding Impact

SynXis PCI – 2008 Objectives

Ongoing

Quarterly internal Reviews to maintain compliance

Quarterly Network Vulnerability Scans

Application Vulnerability Scans for each new release

Planned

Moving from Service Provider to Merchant

- Introduction of Payment Processing in 2008
- Evaluating Payment Applications Best Practices (PABP) Standard

Preparing for 2008 Audit

- Moving Data Center

Evaluating Message level encryption & other enhancements

- Monitoring OpenTravel

Evaluating Application Firewalls

SynXis PCI – Lessons Learned

Larger Than Expected Effort

PCI affects all aspects of the environment

- Application
- Database
- Network
- Administrative / Hiring
- Procedures and Processes

Need realistic resource allocation and commitment

Project Planning

Consulting Assistance Valuable

Minimal Hours

Interpretation and Clarification of the Standard

Validation of Remediation Plan for Gaps

SynXis PCI – Lessons Learned

Worth It

Enforces Best Practices

Results in a More Secure Environment

- Benefits Customers
- Benefits Synxis

PCI is a continuous Effort

Quarterly Scans

Quarterly Reviews

Annual Audits



Questions?