UNIVERSITY OF PIRAEUS,

SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGIES,

DEPARTMENT OF DIGITAL SYSTEMS,

SYSTEMS SECURITY LABORATORY,

POSTGRADUATE PROGRAMME "DIGITAL SYSTEMS SECURITY"

Master Thesis

COMPLIANCE OF AN AIRLINE COMPANY WITH THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS): CASE STUDY

Delga Aggeliki

Piraeus, November, 2014

SUPERVISOR

Professor
Sokratis K. Katsikas
University Of Piraeus

EXAMINATION BOARD

Professor
Sokratis K. Katsikas
University Of Piraeus

Associate Professor
Konstantinos Lambrinoudakis
University Of Piraeus

Assistant Professor
Christos Xenakis
University Of Piraeus

Abstract

The Payment Card Industry Data Security Standard is a set of twelve security requirements that applies to all institutions and systems handling, storing or transmitting cardholder information. It was created by the main card brands in a united effort to respond to the increasing number of attacks and data breach cases targeted and linked to card and cardholder data. The standard considers points such as policy design, data security, network architecture, software design, application security, transmission encryption requirements and so on.

Being compliant with the standard can be both expensive and time consuming for any business willing to do so. Given the complexity of the business environment of Airline Companies, the cost for compliance increases. Airline companies operate differently to other merchants due to the involvement of multiple entities during the whole process, which initiates from the customer's purchase of a ticket and ends at customers boarding to the airplane. These entities, including travel agencies, airline companies, airports, as well as service and network providers, that check seats availability, issue tickets, process payments and so on, may have access to cardholder data and consequently may pose great risk for security of cardholder data.

Cardholder data are often used for functions, other than completing the payment. For instance, many airlines use payment card data as a unique form of identity for their customers. Card data is passed through systems at the time of reservation and then used at check-in to verify the customer's identity. Moreover, travel agents use systems provided by a Global Distribution System (GDS) provider that link to the airline systems to check ticket availability, to financial systems for authorisation and then to IATA (International Air Transport Association) systems for clearing and settlement purposes.

This is a case study, based on a real situation, where the current state of an airline company (infrastructure, applications, information security policies and procedures) is going to be evaluated against the requirements of the Payment Card Industry Data Security Standard (PCI DSS) and recommendations will be made in order for the company to comply with the standard. Moreover, the present study is going to analyze in depth the difficulties that arise towards compliance with the PCI DSS standard in the airline industry from the involvement of multiple entities and to make suggestions, requiring the smallest possible cost and effort for the organization, that can help to overcome such difficulties.

Acknowledgements

I would firstly like to thank my supervisor, Mr. Sokratis Katsikas for his contribution, by providing me with assistance and helpful guidelines during the development of this dissertation. In addition, I would like to thank Encode S.A. and especially my Manager Mr. Charalambos Paganos and my colleagues Mr. Emmanuel Fragkos and Mr. Lampros Patseas, whose contribution enabled me to develop a better understanding of the subject and were always available anytime I needed their help. Finally, I would like to thank my friends and family for their support throughout this effort.

Table Of Contents

Table of Figures

0. Introduction

During the second half of the twentieth century, payment cards have quietly revolutionized on how products and services are paid.[1] Practices like paying for an article with a click of a mouse, settling an auction purchase via an e-mail account, buying an electronic ticket using a mobile phone, seem very attractive, promising high convenience, flexible use and high transaction speed.[2] While more and more payment card businesses come to life globally and the use of credit and debit cards is rapidly increasing, security has become an important concern. Failure to secure the card information can cause a major damage to the organization in terms of financial fraud, identity theft, legal regulations, loss of consumer confidence, etc.[3]

Over the last years, more and more cyber-attacks come to the forefront, leading to serious data losses and financial damages. One of the biggest data security breach in history, was that of Sony's PlayStation Network. On April of 2011, Sony suffered a massive breach in its video game online network, in which names, addresses, credit card data belonging to 77 million user accounts, were compromised. The data breach lead to outage of the online gaming network for over a week and cost Sony millions of dollars.[4] Sony stated that the credit card data was encrypted, but attackers claimed to have sold them online. In case data was indeed encrypted, the level of protection offered by the encryption mechanism, allowed attackers to decrypt them.[5]

Another high-profile incident was that of TJX Companies Inc. where it was estimated that 45.6 million credit and debit cards numbers were stolen from one of its systems during a period of several months by an identified number of intruders.[6] In depth, TJX's systems where intruded in July 2005 for the first time, followed by further unauthorized accesses later in 2005, 2006 and even once in mid-January 2007 after the breach had already been discovered. However, no further data seem to have been stolen after the 18th of December. This breach not only affected TJX customers but also customers of other stores throughout U.S, Puerto Rico, Canada and U.K. The company didn't manage to find out what kind of data was stolen because the accessed data was deleted by the company in the normal course of the business. TJX had to deal with large financial penalties, several lawsuits filed against it as well some severe reputation damage.[7]

In response to the alarming increase of payment card fraud incidents, the major credit card brands (i.e. Visa, MasterCard, American Express, Discover and JCB) collaborated to develop the Payment Card Industry Data Security Standard (PCI DSS), aiming to reduce the payment card data theft. PCI DSS was published on 2004 and has undergone a number of revisions until today. As a general guideline, the PCI standard applies to any company that accepts payments for services or goods with payment cards.[8]

The present thesis presents the process that an Airline company follows in order to comply with the Payment Card Industry Data Security Standard and the challenges that faces during this process, given the special nature of the industry.

The thesis is structured in overall six chapters, including the abstract, acknowledgements, glossary and bibliography, as follows:

In the first chapter, the Payment Card Industry Data Security Standard (PCI DSS) is presented, along with the history and evolution of the standard, the merchant levels and validation requirements.

The second chapter contains an overview of the payments in the Airline industry, the process that is followed and the entities involving in the process.

In the third chapter, the motivation and scope of the present thesis are explained.

The case study of the present thesis is sited in the fourth and the fifth chapter. The fourth chapter provides intelligible and detailed information about the Cardholder Data Environment scope of the Airline company subject of this case study. The chapter encompasses detailed information about the

cardholder data flows over the Airline's networks, the identified Cardholder Data Environment system components and the cardholder data "locations", both in electronic & paper based format.

The fifth chapter illustrates the difficulties that the Airline is going to face in order to comply with PCI DSS given the current status, identifies areas for improvement and presents certain suggestions that if implemented, will significantly reduce the PCI DSS scope and consequently the required effort and cost for compliance.

In the final chapter, chapter six, conclusions are exported depicting the difficulties that an airline faces in order to achieve a full compliance with the standard and steps forward, that the entire industry could make regarding PCI DSS, are proposed.

1. The Payment Card Industry Data Security Standard (PCI DSS)

1.1 What is PCI DSS ?

A quick answer to the question "What is PCI-DSS?" would be that it is a security standard which has been created by the **PCI Security Standards Council (PCI SSC)** in 2004, which consists of the major payment brands (Visa International, MasterCard Worldwide, American Express, JCB and Discover Financial Services), in order to reduce losses from fraud and data theft. According to the official site of PCI Security Standards Council, "*PCI Security Standards Council is an open global forum for the on-going development, enhancement, storage, dissemination and implementation of security standards for account data protection*".[9] The goal of the council is to enhance payment account security by carrying forward broad adoption of the PCI Security Standards.[10]

Entities interested to comply with PCI DSS must follow and satisfy a set of requirements which offer a solid step to the protection of cardholder's data. PCI DSS establishes the following six high level objectives, broken down further into twelve requirements [11], [12], covering the protection of cardholder data both at a procedural and technical level.

Build and Maintain a Secure Network and Systems	**1.** Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update anti-virus software or programs
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know
	8. Identify and authenticate access to system components
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel

Figure 1 - PCI Data Security Standard – High Level Overview [12]

PCI DSS is focusing on the protection of account data which consists of cardholder data and / or sensitive authentication data, whether it is stored or transmitted. Cardholder data contain any personal identifiable data connected with a cardholder. This would be the cardholder's name and address, PAN (Primary Account Number or also for short Card Number), expiration date and service code. If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment, they must be protected in accordance with all PCI DSS requirements except certain encryption requirements, which apply only to

PAN. Account data also include Sensitive Authentication Data (SAD) which would be the full magnetic stripe data, card validation codes/values that includes (CAV2/CVC2/CVV2/CID1), PINs and PIN blocks. As shown on the figure below, this type of data must not be stored post authorisation, even if encrypted.[13]

		Data Element	Storage Permitted	Render Stored Unreadable per Requirement 3.4
Account Data	**Cardholder Data**	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data	Full Track Data	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

Figure 2 - Storage of commonly used elements of Cardholder and Sensitive Authentication data [12]

1.2 History and Versions of the Standard

Long before the creation of PCI DSS, in the 1990's, market's most well-known payment card brands (American Express, Discover Financial Services, MasterCard, Visa and JCB International) had developed various standards in order to safeguard their sensitive information.[14] Before the foundation of PCI DSS, each company had its own program to deal with the arising problems. In June 2001, Visa USA launched its own program named Cardholder Information Security Program (CISP).[15] Such kind of programs was also developed by the rest credit card companies to shield their sensitive data. American Express developed a program called Data Security Operating Policy (DSOP), the Discover program is called Discover Information Security and Compliance (DISC) and finally MasterCard program was called MasterCard Site Data Protection (SDP).[16]

On December 15, 2004 these companies aligned their policies and formed the Payment Card Industry Security Standards Council or PCI SSC which in turn created PCI DSS. Version 1.0 as well as other supporting documents was also released with the creation of PCI DSS. Later in September 2006 after a few revisions and clarifications which led to minor modifications, Version 1.1 was released.[17] One important section of this version was Section 2.2, referring to the development of configuration standards for all the components of the system to certify that these standards are applying all the possible issues and are following the best practices standards. Another addition was Section 4.1.1 which focuses on the transmission of cardholder data via the Internet through wireless connections.

PCI SSC announced on October 2008 the release of the new version 1.2 of PCI DSS, introducing more in depth explanations to merchant's queries, intending to offer better comprehension of the security challenges.[18] This version was introduced after the Council requested feedback from the organizations that were participating in order to find out ambiguities in the stated requirements. After the release of a new version, changes to the PCI DSS follow a defined 24-month lifecycle consisting of five stages. The lifecycle ensures a gradual, phased use of new versions of the standard without invalidating current implementations of the PCI DSS or putting any organization out of compliance the moment changes are published. With the release of PCI DSS version 1.2 the Council became committed to following this process to ensure transparency and continuity of compliance. Except from this one, Version 1.2 didn't introduce any major changes to the twelve requirements.

Next was Version 1.2.1, released on August 2009 which suggested a few minor changes to all previous forms of PCI DSS, PED and PA-DSS.[19] These changes were characterized as "administrative in nature". They were mainly constituted by redundant lines elimination, language updates for better comprehension, as well as the attachment of supportive documents and spelling corrections.[20]

On October 2010, Version 2.0 was created that applied to PCI DSS, PED and PA-DSS. All merchants were required to comply with its requirements until January 2011.[21] There were as many as one hundred –thirty changes to the documents that were based on the feedback received by the major card companies and participating organisations. The changes focused on further clarification of the twelve requirements, extra guidance and evolution of the requirements.

On November 2013, Version 3.0 was introduced.[22] The updated introduced more changes than Version 2.0 but the core 12 security areas remained the same. However, the updates included several new sub-requirements that did not exist previously. Due to the fact that additional time may be required for implementation of the new sub-requirements, the Council introduced future implementation dates accordingly, meaning that until 1 July 2015 some of these sub-requirements remain best practices only.[23]

In conclusion, the management, development, maintenance, clarification and revision of PCI DSS are tasks that have been established by the Payment Card Industry Security Standards Council.

1.3 Who is subject to compliance?

The Payment Card Industry Data Security Standard (PCI DSS) applies to everyone that processes credit or debit card data, including third parties such as service providers and merchants that store, process and/or transmit payment card data. Anyone that accepts payment cards (e.g. credit, debit or pre-paid cards) as a form of payment is required to comply with PCI DSS, otherwise failure to comply can result in fines and penalties. While non-compliance penalties vary among major credit card networks, they can be substantial. Participating companies can be barred from processing credit card transaction, higher processing fees can be applied and in the event of a serious security breach, unaffordable fines can be levied for each instance of non- compliance.[24]

The standard is applicable to merchants, service providers, payment processors and financial institutions. Merchants are defined as any company that receives a card payment in exchange of a good or service. Service Providers are companies that process, store or transmit cardholder data on behalf of merchants or other service providers. Service providers are also considered to be companies that provide services that control or could impact the security of cardholder data.[25] In the context of PCI a service provider could be managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. The basic component that determines whether an entity is required to comply with PCI DSS is if they store, process, or transmit cardholder data through any payment channel, including brick-and-mortar, mail, telephone, e-commerce.[13]

1.4 Merchant and Service Provider Levels

In order for an entity to become PCI DSS compliant, each payment brand had set their own criteria for assigning merchants compliance validation level. Merchant levels are defined by the payment brands and determined by the acquirer or by the payment brand where it is an acquirer. Based on that, organisation may be assigned a different payment level for different payment brands. The final decision for the merchants' validation level lies to the acquirers, since they are shouldered the merchants' compliance. The levels are assigned depending on the number of transactions the merchant or service provider process annually. The table below illustrates the different merchant levels as defined by each payment brand.

Level	Visa	AMEX	Discover	JCB	MasterCard
1	Merchants processing over 6 million Visa transactions annually (all channels), or global merchants identified as Level 1 by any Visa region.	Merchants processing over 2.5 million AmEx card transactions annually or any merchant that AmEX otherwise deems a Level 1.	Merchants processing over 6 million card transactions annually on the Discover network. Any merchant Discover determines to be a Level 1. Merchants required by another payment brand to validate and report as a Level 1.	Merchants processing over 1 million JCB International transactions annually, or compromised merchants.	Merchants processing over 6 million total combined MasterCard and Maestro transactions annually. Merchants that have experienced an account data compromise. Any merchant that MasterCard otherwise deems a Level 1. Any merchant meeting the Level 1 criteria of Visa.
2	Merchants processing 1 million to 6 million Visa transactions annually (all channels)	Merchants processing 50,000 to 2.5 million AmEx transactions annually.	Merchants processing 1 million to 6 million card transactions annually on the Discover network. Merchants required by another payment brand to validate and report as a Level 2 merchant.	Merchants processing less than 1 million JCB International transactions annually.	Merchants with greater than 1 million but less than or equal to 6 million total combined MasterCard and Maestro transactions annually. Any merchant meeting the Level 2 criteria of Visa.
3	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually.	Merchants processing less than 50,000 American Express transactions annually.	Merchants processing 20,000 to 1 million card-not-present only transactions annually on the Discover network. Merchants required by another payment brand to validate and report as a Level 3 merchant.	N/A	Merchants with greater than 20,000 combined MasterCard and Maestro e-commerce transactions annually but less than or equal to one million total combined MasterCard and Maestro ecommerce transactions annually. Any merchant meeting

Level	Visa	AMEX	Discover	JCB	MasterCard
					the Level 3 criteria of Visa.
4	Merchants processing less than 20,000 Visa e-commerce transactions annually, and all other merchants processing up to 1 million Visa transactions annually.	N/A	All other Discover Network merchants.	N/A	All other MasterCard merchants.

Figure 3 – PCI DSS Merchant Levels [26], [27], [28], [29]

The table below illustrates the different levels for Service Providers, as defined by each payment brand.

Level	Visa	AMEX	Discover	JCB	MasterCard
1	VisaNet processors or any service provider that stores, processes and/or transmits over 300,000 transactions per year.	Service Providers processing over 2.5 million AmEx card transactions annually or any service provider that AmEx otherwise deems a Level 1.	All Service Providers, including but not limited to: third party Processors (TPPs) and Payment Service Providers (PSPs) are expected to meet the same validation and reporting requirements.	All TPPs are expected to meet the same validation and reporting requirements.	All TPPs. All DSEs that store, transmit, or process greater than 300,000 total combined MasterCard and Maestro transactions annually. All compromised TPPS and DSEs.
2	Any service provider that stores, processes, and/or transmits less than 300,000 transactions per year.	Service Providers processing 50,000 to 2.5 million AmEx transactions annually.	N/A	N/A	All DSEs that store, transmit, or process less than 300,000 total combined MasterCard and Maestro transactions annually.
3	N/A	Service Providers processing less than 50,000 AmEx transactions annually.	N/A	N/A	N/A

Figure 4 - PCI DSS Service Provider Levels [29]

1.5 Validation Requirements

Depending on their PCI DSS compliance level, merchants and service providers are required to validate and report their PCI DSS compliance to their acquirer (for merchants) or payment brands (for service providers). Validation requirements might include an Annual On-Site Security Assessment for Level 1 merchants (conducted by a Qualified Security Assessor – QSA), Annual Self-Assessment, and Quarterly Network Scans (performed by an Approved Scanning Vendor – ASV). It has to be noted that each payment brand has its own set of validation and reporting requirements. The table below provides an overview of merchant validation requirements as defined by each Payment Brand.[13]

Level	Visa	AMEX	Discover	JCB	MasterCard
1	• Annual onsite assessment by QSA. • Quarterly network scans by ASV. • Attestation of compliance form.	• Annual onsite assessment performed by QSA or merchant if certified by the CEO, CFO, CISO or principal of the merchant. • Quarterly network scans by ASV.	• Annual onsite assessment by QSA or merchant's internal auditor. • Quarterly network scans by ASV.	• Annual onsite assessment by QSA • Quarterly network scans by ASV.	• Annual onsite assessment by QSA. • Quarterly network scan by ASV.
2	• Annual self-assessment questionnaire (SAQ). • Quarterly network scans by ASV. • Attestation of compliance form.	• Annual SAQ performed by the merchant and certified by the CEO, CFO, CISO, or principal of the merchant. • Quarterly network scans by ASV.	• Annual SAQ. • Quarterly network scans by ASV.	• Annual SAQ. • Quarterly network scans by ASV.	• Annual onsite at merchant discretion. • Quarterly network scans by ASV.
3	• Annual SAQ. • Quarterly network scans by ASV.	• Annual SAQ. • Quarterly network scans by ASV.	• Annual SAQ. • Quarterly network scans by ASV.	N/A	• Annual SAQ. • Quarterly network scans by ASV.
4	• Annual SAQ recommended. • Quarterly network scans by ASV recommended. • Compliance validation requirements set by acquirer.	N/A	• Compliance validation requirements determined by acquirer. • Recommended validation: Annual SAQ and quarterly network scans by ASV.	N/A	• Compliance validation is at discretion of acquirer. • To validate: annual SAQ; quarterly network scans by ASV.

Figure 5 -PCI DSS Validation Requirements for Merchants [26], [27], [28], [29]

The table below illustrates validation requirements for Service Providers, as defined by each Payment Brand.

Level	Visa	AMEX	Discover	JCB	MasterCard
1	• Annual ROC by QSA. • Quarterly network scans by ASV. • Attestation of compliance form. • Included on Global list of PCI DSS validated service providers.	• Annual onsite assessment performed by QSA or service provider if certified by the CEO, CFO, CISO, or principal of the service provider. • Quarterly network scans by ASV.	• Annual onsite review by QSA or internal auditor (if signed by officer of service provider) or annual self-assessment using SAQ D. • Quarterly network scans by ASV.	• Annual onsite review by QSA. • Quarterly network scans by ASV.	• Annual onsite review by QSA. • Quarterly network scans by ASV.
2	• Annual SAQ. • Quarterly network scans by ASV. • Attestation of compliance form. • Not included on global registry of service providers (can complete level 1 validation requirements to be included on list).	• Annual SAQ performed by the service provider and certified by the CEO, CFO, CISO, or principal of the service provider. • Quarterly network scans by ASV.	N/A	N/A	• Annual SAQ. • Quarterly network scan. • All noncompliant service providers are required to submit a completed MasterCard Action plan.
3	N/A	• Annual SAQ. • Quarterly network scans by ASV.	N/A	N/A	N/A

Figure 6 - PCI DSS Validation Requirements for Service Providers [29]

In case of merchants, or service providers which are at Level 1 or Level 2, one of the major PCI DSS validation components is the Annual On-Site Assessment that is based on the PCI DSS Audit Procedures document. This means that merchants and service providers should choose a Qualified Security Assessor (QSA) to carry out the audit. A list of approved QSAs is displayed on the official web site of the PCI SSC. An assessor is supposed to strictly adhere to the Audit Procedures document and complete the mandatory report on compliance, required for PCI certification and validation on behalf of the merchant or service provider.

Another validation requirement for almost all merchant and service provider levels are quarterly network scans which provide them with useful information regarding their Internet-facing information systems and give them the opportunity to work alongside with a comprehensible vulnerability management program. The PCI Approved Scanning Vendors (ASVs) can help a merchant or service

provider locate the misconfigurations on web sites, applications and IT infrastructures with Internet-facing IP addresses. After the process of scanning, depending on the results that have been acquired the Approved Scanning Vendor (ASV) produces an exhaustive report that describes types of vulnerabilities or risks, finding out issues that are linked to the vulnerability types, implement ways to fix or patch the isolated vulnerabilities and finally, assign a rating for the isolated vulnerabilities.[30]

Moreover, merchants and service providers that are not required to undergo an on-site data security assessment, as shown on the figures above, are required to complete a Self-Assessment Questionnaire (SAQ), in order to validate their compliance with the standard. There are multiple versions of the PCI DSS SAQ to meet various business scenarios, as can be seen at the figure that follows.[31]

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. Not applicable to face-to-face channels.
A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. Applicable only to e-commerce channels
B	Merchants using only: • Imprint machines with no electronic cardholder data storage; and/or • Standalone, dial-out terminals with no electronic cardholder data storage. Not applicable to e-commerce channels.
B-IP	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. Not applicable to e-commerce channels.
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. Not applicable to e-commerce channels.
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. Not applicable to e-commerce channels
P2PE-HW	Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. Not applicable to e-commerce channels.
D	**SAQ D for Merchants:** All merchants not included in descriptions for the above SAQ types.
	SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete a SAQ.

Figure 7 - PCI DSS Self-Assessment Questionnaires [32]

2. Airline Industry Payments Overview

Airline companies operate differently to other merchants due to the involvement of multiple entities during the whole process, that initiates from the customer's purchase of a ticket and ends at customers boarding to the airplane. Airlines & travel companies are paying billions of dollars annually, in order to collect their payments.

Airline tickets distribution can be divided in the following two main categories, according to the involvement of third parties between the consumer and the airline during the payment process.[33]

- ***Direct Distribution*** – which refer to sales performed directly within the Airline's system using one of the following payment channels managed by the Airline, without the interference of any other entity or third parties' system:
    - Airline's offices (POS – Point of Sale)
    - Airline's Call center (MOTO – Mail Order Telephone Order)
    - Airline's website (E-commerce)
- ***Indirect Distribution*** – refer to sales originating from third parties that the Airline has provided them with the ability to sell ticket on behalf of the Airline
    - Traditional travel agents
    - On-line travel agents (Booking.com, Expedia, Priceline.com,..)

Regarding the use of payment cards, airline industry seems to be no different to the normal transaction flow of other retailers, there are, however, multiple touch points to a transaction depending on where and how the customer purchases their ticket. With the exception of direct ticket sales at airline websites or airline operated stores, the transaction and the associated cardholder data flows through multiple parties' systems, and is used for ticket sales or other ancillary charges (e.g. excess baggage, seat upgrade) and functions other than completing the payment. For example, airlines use the customer's card number to validate their identity at check-in, both at staffed check-in desks and at self-service kiosks. A comprehensive analysis of the distribution channels and the functions, in which cardholder data flows, will be included in the following chapters.

2.1 Airline's Direct Distribution Channel

The process during a direct ticket sale is pretty much straightforward. Sales methods may include Mail Order or Ticket-by-Mail, Web-site or E-Commerce, Sales Offices owned by the Airline at the Airport Ticket Office or City Ticket Office. There is also a wide range of different sales, e.g., in-flight duty free sales, excessive baggage, upgrades and annual membership fees for lounges.[34]

An airline's direct distribution originates by the Airline mostly through point of sales devices or airline integrated systems or in some cases Computer Reservation Systems (CRS) or Global Distribution Systems (GDS) are utilized.[35]

Since the ticket purchase is carried out through the Airline's system, the payment card details are sent to the Airlines Acquiring Bank Authorization System for authorization of the transaction. In order for clearing and settlement of the transactions to be performed, reconciliation files are sent from Airline System to the Acquiring Bank Clearing System. The figure below depicts the Airline Direct Ticket Sales Process and the involved entities.

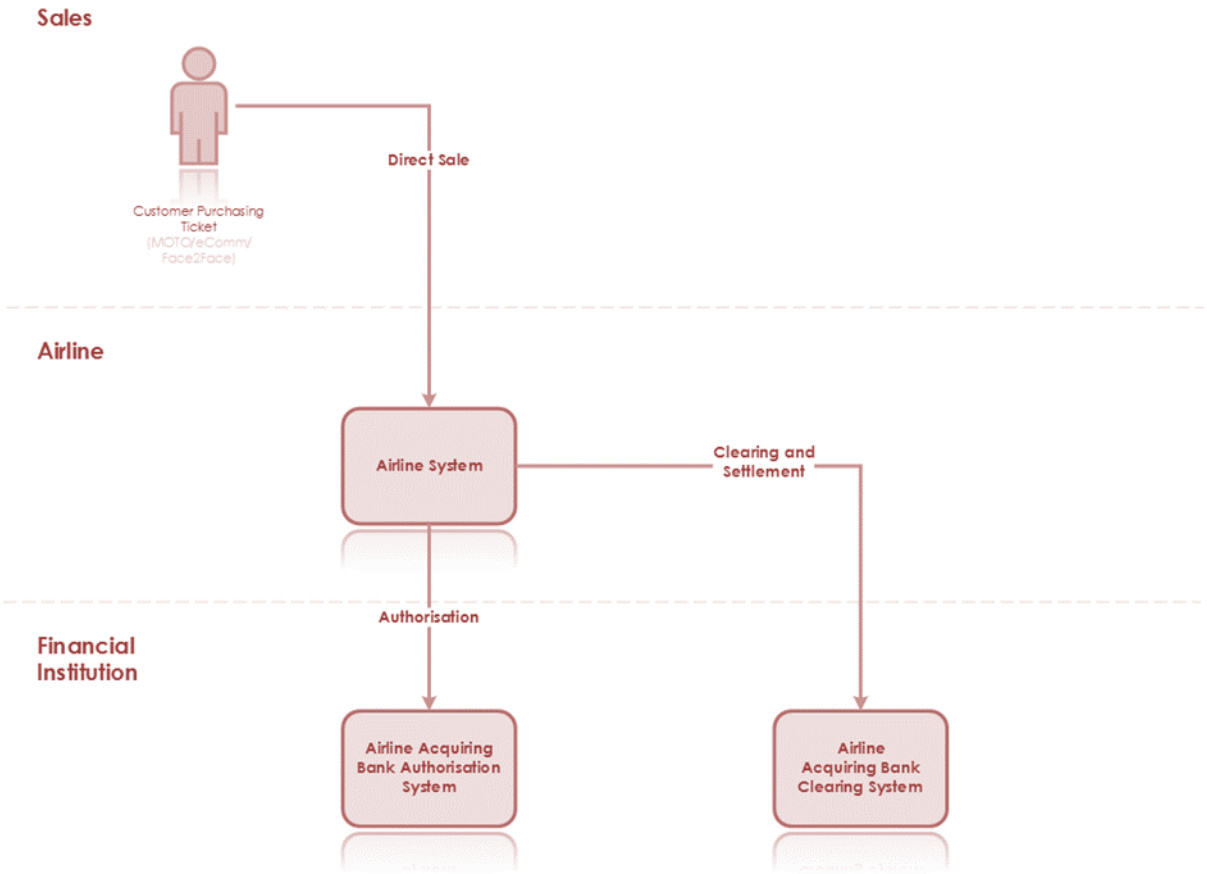

Figure 8 - Airline Direct Ticket Sales Process

2.2 Airline's Indirect Distribution Channel

The majority of airline tickets are distributed through travel agents either by face-to-face transactions, telephone or Internet (card not present). Travel agents use systems provided by a Global Distribution System (GDS) provider. These GDS systems (e.g. Sabre, Amadeus, Galileo) link to the airline systems to check ticket availability, to financial systems for authorisation and then to IATA (International Air Transport Association) systems, like the IATA Bank Settlement Plan (BSP), for clearing and settlement purposes.

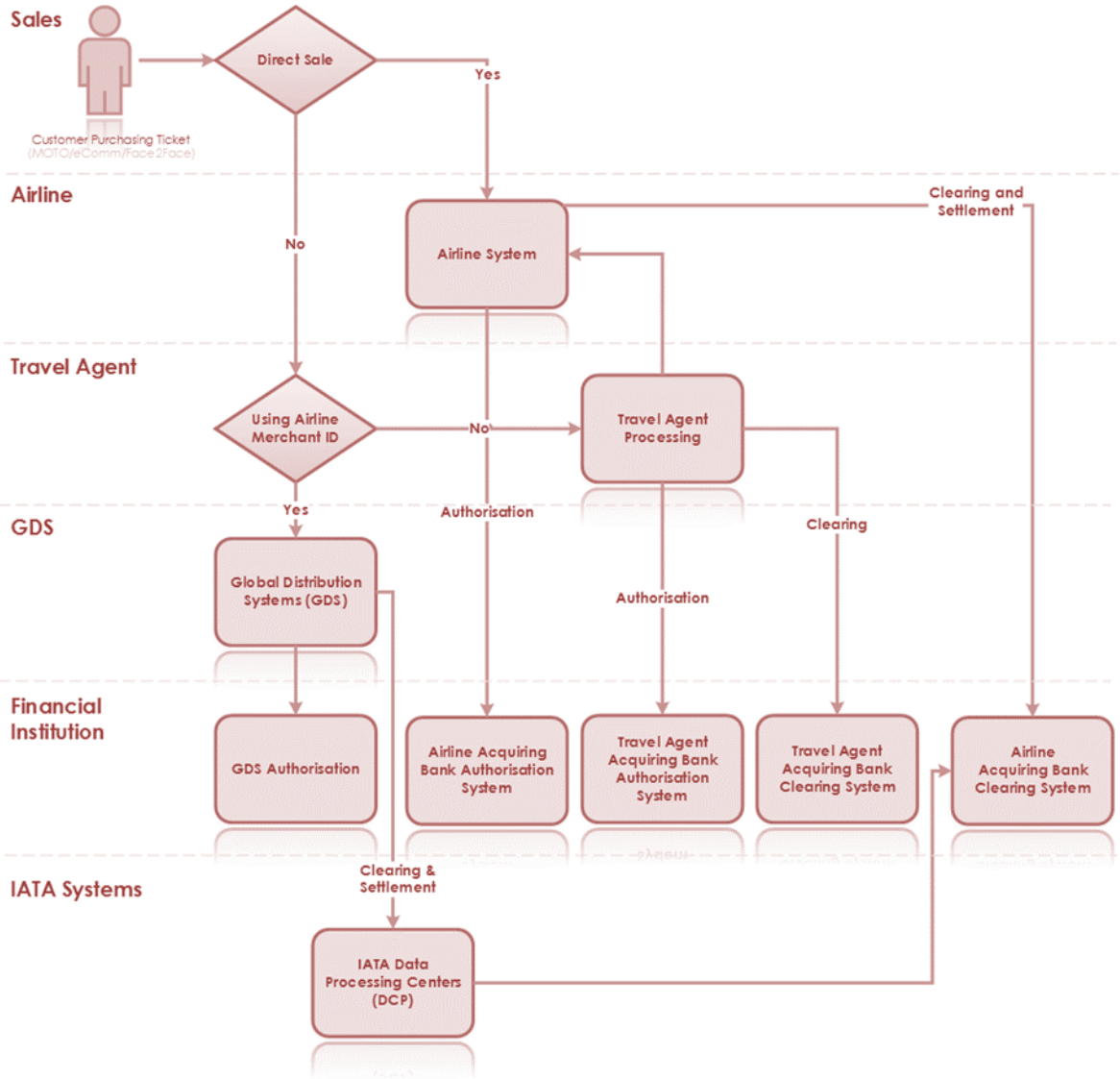

Figure 9 - Travel Agent Ticket Sales Process

The Ticket Sales process, depicted on the diagram above, initiates at the time the customer, by using one of the travel agent's distribution channels, wishes to purchase a ticket. Depending on the type of transaction or fare type, the airline or the travel agent may be the merchant. The procedures differ based on to whom the merchant ID used belongs.

For cases where the travel agent uses his own merchant ID, the processing is performed through the Travel Agent's system and the authorization and clearing will be carried out by the Travel Agent's Acquiring Bank Authorisation System and the Travel Agent's Acquiring Bank Clearing System, respectively.

In the majority of the cases, the Travel Agent uses the Airline's merchant ID and checking for ticket availability and issuance of the ticket is almost always performed through Global Distribution System (GDS). The authorization is generally directly through a GDS using its own Authorisation Card Scheme (Direct Connection). GDS forwards the reservation file containing payment card numbers to the Billing Settlement Plan (BSP). The BSP has a designated processor, which then forwards the settlement file to the Airline Acquiring Bank Clearing System. At the close of 2013, there were 88 BSPs, covering 179 countries and territories serving about 400 airlines, while gross sales processed amounted to $259 billion. The on-time settlement rate was 99.96%.[36]

The agent reports all sales and refunds at the end of the reporting period. This is performed electronically, through BSPlink. All transactions are forwarded to a central BSP Data Processing Centre (DPC).[37]

2.3 Functions using Payment Cards other than completing the payment

At present, payment card information is being passed through the airline industry networks for multiple purposes, other than completing payments. These purposes include the following:

- **Payment card as a form of identity (FOID)**

  Many airlines use payment card data as a form of identity for their customers. Card data is passed through the systems at the time of reservation and then used at check-in to verify the customer's identity. The check-in may occur at a staffed counter or at a kiosk. At present the check-in process uses the full PAN details to identify the customer and these details are passed and held within the airline systems.

- **Common Use Self Service (CUSS)**

  Common-use self-service or CUSS are shared kiosks that provide passengers with the ability to check-in without the need for ground staff.[38] CUSS terminals are also used to process payments from customers for excess baggage, seat upgrades and so on. Unlike kiosks in other industries (e.g. rail), each CUSS kiosk may serve all airlines operating out of a particular terminal at an airport.

2.4 Impact of Third Party Service Providers to Airline's PCI DSS Compliance

As described in previous chapters, a number of third parties are involved during the processing of cardholder data and interpose between the Customer and the Airline. According to PCI Requirement 12.8, each airline, as the sole merchant of record for a card transaction, is responsible for the PCI compliance of its third party Service Providers, including shared infrastructures and processes such as the BSP.

As an individual airline is not able to carry on its own the PCI compliance of such entities, Airlines have demanded that IATA support them on this task by making the BSP card sales channel PCI DSS compliant. In addition, an IATA committee agreed to remove the transmission and storage of full PAN numbers as a form of identity and replace the full PAN numbers with the truncated version of them.

During this initiative IATA was tasked to develop recommendations for self-service devices (airline kiosks deployed at airports and other locations) that are using card numbers as FOID or support card payments. Moreover, IATA is also working with airline service and network providers and accredited travel agents on PCI DSS compliance.[39] IATA is also surveying the individual GDS and eTSP on their PCI DSS status as part of their ongoing PCI DSS roadmap.[40]

3. Motivation and Scope

The scope of the present study is to outline the challenges that Airline Industry faces in order to comply with PCI DSS, by presenting the processes that a specific Airline company follows regarding the administration of payment cards, and to propose certain suggestions for making compliance process much easier. As acquirers and payment brands forcing entities to comply with the standard, more and more card industry stakeholders including banks, merchants, service providers and issuers are working to get the compliance. Compliance process can be very cost and effort demanding, if not approached correctly.

Airlines have evolved rapidly the last decades by gradually moving away from the traditional models inherited, such as imprinted tickets and so on. However, the Internet, a convenience to travelers looking to quickly book a trip, is also a gateway to fraud, costing the airline industry tens of millions of dollars a year. The motivation of the present study was the fact that the Airline industry faces some very unique challenges that makes it very interesting for studying. Moreover, studying and analyzing an organization of that size provides extensive knowledge about the standard that I could be use in the future during a career in the field of Information Security.

4. Case Study – Description of Cardholder Data Environment

The purpose of this Chapter is to provide intelligible and detailed information about the organisation's Cardholder Data Environment. The Chapter encompasses detailed information about:

- The cardholder data flows over the Company's networks, including the identified card transaction acceptance channels utilized by the organization for processing payment card transactions coming from its clients.
- The cardholder data "locations", both in electronic & paper based format.

4.1 Company Profile

The organization featured on this case study is an airline company operating in the sector of aviation transportation, providing services that concern the transportation of passengers and commodities in the sector of public aviation transportation worldwide, conducting scheduled and unscheduled flights. At the same time, it renders services of aviation applications, technical support and on ground handling aircraft services. It also provides charter flights, cargo services and technical services, as well as operates a network of ticket offices and also offers e-ticket services.

4.2 Company's Payment Card Business

The Company's customers can pay for tickets, products and excess baggage allowance by using their payment cards. In particular:

- Tickets can be purchased through:
  - Company's web-site,
  - Company's mobile site,
  - Company's call-center located in the company's headquarters,
  - Ticket sale desks operated by the Company in a number of airports,
- Products including perfumes, cosmetics and accessories can be purchased on all Company's international flights.
- Passengers who wish to carry additional bags or bags that exceed their weight allowance may prepay through the company's website, company's check-in desks in all domestic airports, the mobile site or through the call center.

4.3 Card Brands Accepted by the Company

The Company accepts for the payment of its services and products, payment cards that come from the following Card Brands:

- Visa
- MasterCard
- American Express
- Discover (Diners)

4.4 Cardholder Data & Sensitive Authentication Data Captured

For conducting payment card transactions at the various sales points, the Company captures the following cardholder and sensitive authentication data types for authorisation purposes:

Payment Channels	Data Types Captured for Transaction Authorisation
eCommerce	• Cardholder Name • PAN • Expiration Date • Card Verification Code/Value [CVV2, CVC2, CID depending on the card]
Mobile Commerce	• Cardholder Name • PAN • Expiration Date • Card Verification Code/Value [CVV2, CVC2, CID depending on the card]
MOTO (call center, town offices)	• Cardholder Name • PAN • Expiration Date • Card Verification Code/Value [CVV2, CVC2, CID depending on the card)]
POS (domestic airports)	• Full Magnetic stripe or magnetic stripe image on chip, depending on card • PIN

Figure 10 - Cardholder Data Types Captured for Transaction Authorisation per Payment Channel

4.5 Compliance Level

The merchant examined for this thesis is processing more than 20,000 Visa e-commerce transactions per year. Based on this and according to Visa Europe compliance validation framework for merchants, the Company is considered to be a Level 3 Merchant. As a Level 3 merchant, the Company must:

1. Complete on an annual basis the appropriate Self-Assessment Questionnaire (SAQ).
2. Conduct on a quarterly basis and after any significant change in its network external network vulnerability scans (ASV Scans). The external network vulnerability scans must be performed by an Approved Scanning Vendor (ASV).

4.6 Card Transactions Authorization, Clearing & Settlement Processing

On a daily basis the Company processes hundreds of payment card transactions generated from the sales of company's tickets, products sold on the Company's international flights and excess baggage charges to Company's customers.

4.6.1 Authorization Processing

In the Company, authorisation processing involves the transmission of payment card transaction authorization messages to the acquiring banks and payment card transaction processors. Company's locations where payment card transactions are processed for authorisation purposes include the following:

- E-commerce web site (ticket sales and payments for extra baggage allowance)
- Mobile site (ticket sales and payments for extra baggage allowance)
- Call center (ticket sales and payments of extra baggage charges)
- Accounting Department (payments of products sold on international flights)
- Domestic airports (ticket sales offices, check-in desks).
- Town Offices (ticket sales)

The following list contains all technologies utilized by the Company to process payment card transactions for authorization purposes:

- Dial-up / wireless POS devices (domestic airports, town offices)
- E-commerce web-site
- Mobile site
- Virtual POS (can be found in the company's headquarters)
- Call Center System

Authorisation traffic flows are described in detail in Section 4.7 "Payment Card Transactions Authorization Traffic Flows".

4.6.2 Clearing & Settlement Processing

With the exception of payment card transactions conducted via dial-up and wireless POS devices, the Company's payment card transactions are automatically cleared and settled by the Company's acquirers and payment card transaction processors, without the need for any employee to ever get involved or view any customer cardholder data.

In the case of POS devices, both dial-up and wireless, the clearing & settlement process is initiated as soon as the Company's responsible employees activate manually on each POS device operated by the company, the batch file upload function. The batch file contains all completed payment card transactions conducted at the POS during a business day. By activating the particular function the batch file is sent automatically to the acquirer or payment card transaction processor for further processing. It must be noted that during the conduct of this process none of the Company's employees can view any customer's cardholder data.

4.7 Payment Card Transactions Authorization Traffic Flows

4.7.1 E-Commerce

Company's customers can purchase tickets and extra baggage allowance through the company's e-commerce web-site. After they select the tickets they want to purchase and / or the extra baggage allowance they want to pay they are redirected to a payment page provided by a GDS provider.

4.7.2 Mobile Commerce

Extra baggage allowance and tickets can also be purchased by Company's customers through the Company's mobile commerce site. In a similar way to the e-commerce web-site, when a Company's customer selects the ticket(s) and / or extra baggage allowance he / she wants to purchase, he / she is redirected to a payment page provided of a GDS provider.

4.7.3 Call Center

Company's customers can purchase tickets and pay for excess baggage allowance / charges through the Company's call center. The call center agents process these two types of payment card transactions through a Global Distribution System, using a web browser.

4.7.4 Accounting Department

For each product sold on Company's international flights, the Company's Accounting Department is responsible to complete the purchase process. To process the payment card transactions, staff of Accounting Department utilize a payment service through a web browser.

4.7.5 Dial-up / Wireless POS Devices

Dial-up and wireless POS devices are utilized by the Company in its sales offices in the domestic airports and the Company's town offices in order for its customers to be able to purchase tickets and pay for excess baggage charges using their payment cards.

The majority of the POS devices utilized by the Company are dial-up and there are a few wireless POS devices in use in international airports.

4.7.6 Town Offices

All the POS devices utilized by the Company in its Town Offices are dial-up POS devices. In all Town Offices the set-up of the POS devices is the same.

4.7.7 Check-In Desks

In all domestic airports, during the check-in process Company's customers can pay for extra baggage charges using their payment cards. It has to be noted that the payments are processed through a GDS system.

4.8 Departments involved in the Processing, Storage and Transmission of Cardholder data

4.8.1 Call Center Department

The Company's Call Center Department provides telephone support services to company's customers. Among other things, the Call Centre Department is responsible for:

- Issuing tickets,
- Performing ticket changes and cancellations,
- Handling customers' complaints,
- Processing payment card transactions for extra baggage allowance,
- Communicating with other Company's departments and external entities for the resolution of various issues concerning payment card transactions conducted by the Company's customers.

In order to conduct their duties all call center agents have access to a GDS system, among other systems. It must be noted that all telephone conversations taking place between the call center agents and the customers are recorded by a telephone conversations recording system. In addition, the system is configured to record call center agents screen interactions, providing this way the ability to the Call Center Manager to search and replay agents' captured interactions.

4.8.1.1 Ticket Issuance

When a customer contacts the Company's call center to purchase a ticket, the following steps are performed:

- the call center agent collects from the customer the necessary cardholder data (PAN, Card Verification Code, Expiration Date)
- the call center agent enters the collected cardholder data into the GDS to process the payment and issue the ticket
- when the payment is accepted and the ticket is issued the agent notifies the customer.

4.8.1.2 Ticket Change

The Company's customers can contact the Company's call center to request the change of their tickets. In this case, when a customer contacts the Company's call center in order to request the change of his / her ticket and to find out if there are seats available on the new flight, the following actions are performed:

- In order for the agent to identify through the GDS the ticket that needs to be changed, requests from the customer to be provided with an identifier, such as the ticket number, or the passenger name record (PNR).
  It must be noted that there are certain Airlines that in such cases they request for the payment card number in order to identify the ticket.
- Once the ticket is identified, the agent checks through the GDS the availability of seats on the new flight, and in case the new tickets costs more, the customer is asked to pay for the additional amount (e.g. by a payment card).

4.8.1.3 Ticket Cancellation

The Company's customers can contact the Company's call center in order to request the cancellation of their tickets. In order for this procedure to take place, the following actions are performed:

- In order for the agent to identify through the GDS the ticket that needs to be cancelled, requests from the customer to be provided with an identifier, such as the ticket number, or the passenger name record (PNR).
  It must be noted that there are certain Airlines that in such cases they request for the payment card number in order to identify the ticket.
- Once the ticket is identified, the call center agent cancels it.

4.8.1.4 Customers' Complaints Handling

Customers can contact the Company's call center when they have to make a complaint. Complaints made by the Company's customers may concern double charges made by the Company on their payment cards, tickets never issued by the Company although charges on their payment cards were made, or may concern other issues which are not related to payment cards processing. Depending on the nature of the customer's complaint the call center agents and / or supervisors handle the complaints through one of the following ways:

- Call Center Agent Informs the Accounting Department
  - In order for the call center to identify the ticket, requests from the customer to be provided with an identifier, such as the ticket number, or the passenger name record (PNR).
  - The call center agent uses an application provided by the clearing bank to confirm the existence of the double charged payment card transaction.
  - Once the double charged transaction is confirmed, the call center agent records the details of the transaction. It must be noted that no cardholder data is included in the record.

On regular time intervals, a call center agent accesses the application in which the details of the transactions are recorded, in order to create a file that will include all transactions reported to have been double charged and need to be refunded. The file is sent to the Accounting Department for further processing (i.e. refunds processing). It is noted that no cardholder data is included in the file.

- Call Center Supervisor informs the clearing Bank
  - In order for the agent to identify through the GDS the ticket for which the double charge on the customer's payment card, requests from the customer to be provided with an identifier, such as the ticket number, or the passenger name record (PNR).

- The call center agent uses an application provided by the clearing bank to confirm the existence of the double charged payment card transaction.
- Once the double charged transaction is confirmed, the call center agent informs the call center supervisor about the transaction's information.
- The call center supervisor requests from the clearing bank he refund of the transaction that was double charged.

- Call Center Supervisor informs Customer Relations Department
  - Call center agent informs the company's customer to contact the Company's Customer Relations Department to discuss its complaint.
  - In certain cases the Customer Relations Department may request from the Call Center Department the electronic record that contains the conversation which took place between the customer and the call center agent and is associated with the customer's complaint. It must be noted that the telephone conversation electronic record may contain cardholder data and / or sensitive authentication data (e.g. payment card number, card verification code, etc.)
  - The Manager of the Call Center Department identifies the corresponding telephone conversation record. and forwards it to the Customer Relations Department..
  - Upon receipt of the telephone conversation record, the responsible staff in the Customer Relations Department performs all necessary actions to address the customer's complaint.

4.8.1.5 Extra Baggage Allowance Payments Processing

The Company's customers wishing to purchase extra baggage allowance can contact the Company's call center. The actions performed by the call center agents to process the particular payments are described below:

- The Company's customer contacts the Company's call center requesting to purchase extra baggage allowance.
- Customer provides the call center agent with his / her payment card information.
- The call center agent enters the customer's payment card details into the GDS in order to process the payment.
- When the payment is authorised and processed, the customer is notified.

4.8.1.6 Communications with Domestic Airports

On a daily basis the call center agents and supervisors communicate with Domestic Airports in order to resolve various issues concerning payment card transactions conducted by the Company's customers.

The Company's customers can contact the Company's call center when they want to cancel a ticket that it was purchased and issued in one of the domestic airports where the Company operates. When the ticket is cancelled by the call center agent (through the process described in section 4.8.1.3), an email is sent to the domestic airport that issued the ticket. The email contains cardholder data (i.e. payment card number) and its purpose is to inform Company's member of staff in the domestic airport that the ticket is cancelled and that a refund for the amount of the ticket purchase must be conducted.

4.8.2 Airport Station

The Company's personnel in the Airport Station are responsible among other things to perform on a daily basis the following payment cards related duties:

- Issue tickets for customers.
- Process payments for extra baggage allowance or excess baggage charges.
- Administer the payment slips and totals balance slips printed out by the dial-up POS devices operated by the Company in the airport.

It has to be noted that all the above duties are also performed by the Company's personnel in all domestic airports where the Company operates.

4.8.2.1 Tickets Issuance for Customers

Company's customers can visit the company's Ticket Sales Office at Airport Station in order to purchase their tickets. The actions performed by Company's personnel in the company's Ticket Sales Office at the Airport Station to issue the tickets are described below:

- A customer visits the Ticket Sales Office at the airport and requests to purchase a ticket on a particular flight.
- A staff member in the Ticket Sales Office informs the customer on the availability of seats for the particular flight and the price of the ticket.
- If the customer decides to purchase the ticket he / she gives his / her payment card to the member of staff who is responsible to process the payment card transaction for the ticket purchase and also to issue the ticket.
- The staff member in the Ticket Sales Office swipes the customer's payment card through the dial-up POS device and waits for the payment card transaction to be authorised.
- Once the transaction is authorised the customer is asked to sign the merchant's copy of the payment slip printed out by the dial-up POS device and at the same time he / she is provided with a copy of the customer's payment slip.
- In order for the ticket to be issued, the Company's member of staff enters the customer's payment card details into the GDS.
- Once the ticket is issued the customer is provided with his / her ticket booking details.
- The ticket purchase process completes when the customer is provided with an invoice for his / her ticket purchase. The invoice does not contain any cardholder data.

4.8.2.2 Extra Baggage Allowance Payments Processing

Customers can purchase extra baggage allowance in the Airport during the check-in process. In order to do so, the customer must provide his / her payment card data to the Company's member of staff. This is usually performed via a card reader connected to the employee's workstation.

When the payment card transaction authorization process completes and is successful, some of the details of the payment transaction are printed on the customer's boarding pass. In particular, on the boarding pass the number of the payment card used in the transaction is printed but in a masked form.

4.8.2.3 Administration of Payment Slips and Totals Balance Slips

Company's personnel in the Company's Ticket Sales Office at the Airport are responsible for the administration of the payment slips and totals balance slips produced daily by the dial-up POS devices operated in the office. Both the payment slips and totals balance slips are sent twice a day, via internal post, to the Accounting Department and Revenue Accounting Department respectively. It must be noted that both types of slips may contain payment card numbers.

4.8.3 On-board Sales Department

The On-board Sales among other things is responsible for administering the sales of products occurring on all Company's international flights. The payment process for any product sold on international flights is initiated on the aeroplane during the flight and is usually completed by the Accounting Department which is responsible to process the corresponding payment card transaction.
The parties involved in the payment process are the following:

- Passenger – uses a payment card to purchase a product.
- Flight attendant – collects payment details from the passenger through a collection terminal.

- On-board Sales Department – forwards payment details to Accounting Department for further processing.
- Accounting Department – process the corresponding payment card transactions and transmits them to the Bank.

4.8.4 Accounting Department

Among other things, the Accounting Department is responsible for:

- Administering the totals balance slips received daily from all domestic airports.
- Completing the process which relates to the selling of products on international flights, by processing the corresponding payment card transactions.
- Administering charged back payment card transactions.
- Conducting accounting audits using GDS HOT Files.
- Communicating with payment service providers to resolve issues related to the settlement of payment card transactions.

4.8.4.1 Totals Balance Slips Administration

On a daily basis the Accounting Department receives from all domestic airports where the Company operates, the totals balance slips produced by the POS devices operated by the company in the airports. The received slips are used by the department's members of staff to conduct various accounting related audits. Once the audits are completed the slips are stored securely. It must be noted that the totals balance slips may contain cardholder data (i.e. payment card numbers).

4.8.4.2 On-board Sales Payment Card Transactions Processing

On a regular basis, the Accounting Department processes, for every product sold on international flights, the corresponding payment card transaction. To process the payment card transactions the responsible employee needs to gather the receipts produced by the collection terminal on international flights and uses a Bank's application to process the corresponding payment card transactions.

At this point, it must be highlighted that the employee may face issues with transactions which are not authorised by the Bank. In such cases, the Company must investigate the case and during this course cardholder data (e.g. PANs) may be stored electronically depending on the company's business process.

4.8.4.3 Charged Back Transactions Processing

The Accounting Department receives faxes from acquirers and payment service providers concerning payment card transactions that have been charged back. The faxes sent to the Accounting Department do not contain cardholder data.

Every time the Accounting Department receives a fax containing a transaction that has been charged back, a member of staff in the department sends an email to the Revenue Accounting Department requesting information about the issued ticket. The email contains information about the payment card transaction that it was charged back. When the Accounting Department receives the information requested from the Revenue Accounting department, forwards the information to the acquirer or payment service provider. It has to be noted that no payment card numbers are included in the Accounting Department's response to the acquirer or payment service provider.

4.8.4.4 Accounting Audits

On a regular basis a particular member of staff in the Accounting Department downloads the GDS HOT File. The HOT File is downloaded for accounting audit purposes. Once the audit is completed the file is deleted. It has to be noted that the file contains payment card numbers.

In addition, on regular time intervals the Accounting Department produces a file in order to perform various accounting related audits. The file may contain cardholder data (i.e. payment card numbers) and is stored from an employee in the Accounting Department responsible to conduct the accounting audits.

4.8.4.5 Communications with Payment Service Providers

The Accounting Department is responsible to provide payment service providers with information about transactions that were not settled by the provider. Whenever such a case occurs, a member of the Accounting Department staff uses the GDS to identify the related transactions. Once the list of transactions is created, it is sent to the payment service provider. It has to be noted that this communication contains payment card numbers.

4.8.5 Revenue Accounting Department

The Revenue Accounting Department among other things is responsible for:

- Receiving from domestic airports the payment slips (merchant's copy) printed by the POS devices operated by the company in the airports.
- Administration of GDS HOT File and BSP files.
- Notifying the Accounting Department about transactions that need to be refunded.

4.8.5.1 Payment Slips Administration

The payment slips produced by the dial-up POS devices in the domestic airports are sent to the Revenue Accounting Department. When the payment slips are received they are securely stored.

4.8.5.2 Administration of HOT Files and BSPs Files

The Revenue Accounting Department receives from GDS and BSPs, electronic files containing payment card numbers. In particular, the following two types of electronic files are received by the department:

- **HOT Files:** These are files that contain information related to payment card transactions processed by the GDS on behalf of the Company. The files are created by the GDS on a daily basis and they are transferred to the Company via an SFTP service. On a daily basis, a member of the Company's staff in the Revenue Accounting Department stores the file.
- **BSP Files:** These files contain information on payment card transactions conducted by travel agents on behalf of the Company. On a daily basis a staff member of the Revenue Accounting Department logs on to IATA's web-site in order to download files produced by different BSPs.

4.8.5.3 Sending Refund Requests to the Accounting Department

Whenever a member of the Company's staff in the Revenue Accounting Department wishes to refund a ticket purchased by a customer, he / she requests from the Accounting Department the ticket refund. Among other things this communication may contain the full number of the payment card to be refunded.

4.8.6 Fraud Detection Department

The Fraud Detection Department, among other things, is responsible for:

- Carrying out investigations on suspicious payment card transactions.
- Providing assistance to third parties and Company's customers on payment cards related issues.

4.8.6.1 Investigations on Suspicious Payment Card Transactions

The Company's members of staff in the Fraud Detection Department perform investigations in order to identify any tickets that were purchased with payment cards that were used in a fraudulent way. The investigations are mainly performed on flights that the Company considers to be high risk flights (i.e. flights to destinations that where the number of fraudulent payment card transactions from the tickets sales is very high).

In the course of the department's operations, its employees gather payment card related information mainly from the GDS in order to identify cards used in high risk flights. Doing so, the department is able to block the particular tickets and even to search for additional tickets purchased using the same payment card.

4.8.6.2 Communication with Third Parties and Customers

The department is often contacted by third parties and customers who request information on suspicious payment card transactions. Most of the times the requests received contain payment card numbers. When the responsible member of staff in the department completes the investigation, informs the interested party about the outcome of the investigation .This communication may contain, among other things, the payment card number used in the transaction.

4.8.7 Customer Relations Department

The Customers Relations Department is responsible for handling complaints coming from customers. The department handles on a daily basis various types of complaints including complaints which are related to payment cards.

The process followed by the staff members in the Customer Relations Department to address and resolve customers' payment card related complaints is the following:

- A customer communicates with the Customer Relations Department in order to make a complaint on a payment card related issue.
- During the conversation the responsible member of staff in the Customer Relations Department requests from the customer information regarding his/ her payment card. These details will be used for the investigation of the customer's case.
- The Customer Relations Department dealing with the customer's complaint communicates with the company's Call Center Department in order to request the telephone conversation record that relates to the customer's complaint.
- The Manager of the Call Center Department provides the telephone conversation record to the Manager of the Customer Relations Department.
- When the investigation is completed the customer is informed about the outcome of the investigation.
- In the case where a refund to the customer's payment card must be performed the Accounting Department is informed. This communication may contain payment card information.

4.8.8 Town Offices

The Company maintains town offices in various cities. In all town offices the company's customers (e.g. companies and individuals) can purchase tickets and pay for them using their payment cards. This section provides information about the payment card related processes followed by the company's members of staff in the town offices.

Among other things, town offices are responsible for:

- Issue tickets for customers.
- Administer the payment slips and totals balance slips printed out by the dial-up POS devices operated by the Company.
- Performing ticket changes and cancellations.

4.8.8.1 Tickets Issuance for Customers

Company's customers can visit the company's Town Office in order to purchase their tickets. The actions performed by Company's personnel in the Company's Town Office to issue the tickets are described below:

- A customer visits the Town Office and requests to purchase a ticket on a particular flight.
- A staff member in the Town Office informs the customer on the availability of seats for the particular flight and the price of the ticket.
- If the customer decides to purchase the ticket he / she gives his / her payment card to the member of staff who is responsible to process the payment card transaction for the ticket purchase and also to issue the ticket.
- The staff member in the Town Office swipes the customer's payment card through the dial-up POS device and waits for the payment card transaction to be authorised.
- Once the transaction is authorised the customer is asked to sign the merchant's copy of the payment slip printed out by the dial-up POS device and at the same time he / she is provided with a copy of the customer's payment slip.
- In order for the ticket to be issued, the Company's member of staff enters the customer's payment card details into the GDS.
- Once the ticket is issued the customer is provided with his / her ticket booking details.
- The ticket purchase process completes when the customer is provided with an invoice for his / her ticket purchase. The invoice does not contain any cardholder data.

4.8.8.2 Administration of Payment Slips and Totals Balance Slips

Company's personnel in the Company's Town Office are responsible for the administration of the payment slips and totals balance slips produced daily by the dial-up POS devices operated in the office. Both the payment slips and totals balance slips are sent to the Accounting Department and Revenue Accounting Department respectively. It must be noted that both types of slips may contain payment card numbers.

4.8.8.3 Tickets Change

When a Company's customer wishes to change his / her ticket, he / she can contact the Company's town office to request the change of his / her ticket. In this case, the actions performed by the Company's responsible member of staff in the town office are described below:

- A customer contacts the Company's town office in order to request the change of his / her ticket and to find out if there are seats available on the new flight.

- In order for the employee to identify through the GDS the ticket that needs to be changed, requests from the customer to be provided with an identifier, such as the ticket number, or the passenger name record (PNR).
- Once the ticket is identified, the employee checks through the GDS the availability of seats on the new flight, and in case the new tickets costs more, the customer is asked to pay for the additional amount (e.g. by a payment card).

4.8.8.4 Tickets Cancellation

The actions performed by the Company's members of staff in town office in order to cancel and refund a ticket are described below:

- The customer communicates via telephone with the town office in order to request the cancellation of his / her ticket.
- In order for the employee to identify through the GDS the ticket that needs to be cancelled, requests from the customer to be provided with an identifier, such as the ticket number, or the passenger name record (PNR).
  It must be noted that there are certain Airlines that in such cases they request for the payment card number in order to identify the ticket.
- Once the ticket is identified, the employee cancels it.

4.9 Cardholder Data Environment Network Diagram

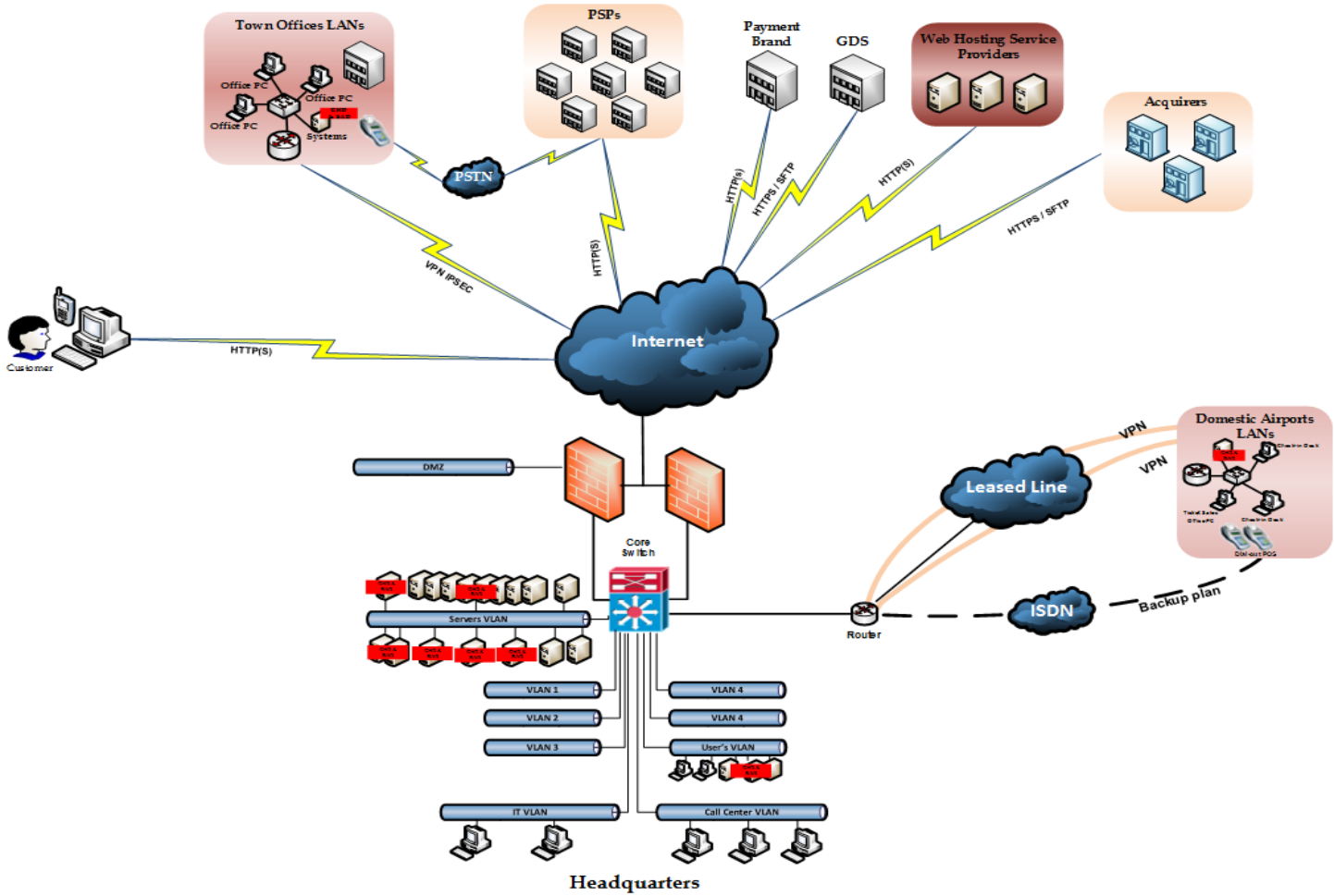

Figure 11 - Airline's Cardholder Data Environment (CDE)

5. Case Study – Analysis of Current State and Scope Minimization Suggestions

Airlines, like all other merchants and entities that store, process and/or transmit cardholder data, in order to comply with the Payment Card Industry Security Standard (PCI DSS) are obliged to meet PCI DSS requirements, applicable to their cardholder data environment (CDE), regarding security management, policies, procedures, network architecture, software design and other critical protective measures. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data, including terminals, network components, servers and applications. Devices and applications that process, transmit or store cardholder data and any other component connected to those devices or applications are considered to be in scope for the PCI DSS compliance assessment.

In Chapter 4 of the current thesis, the business functions and infrastructure components involved in cardholder data processing, storage and / or transmission and therefore comprise the Cardholder Data Environment (CDE), of the Airline subject of this case study, were identified and determined. Given the current status of the Airline, the cost and effort required in order for the Company to achieve compliance against PCI DSS will be significant for the Company. The aim of the current Chapter is to identify areas of improvement and present certain suggestions that if implemented will significantly reduce the PCI DSS scope and consequently the required effort and cost for compliance. Minimization of the cardholder data environment can be achieved through the reengineering of long-standing business processes and also by restricting cardholder data to as few locations as possible through the elimination of unnecessary data, and consolidation of necessary data.

After analysing the Airline's business functions and infrastructure components that form Airline's current state and bearing in mind the PCI DSS requirements, the following company's practices could be modified in order for the PCI DSS scope of the Airline to be reduced.

5.1 Cardholder Data Electronic Storage

Storage of Cardholder data should not be conducted unless merchants have a legitimate business reason to store cardholder data. PCI DSS allows merchants to store certain data elements such as primary account number (PAN), cardholder name and expiration date, but forbids, for any reason, the storage of sensitive authentication data (as shown on Figure 2).[41]

It is a violation of PCI DSS Requirement 3.2 to store any sensitive authentication data, including card validation codes and values (e.g. CVC2, CCV2, etc.), after authorization even if encrypted.

During the recording of the Cardholder Data Environment of the Airline, the following business processes were identified in which Sensitive Authentication Data is stored:

5.1.1 Extra Baggage Allowance Payments Processing

5.1.1.1 Current process

At the Airport station during the payment of extra baggage allowance, the customer's payment card is swiped through a card reader connected to the employee's workstation. This basically means that the

sensitive data contained on the magnetic stripe are stored at the PC used by the staff during the check-in.

As mentioned earlier this practice is strictly prohibited by the standard, specifically Requirement 3.2 states that:

*"**Requirement 3. Protect stored cardholder data***

***3.2** Do not store sensitive authentication data after authorization (even if encrypted).*

3.2.1 Do not store the full contents of any track

3.2.2 Do not store the card verification code or value.

3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block. "[42]

5.1.1.2 Recommendations

Based on that the aforementioned procedure should be altered, in order for sensitive authentication not to be stored. Alternatively a POS Device should be placed at the check-in desk and the charge for extra baggage allowance should be performed through the POS. The card should not be swiped by a card reader connected to the Airline's system. In case the Airline needs the payment card number for identification of the transaction or for reconciliation purposes, the check-in desk's employee could manually insert to the system a masked form of the payment card number (i.e. only the first six and the last four numbers of the card to be entered at the system).

5.1.2 Call Center Services

5.1.2.1 Current process

As described in Section 4.8.1, the Call Center Department is responsible for performing various activities that involve cardholder data. Due to the fact that, all telephone conversations and call center agents screen interactions are recorded, as a result the call recording systems stores cardholder data and sensitive authentication data (e.g. card verification codes/values). Audio/voice recordings containing cardholder data and sensitive authentication data are included in the scope of PCI DSS and should comply with relevant requirements.

It is a violation of PCI DSS Requirement 3.2 to store any sensitive authentication data, including card validation codes and values, after authorization even if encrypted. It is therefore prohibited to use any form of digital audio recording (using formats such as WAV, MP3, etc.) for storing CAV2, CVC2, CVV2 or CID codes after authorization if that data can be queried; recognizing that multiple tools exist that potentially could query a variety of digital recordings.[43]

5.1.2.2 Recommendations

Based on the aforementioned and the guidelines provided by PCI SSC regarding protection of telephone based payments, the Company should consider changing the current procedure in order to avoid storage of payment card information and primarily storage of sensitive authentication data.[43]

It is recommended that, if supported by the call center technology currently used, appropriate configuration should be performed, in order to prevent recording of these data elements. In case the call center solution used by the Company supports this function, the system should be configured to

allow the agents to stop recording the call at the time the customer provides his/her payment card's details to the agent. Moreover if the recording solution cannot block the audio or video from being stored, or the Company believes it is not functional enough, the code must be deleted from the recording after it is stored. In this way the payment card information won't be electronically stored and the Company could reduce the cost and effort for making the whole Call center infrastructure PCI DSS compliant.

In addition another solution that could exclude the entire call center environment from PCI DSS scope would be the Company to fully outsource the call center services to a PCI DSS certified Call Center Services Provider. This solution not only would reduce the cost and effort for compliance of the Call Center infrastructure, but would significantly reduce the scope of the entire PCI DSS compliance project by setting the VoIP Infrastructure out of PCI DSS scope.

5.1.3 Sales of Products on International Flights

5.1.3.1 Current process

During international flights passengers are able to purchase products and pay for them using their payment card. In order for the payments to proceed, flight attendants collect payment details from passenger through a collection terminal. In particular, the flight attendant swipes the passenger's payment card through the device's integrated card reader in order to collect the required payment card details. This basically means that the sensitive data contained on the magnetic stripe are stored at the device. As mentioned in previous Chapter this practice is strictly prohibited by the standard, specifically Requirement 3.2 states that:

*"**Requirement 3. Protect stored cardholder data***

***3.2** Do not store sensitive authentication data after authorization (even if encrypted).*

3.2.1 Do not store the full contents of any track

3.2.2 Do not store the card verification code or value.

3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block. "[42]

5.1.3.2 Recommendations

The company should consider changing the technology used for accepting payments for products sold on a company's international flights. The current technology does not address the requirements set by PCI DSS due to the fact that it stores sensitive authentication data post authorization. A proposed solution is that payments could be performed through wireless POS devices that will collect the payment card information during the flight and as soon as the airplane lands, the POS device will connect to the acquiring bank and receives authorization for all the transaction performed during the flight.

5.1.4 Administration of HOT Files and BSPs Files

5.1.4.1 Current process

The Revenue Accounting Department receives from GDS and BSPs, electronic files containing payment card numbers. In particular, the following two types of electronic files are electronically received and stored:

- **HOT Files:** These are files that contain information related to payment card transactions processed by the GDS on behalf of the Company.
- **BSP Files:** These files contain information on payment card transactions conducted by travel agents on behalf of the Company.

As long as the Company stores files that contain payment card information, the Company is obliged to secure this type of files by applying a number of requirements.

5.1.4.2 Recommendations

During the business function analysis it was identified that there is no business need for the respective files to include cardholder data information. These files are used for reconciliation purposes and therefore the full payment card numbers are not required and should be replaced by truncated payment card numbers (e.g. 123456xxxxxx7890). In addition, IATA has suggested that the Airlines should review if they make use of the payment card numbers and if they don't they should request from GDSs and BSPs to send these type of files with truncated payment card numbers.

5.2 Storage of Paper Media containing Cardholder Data

5.2.1 Administration of printouts of POS devices

5.2.1.1 Current process

Payment Slips and Totals Balance Slips produced by POS devices utilized by the Company, in its sales offices in the domestic airports and the Company's town offices, may display full payment card numbers (PANs). Accounting Department receives from all domestic airports where the Company operates, the totals balance slips produced by the POS devices operated by the company in the airports. The received slips are stored securely. Due to the fact that printouts of POS may display the full PANs, the company is required to protect this kind of paper and therefore should comply with a number of PCI DSS requirements. Some of these requirements are listed below.

*"**Requirement 9. Restrict physical access to cardholder data***

9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:

9.6.1 Classify media so the sensitivity of the data can be determined.

9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.

9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).

9.7 Maintain strict control over the storage and accessibility of media.

9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually

9.8 Destroy media when it is no longer needed for business or legal reasons as follows:

9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed

9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed" [42]

5.2.1.2 Recommendations

The company should consider requesting from the Acquirers and Payment Service Providers to upgrade the software run by the dial-up POS devices so that the payment slips and totals balance slips printed out by the devices contain only truncated payment card numbers. This way the Company will take out of its PCI DSS assessment scope paper media (i.e. payment slips and totals balance slips) and there will be no need to protect them in accordance with the PCI DSS requirements.

5.2.2 Sales of Products on International Flights

5.2.2.1 Current process

During international flights passengers are able to purchase products and pay for them using their payment card. In order for the payments to proceed, flight attendants collect payment details from passenger through a collection terminal. The terminal prints out a receipt that contains among others cardholder data.

In order for the payment card transaction to be processed, the Accounting Department receives the aforementioned print-outs. During this process paper media are stored by the Accounting Department containing cardholder data. In order to protect the paper media containing such data, the Airline is required to comply with a number of requirements. Some of these requirements are listed below.

*"**Requirement 9. Restrict physical access to cardholder data***

9.3 Control physical access for onsite personnel to the sensitive areas as follows:

- Access must be authorized and based on individual job function.

- Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.

9.7 Maintain strict control over the storage and accessibility of media.

9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually

9.8 Destroy media when it is no longer needed for business or legal reasons as follows:

9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed

9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed" [42]

5.2.2.2 Recommendations

In order for the Company to reduce the cost and the effort for compliance with the aforementioned requirements, the company should consider changing the current process used for accepting payments

for products sold in the company's international flights. With the current procedure paper media containing payment card data, including sensitive authentication data, are stored and needs to be protected.

If the Company decides to provide airplanes with wireless POS devices that will collect the payments, the printouts of the POS will display a truncated form of the PAN's and therefore no special handling of the paper media will be necessary.

5.3 Cardholder Data Transmission

5.3.1 Transmission of Cardholder Data via email

5.3.1.1 Current process

There are several procedures performed by the company's employees that involve the transmission of cardholder data through email. Some of them are listed below:

- Call center department communicates with domestic airports, in order to inform the Company's member of staff in the domestic airport for a ticket cancellation. This communication may contain cardholder data.
- Every time the Accounting Department receives a request containing a transaction that has been charged back, a member of staff in the department communicates with the Revenue Accounting Department requesting information about the issued ticket.
- During the communication with the Payment Service Provider the Accounting Department provides payment service providers with information about transactions that were not settled by the provider.
- Whenever a member of the Company's staff in the Revenue Accounting Department wishes to refund a ticket purchased by a customer, he / she communicates with the Accounting Department requesting the ticket refund.
- In cases of customers' complaints, during the telephone conversation the responsible member of staff in the Customer Relations Department requests from the customer to send his / her payment card details, including the payment card number. These details are used for the investigation of the customer's case.

As long these communications are performed via e-mail and consequently the email Infrastructure transmits payment cards' information, the whole infrastructure along with system that communicate directly with the infrastructure are considered to be in scope for PCI DSS assessment and should comply with a large amount of requirements. Some of these requirements are listed below:

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

2.2 *Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards (among these standards are Center for Internet Security (CIS), International Organization for Standardization (ISO) and National Institute of Standards Technology (NIST)).*

2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server.

2.2.2 Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system
2.2.3 Configure system security parameters to prevent misuse.
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.
2.3 Encrypt all non-console administrative access using strong cryptography
2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data (according to additional requirements).

Requirement 6. Develop and maintain secure systems and applications

***6.4** Follow change control processes and procedures for all changes to system components. The processes must include the following:*
6.4.1 Separate development/test and production environments
6.4.2 Separation of duties between development/test and production environments
6.4.3 Production data (live PANs) are not used for testing or development
6.4.4 Removal of test data and accounts before production systems become active
6.4.5 Change control procedures for the implementation of security patches and software modifications, including the relevant documentation, the approval by authorized parties, the verification tests and the back-out procedures.
***6.5** Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, according to latest industry best practices (including injection flaws, buffer overflow, insecure cryptographic storage and communications, improper error handling etc.).*
***6.6** For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks.*

Requirement 11. Regularly test security systems and processes

***11.2** Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).*
***11.3** Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification*
***11.4** Use intrusion-detection systems and keep these systems updated.*
***11.5** Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly." [42]*

In addition transmission of cardholder through unencrypted mail is strictly forbidden by Requirement 4.2 of PCI DSS, which states that:

"Requirement 4. Encrypt transmission of cardholder data across open, public networks

***4.2** Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.)." [42]*

5.3.1.2 Recommendations

Due to the fact that the Company's email infrastructure is directly connected with many systems, the cost in order to achieve PCI DSS compliance for these systems as well as the email infrastructure can be

overwhelming for the Company. In addition cardholder information sent via end-user messaging technologies, email, should be rendered unreadable or secured with strong cryptography. As a result of this the Company must implement an encryption mechanism on its email infrastructure, meaning higher compliance cost for the company.

The business function analysis has shown that there is no legitimate need that the Company should use full PANs in the communications listed above. In order to avoid setting within its PCI DSS scope the email infrastructure and systems that directly communicates with the email infrastructure, the Airline should consider stop using full PANs in email communications and replace the full PANs with truncated PANs (e.g. 123456xxxxxx7890).

5.3.2 Transmission of Cardholder through VoIP Infrastructure

5.3.2.1 Current process

As described in Section 4.8.1, the Call Center Department is responsible for performing various activities that involve cardholder data. The Call Center department uses a VoIP telephone system in order to perform the department's activities. As long as cardholder data along with sensitive authentication data (such as CAV2, CVC2, CVV2 or CID) are transmitted through VoIP Infrastructure the Infrastructure should be considered to be in PCI DSS scope. That practically means that VoIP infrastructure should comply with various requirements, such as:

"Requirement 1. Install and maintain a firewall configuration to protect cardholder data

1.2 *Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.*

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment

1.2.2 Secure and synchronize router configuration files.

1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control any traffic from the wireless environment into the cardholder data environment.

1.3 *Prohibit direct public access between the Internet and any system component in the cardholder data environment.*

1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.

1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.

1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.

1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ.

1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.

1.3.6 Implement stateful inspection, also known as dynamic packet filtering.

1.3.7 Place system components that store cardholder data in an internal network zone, segregated from the DMZ and other untrusted networks.

1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties

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

2.2 *Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards (among these standards are Center for Internet Security (CIS), International Organization for Standardization (ISO) and National Institute of Standards Technology (NIST)).*

2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server.

2.2.2 Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system

2.2.3 Configure system security parameters to prevent misuse.

2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

2.3 Encrypt all non-console administrative access using strong cryptography

2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data (according to additional requirements).

Requirement 5. Protect all systems against malware and regularly update anti-virus software or programs

5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).

5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.

5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.

5.2 Ensure that all anti-virus mechanisms are maintained as follows:

- *Are kept current,*
- *Perform periodic scans*
- *Generate audit logs which are retained per PCI DSS Requirement 10.7.*

5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.

5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties. "[42]

5.3.2.2 Recommendations

The Airline should consider fully outsourcing the call center services to a PCI DSS certified Call Center Services Provider and exclude the VoIP Infrastructure and the entire call center environment from its PCI DSS scope. This solution not only would reduce the cost and effort for PCI DSS compliance of the Call Center infrastructure, but it will significantly reduce the scope of the entire PCI DSS compliance project by setting the VoIP Infrastructure out of PCI DSS scope.

5.4 Third Parties' Involvement

As described in Chapter 2 of the current document, multiple other entities are involved in the Company's payment card transaction processing environment. According to the PCI DSS standard, the Airline is responsible for the PCI compliance of its third parties. In case third parties don't comply with PCI DSS requirements, the Airline cannot be certified against the standard. The requirements provided below are mandatory for the Company to comply with, in order to manage its service providers.

"Requirement 12. Maintain a policy that addresses information security

12.8 *Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:*

12.8.1 Maintain a list of service providers.

12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.

12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.

12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.

12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. "[42]

As emerged from the analysis of the Company's business functions, currently the Airline's cardholder data can be found in systems that belong to the following third parties:

- Airports (e.g. Athens Airport – CUSS kiosks)
- Travel Agents
- BSPs & DPCs
- GDSs
- Payment Card Transaction Processors & Acquirers
- Others (e.g. hosting companies)

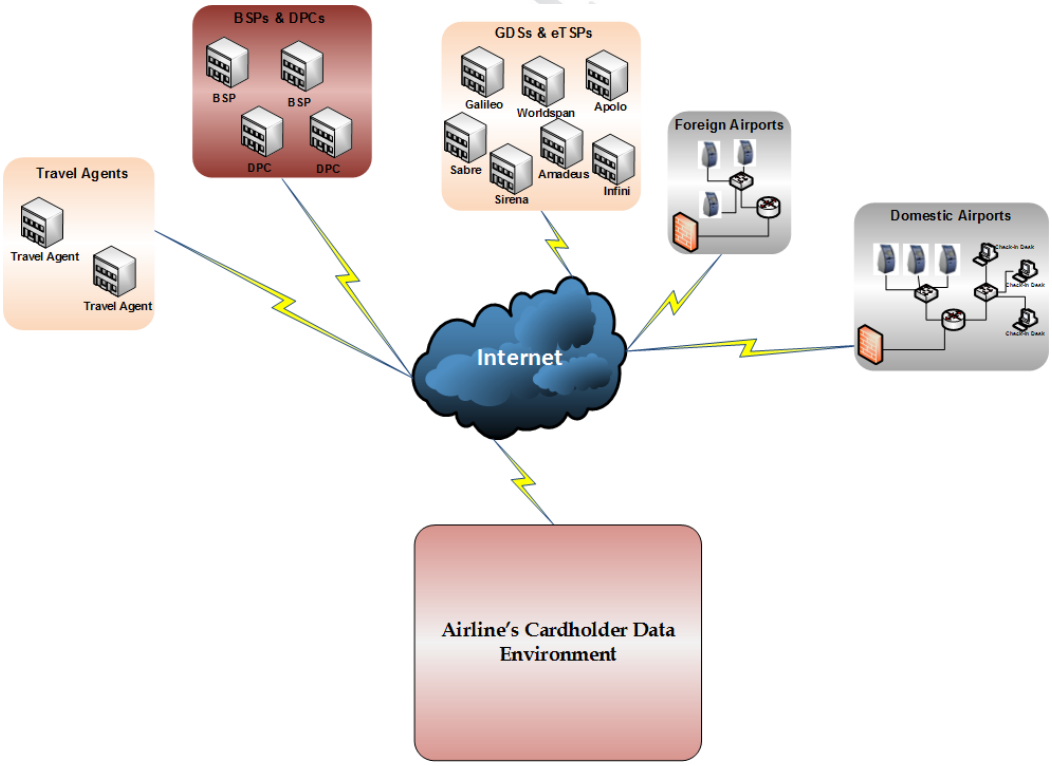

Figure 12 - Environments Excluded from Airline's PCI DSS Scope of Assessment

As an individual airline cannot deliver on its own the PCI compliance of such entities, IATA has taken on the task to lead work on such issues. Based on guidelines provided by Visa Europe and IATA, and after consulting Airline's acquirer, the following third parties environments are excluded from the Airline's Cardholder Data Environment:

- **Travel Agents** - travel agents use an airline's merchant ID when processing airline payment card transactions.
- **Billing & Settlement Plans (BSPs) & Data Processing Centres (DPCs)** – support the sales channels of travel agents.
- **Global Distribution Systems (GDSs)** – A GDS is a worldwide computerized reservation network used by travel agents and airlines as a single point of access for reserving airline tickets.
- **Airports** – provide to airlines various services related to payment cards. For example Common Use Self Service Terminals (CUSS) are used extensively at airports to allow customers to check-in without having to go to a check-in desk, and to process payments from customers for excess baggage, seat upgrades and so on.

Therefore the Airline's PCI DSS assessment scope has been significantly reduced and the focus of the Airline should be turned on its own systems, networks compliance and the compliance of the remaining third parties against the PCI DSS Standard.

5.5 Network Configuration

5.5.1 Flat Network

5.5.1.1 Current process

Although the Airline's network is segmented into different IP networks via VLANs and firewall systems (as depicted in Section 4.9), the network segmentation has not been implemented with the logic to isolate the system components in the network that store, process and / or transmit account data (i.e. cardholder data and sensitive authentication data) from systems that do not. Based on this fact, the Airline's entire network is considered to be in scope of the company's PCI DSS assessment.

Based on the network diagram presented in Section 4.9, the following Airline's environments are currently considered to be within the company's PCI DSS scope of assessment:

- Airline's Headquarters
- Airlines Data Center
- Town Offices

In addition, Airline's Cardholder Data Environment extends to and includes the computing environments of service providers with whom the Company shares account data (i.e. cardholder data & sensitive authentication) and / or uses their environments to host systems that process and transmit account data. In particular, the environments of the following service providers are considered to be within the company's PCI DSS scope of assessment:

- Payment Service Providers
- Acquirers

- Hosting Providers

The Cost in order for the aforementioned environment to comply with PCI DSS Requirements could be tremendous. Indicatively some of the requirements that needs to be addressed for the entire network are the following:

"Requirement 1. Install and maintain a firewall configuration to protect cardholder data

1.2 *Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.*

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment

1.2.2 Secure and synchronize router configuration files.

1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control any traffic from the wireless environment into the cardholder data environment.

1.3 *Prohibit direct public access between the Internet and any system component in the cardholder data environment.*

1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.

1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.

1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.

1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ.

1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.

1.3.6 Implement stateful inspection, also known as dynamic packet filtering.

1.3.7 Place system components that store cardholder data in an internal network zone, segregated from the DMZ and other untrusted networks.

1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties

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

2.2 *Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards (among these standards are Center for Internet Security (CIS), International Organization for Standardization (ISO) and National Institute of Standards Technology (NIST)).*

2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server.

2.2.2 Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system

2.2.3 Configure system security parameters to prevent misuse.

2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

2.3 Encrypt all non-console administrative access using strong cryptography

2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data (according to additional requirements).

Requirement 6. Develop and maintain secure systems and applications

6.4 *Follow change control processes and procedures for all changes to system components. The processes must include the following:*

6.4.1 Separate development/test and production environments
6.4.2 Separation of duties between development/test and production environments
6.4.3 Production data (live PANs) are not used for testing or development
6.4.4 Removal of test data and accounts before production systems become active
6.4.5 Change control procedures for the implementation of security patches and software modifications, including the relevant documentation, the approval by authorized parties, the verification tests and the back-out procedures.

6.5 *Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, according to latest industry best practices (including injection flaws, buffer overflow, insecure cryptographic storage and communications, improper error handling etc.).*
6.6 *For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks.*

Requirement 11. Regularly test security systems and processes

11.2 *Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).*
11.3 *Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification*
11.4 *Use intrusion-detection systems and keep these systems updated.*
11.5 *Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly." [42]*

As can be easily understood the implementation of such controls requires purchasing of expensive hardware and software as well as dedicated employees for the monitoring and maintenance of this project, elements that could increase the cost of compliance to thousands of euros. The recommendations provided below could significantly lessen the cost by reducing number of in-scope systems.

5.5.1.2 Recommendations

Adequate network segmentation ensures the isolation of system components that store, process, or transmit cardholder data from systems that do not. When system components that store, process, or transmit cardholder data are effectively segmented from systems components that do not, the scope of the cardholder data environment can be reduced significantly.

Network segmentation can be achieved through a number of physical or logical means, such as properly configured internal network firewalls, routers with strong access control lists, or other technologies that restrict access to a particular segment of a network.

Based on the above, the following recommendations for the reduction of the company's PCI DSS assessment scope, are recommended.

- **Systems**
    - All systems, including workstations, that store payment card numbers (e.g. database servers, file servers, application servers etc.) are in scope and is recommended to be placed

in a dedicated network zone (e.g. zone A). if other systems are placed in the same network zone they are also considered to be in scope.

- All systems that process or transmit payment card numbers (but do not store) are in scope and is recommended to be placed on a dedicated network zone. If other systems are placed in the same network zone are also considered to be in scope.
- All systems that communicate directly (even through a firewall) with systems that store, process or transmit payment card numbers, and this communication is initiated by the systems under question, are considered to be in scope whether or not payment card numbers are transmitted.
- If a system that stores, process or transmits CHD initiates a communication to a system in a different network zone and the communication does not involve transmission of CHD, the system located in the different network zone is considered to be out of scope.
- Out of scope is also considered to be any other system that doesn't store, process or transmits CHD and has no communication with systems in zones A and/ or B.

It must be noted that systems that store truncated, masked or hashed PANs are out of scope. However, the systems that perform these functions are in scope of PCI DSS.

- **Users / Workstations**
  - Any workstation that stores or process payment card numbers is in scope as well as any other workstation located on the same LAN.
  - Any workstation with direct access to systems that store or process payment card numbers for payment card numbers related communications is considered in scope. Workstations located on the same LAN are in scope too.
  - Any workstation that has access to systems which store or process payment card numbers through Terminal Services and can only view payment card numbers (the workstation does not store or process payment card numbers) is considered in scope. Workstations located on the same LAN are out of scope.
  - Any workstation that has access to systems that store or process payment card numbers through Terminal Services for cardholder data entry is considered in scope. Workstations located on the same LAN are out of scope.
  - Workstations that provide to users the ability to view masked, truncated and / or hashed payment card numbers trough terminal servers are considered to be out of scope.
  - Any workstations that have direct access to systems which store or process payment card numbers and the communications do not involve payment card numbers are in scope. Workstations located on the same LAN are not in scope.
  - Any workstations that have access to systems which store or process payment card numbers through Terminal Services and the communications do not involve payment card numbers are out of scope. Workstations located on the same LAN are out of scope too.
  - Workstations that directly access systems in zones A or B for administrative purposes and have no access to payment card numbers are considered in scope. Workstations located on the same LAN are out of scope too.

- Workstations that access systems in zones A or B for administrative purposes through Terminal Services and have no access to payment card numbers are considered out of scope. Workstations located on the same LAN are out of scope too.
- In the terminal servers farm those terminal servers that are not involved in any payment card numbers related communications must be placed to a different network zone so as to be considered out of scope. Otherwise, the whole terminal servers' farm must be included in the PCI DSS scope.
- Terminal Servers providing access to payment card numbers, even if it is for view only access are recommended to be placed outside the corporate LAN preferably in zone B.

It should be noted that if the Airline decides to implement these recommendations, the company's current cardholder data environment scope will be significantly reduced because systems that store, process and / or transmit payment card numbers will be segmented from those that do not.

6. Conclusions

Airline industry faces very unique challenges when it comes to PCI DSS compliance. The main factor, that makes Airlines different to other merchants that process payment card transactions, is the complexity of their environment. Airline industry has a particular issue in its extended revenue cycle and the extensive use of third party networks and sales locations. Payment data is stored in multiple databases and in numerous desktop applications, while the same data intercept with numerous business and customer service activities. Airports with ticket desks and kiosks as well as travel agents collect payments on behalf of the Airlines. In addition data are collected in-flight, via for example, internet access or purchases in-flight and on-line through the e-commerce sites.

Given the fact that IATA in collaboration with Visa have undertaken the compliance of the third parties evolving in the payment processing of Airlines, the focus of the Airlines should be turned on their own systems. Third parties may not constitute a problem anymore, but even Airlines' own compliance can be very demanding due to the large environment of these companies. Years may be required, in order for such environments to fully comply with the standard, while cost and effort needed will be tremendous.

Even if an organisation manages to comply with the standard, the effort needs to be paid does not ends there. PCI DSS is not just a project, it is an ongoing process of assessment, remediation and reporting. The company should constantly keep track of the changes occurring in its environment and how these changes are being handled and documented and should validate compliance with the standard annually. This might be overwhelming for companies with large infrastructures, such as airlines.

Scope minimisation seems to be the only way towards compliance with the standard. Reducing the scope could lessen the systems and procedures that requirements needs to apply on and consequently the cost and effort required by the Company for PCI DSS compliance. Minimization of the cardholder data environment can be achieved through the reengineering of long-standing business processes and also by restricting cardholder data to as few locations as possible through the elimination of unnecessary data, and consolidation of necessary data.

In addition, it is very often that companies store or exchange full PANs of cardholder data because they used to, without in fact having any business need to do so. Such practices force companies to comply with requirements of the standard that could be excluded and significantly increase the scope of PCI DSS compliance. Companies should review if they make use of the payment card numbers and if they don't they should consider replace full PANs with masked or truncated version of them.

Achieving PCI DSS compliance can be very expensive depending, of course, on the status of the company before compliance, but facing a security breach can be more expensive. However, compliance does not ensure that the company has a secure infrastructure but at least indicates that is following well-known security best practices for certain sensitive data, such as cardholder data. Being compliant gives companies a wildcard for cases of security data breaches. Moreover, PCI DSS certified companies are publically listed in the official list of certified companies that is maintained by PCI SSC. That could provide companies with a trump, that could intelligently use for sales and marketing purposes.

Glossary

Term	Definition
Access Control	Mechanisms that limit availability of information or information-processing resources only to authorized persons or applications.[44]
Account Data	Account data consists of cardholder data plus sensitive authentication data.[44]
Acquirer	Also referred to as "merchant bank," "acquiring bank," or "acquiring financial institution." Entity that initiates and maintains relationships with merchants for the acceptance of payment cards.[44]
ASV	Acronym for "Approved Scanning Vendor." Company approved by the PCI SSC to conduct external vulnerability scanning services.[44]
Authorization	In the context of access control, authorization is the granting of access or other rights to a user, program, or process. Authorization defines what an individual or program can do after successful authentication. In the context of a payment card transaction, authorization occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor.[44]
Bank Settlement Plan (BSP)	Billing and Settlement Plan (BSP) (also known as "Bank Settlement Plan") is an electronic billing system designed to facilitate the flow of data and funds between travel agencies and airlines. The advantage of such an intermediary organization is that instead of each travel agency having an individual relationship with each airline, all of the information is consolidated through the BSP. [46]
BSPlink	BSPlink is the global interface for travel agents and airlines to access the IATA Billing and Settlement Plan (BSP).[47]
Card Verification Code or Value	Also known as Card Validation Code or Value, or Card Security Code. Refers to either: (1) magnetic-stripe data, or (2) printed security features. (1) Data element on a card's magnetic stripe that uses secure cryptographic processes to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand. The following list provides the terms for each card brand: • CAV – Card Authentication Value (JCB payment cards) • CVC – Card Validation Code (MasterCard payment cards) • CVV – Card Verification Value (Visa and Discover payment cards) • CSC – Card Security Code (American Express) (2) For Discover, JCB, MasterCard, and Visa payment cards, the second type of card verification value or code is the rightmost three-digit value printed in the signature panel area on the back of the card. For American Express payment cards, the code is a four-digit unembossed number printed above the PAN on the face of the payment cards. The code is uniquely associated with each individual piece of plastic and ties the PAN to the plastic. The following list provides the terms for each card brand: • CID – Card Identification Number (American Express and Discover payment cards)

Term	Definition
	• CAV2 – Card Authentication Value 2 (JCB payment cards) • CVC2 – Card Validation Code 2 (MasterCard payment cards) • CVV2 – Card Verification Value 2 (Visa payment cards)[44]
Cardholder	Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.[44]
Cardholder Data	At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.[44]
CDE	Acronym for "cardholder data environment." The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.[44]
Change Control	Processes and procedures to review, test, and approve changes to systems and software for impact before implementation.[44]
Compromise	Also referred to as "data compromise," or "data breach." Intrusion into a computer system where unauthorized disclosure/theft, modification, or destruction of cardholder data is suspected.[44]
Computer reservations system (CRS)	A computer reservations system or central reservation system (CRS) is a computerized system used to store and retrieve information and conduct transactions related to air travel, hotels, car rental, or activities. Originally designed and operated by airlines, CRSes were later extended for the use of travel agencies. Major CRS operations that book and sell tickets for multiple airlines are known as Global Distribution System (GDS). [45]
Cryptography	Discipline of mathematics and computer science concerned with information security, particularly encryption and authentication. In applications and network security, it is a tool for access control, information confidentiality, and integrity.[44]
DMZ	Abbreviation for "demilitarized zone." Physical or logical sub-network that provides an additional layer of security to an organization's internal private network. The DMZ adds an additional layer of network security between the Internet and an organization's internal network so that external parties only have direct connections to devices in the DMZ rather than the entire internal network.[44]
FTP	Acronym for "File Transfer Protocol." Network protocol used to transfer data from one computer to another through a public network such as the Internet. FTP is widely viewed as an insecure protocol because passwords and file contents are sent unprotected and in clear text. FTP can be implemented securely via SSH or other technology.[44]
Encryption	Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.[44]
Global Distribution Systems (GDS)	A Global Distribution System (GDS) is a network operated by a company that enables automated transactions between third parties and booking agents in order to provide travel-related services to the end consumers. A GDS can link services, rates and bookings consolidating products and services across all three travel sectors: i.e., airline reservations, hotel

Term	Definition
	reservations, car rentals, and activities. [48]
Hosting Provider	Offers various services to merchants and other service providers. Services range from simple to complex; from shared space on a server to a whole range of "shopping cart" options; from payment applications to connections to payment gateways and processors; and for hosting dedicated to just one customer per server. A hosting provider may be a shared hosting provider, who hosts multiple entities on a single server.[44]
IATA (International Air Transport Association)	The International Air Transport Association (IATA) is the trade association for the world's airlines, representing some 240 airlines or 84% of total air traffic. We support many areas of aviation activity and help formulate industry policy on critical aviation issues. [49]
ID	Identifier for a particular user or application.[44]
IDS	Acronym for "intrusion-detection system." Software or hardware used to identify and alert on network or system anomalies or intrusion attempts. Composed of: sensors that generate security events; a console to monitor events and alerts and control the sensors; and a central engine that records events logged by the sensors in a database. Uses system of rules to generate alerts in response to detected security events.[44]
Injection Flaws	Vulnerability that is created from insecure coding techniques resulting in improper input validation, which allows attackers to relay malicious code through a web application to the underlying system. This class of vulnerabilities includes SQL injection, LDAP injection, and XPath injection.[44]
LAN	Acronym for "local area network." A group of computers and/or other devices that share a common communications line, often in a building or group of buildings.[44]
Masking	In the context of PCI DSS, it is a method of concealing a segment of data when displayed or printed. Masking is used when there is no business requirement to view the entire PAN. Masking relates to protection of PAN when displayed or printed.[44]
Merchant	For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.[44]
Network Security Scan	Process by which an entity's systems are remotely checked for vulnerabilities through use of manual or automated tools. Security scans that include probing internal and external systems and reporting on services exposed to the network. Scans may identify vulnerabilities in operating systems, services, and devices that could be used by malicious

Term	Definition
	individuals.[44]
Network Segmentation	Also referred to as "segmentation" or "isolation." Network segmentation isolates system components that store, process, or transmit cardholder data from systems that do not. Adequate network segmentation may reduce the scope of the cardholder data environment and thus reduce the scope of the PCI DSS assessment.[44]
PAN	Acronym for "primary account number" and also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.[44]
Payment Cards	For purposes of PCI DSS, any payment card/device that bears the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or Visa, Inc.[44]
PCI	Acronym for "Payment Card Industry."[44]
PCI DSS	Acronym for "Payment Card Industry Data Security Standard."[44]
Penetration Test	Penetration tests attempt to identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components. Penetration testing includes network and application testing as well as controls and processes around the networks and applications, and occurs from both outside the environment (external testing) and from inside the environment.[44]
PIN	Acronym for "personal identification number." Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typical PINs are used for automated teller machines for cash advance transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder's signature.[44]
PIN Block	A block of data used to encapsulate a PIN during processing. The PIN block format defines the content of the PIN block and how it is processed to retrieve the PIN. The PIN block is composed of the PIN, the PIN length, and may contain subset of the PAN.[44]
POS	Acronym for "point of sale." Hardware and/or software used to process payment card transactions at merchant locations.[44]
QSA	Acronym for "Qualified Security Assessor." QSAs are qualified by PCI SSC to perform PCI DSS on-site assessments. Refer to the QSA Qualification Requirements for details about requirements for QSA Companies and Employees.[44]
Risk Analysis / Risk Assessment	Process that identifies valuable system resources and threats; quantifies loss exposures (that is, loss potential) based on estimated frequencies and costs of occurrence; and (optionally) recommends how to allocate resources to countermeasures so as to minimize total exposure.[44]
ROC	Acronym for "Report on Compliance." Report documenting detailed results from an entity's PCI DSS assessment.[44]
SAQ	Acronym for "Self-Assessment Questionnaire." Reporting tool used to document self-assessment results from an entity's PCI DSS

Term	Definition
	assessment.[44]
Scoping	Process of identifying all system components, people, and processes to be included in a PCI DSS assessment. The first step of a PCI DSS assessment is to accurately determine the scope of the review.[44]
Secure Coding	The process of creating and implementing applications that are resistant to tampering and/or compromise.[44]
Sensitive Authentication Data	Security-related information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.[44]
Service Provider	Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. If an entity provides a service that involves only the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although they may be considered a service provider for other services).[44]
Track Data	Also referred to as "full track data" or "magnetic-stripe data." Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions. Can be the magnetic-stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe.[44]
Transaction Data	Data related to electronic payment card transaction.[44]
Truncation	Method of rendering the full PAN unreadable by permanently removing a segment of PAN data. Truncation relates to protection of PAN when stored in files, databases, etc.[44]
VLAN	Abbreviation for "virtual LAN" or "virtual local area network." Logical local area network that extends beyond a single traditional physical local area network.[44]
VPN	Acronym for "virtual private network." A computer network in which some of connections are virtual circuits within some larger network, such as the Internet, instead of direct connections by physical wires. The end points of the virtual network are said to be tunneled through the larger network when this is the case. While a common application consists of secure communications through the public Internet, a VPN may or may not have strong security features such as authentication or content encryption. A VPN may be used with a token, smart card, etc., to provide two-factor authentication.[44]

References

[1] David S. Evans and Richard Schmalensee, "The Digital Revolution in Buying and Borrowing", Paying with Plastic, Massachusetts Institution of Technology, 2005

[2] Monika E. Hartmann, "E-Payments Evolution", European Central Bank, Frankfurt, Springer, 2006

[3] Rajesh Kumar Dilli, OWASP "Security of Payment cards (Credit/Debit) in E-commerce applications" [Online]. Available: https://www.owasp.org/images/f/f7/Security_of_Payment_cards.doc

[4] Reuters. (2011, April 26) "Factbox: Sony breach latest in string of cyber attacks" [Online]. Available: http://www.reuters.com/article/2011/04/26/us-sony-stolendata-factbox-idUSTRE73P7GF20110426

[5] Tony Bradley, PCWorld. (2011, Apr 29) "Sony Says Data Is Protected, Attackers Say It's For Sale" [Online]. Available: http://www.pcworld.com/article/226737/sony_says_data_is_protected_attackers_say_its_for_sale.html

[6] Wikipedia. "TJX Companies" [Online]. Available: http://en.wikipedia.org/wiki/TJX_Companies

[7] Jaikumar Vijayan. (2007, March 29) "TJX data breach: At 45.6M card numbers, it's the biggest ever" [Online]. Available: http://www.computerworld.com/s/article/9014782/TJX_data_breach_At_45.6M_card_numbers_it_s_the_biggest_ever

[8] PricewaterhouseCoopers (2008). "Focus on risk, and compliance will follow: Overcoming the challenges of Payment Card Industry requirements" [Online]. Available: https://www.pwc.com/en_US/us/issues/data-loss-prevention/assets/payment_card_requirements.Pdf

[9] PCI Security Standards Council. "What Is the PCI Security Standards Council?" [Online]. Available: https://www.pcisecuritystandards.org/security_standards/role_of_pci_council.php

[10] PCI Security Standards Council. "Organizational Structure" [Online]. Available: https://www.pcisecuritystandards.org/organization_info/org_fact_sheet.php

[11] PCI Security Standards Council (2008). "PCI Security Standards Council, Payment Card Industry Security Standards: Standards Overview" [Online]. Available: https://www.pcisecuritystandards.org/pdfs/pcissc_overview.pdf

[12] PCI Security Standards Council (2013, November). "Payment Card Industry (PCI) Data Security Standard , Requirements and Security Assessment Procedures" [Online]. Available: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

[13] Dimitris Ergazakis, "PCI DSS at a Glance", Enterprise IT Security, February, 2011

[14] Techtarget (2013, November). "The history of the PCI DSS standard: A visual timeline" [Online]. Available: http://searchsecurity.techtarget.com/feature/The-history-of-the-PCI-DSS-standard-A-visual-timeline

[15] Visa. "CISP Overview" [Online]. Available: http://usa.visa.com/merchants/protect-your-business/cisp/index.jsp?ep=v_sym_cisp

[16] XYPRO Technology Corporation (2011, March). "XYGATE® & PCI COMPLIANCE PCI DSS Version 2.0" [Online]. Available: https://www.xypro.com/whitepapers/White_Paper_-_PCI_Compliance.pdf

[17] PCI Security Standards Council (2008, October 1). "PCI Security Standards Council Releases Version 1.2 of PCI Data Security Standard", Press release.

[18] PCI Security Standards. "Supporting Documents PCI DSS" [Online]. Available: https://www.pcisecuritystandards.org/security_standards/documents.php?category=supporting

[19] PCI Security Standards Council (2009, August 10). "PCI Security Standards Council on minor corrections to PCI DSS and PA-DSS standards documentation"

[20] PCI Compliance Forum (2011, April 9). "The History of PCI Compliance Versions" [Online]. Available: http://pcicomplianceforums.com/content/124-The-History-of-PCI-Compliance-Versions

[21] PCI Security Standards Council (2010, October 28). "PCI Security Standards Council Releases Version 2.0 of the PCI Data Security Standard and Payment Application Data Security Standard", Press release

[22] PCI Security Standards Council (2013, November 07). "PCI Council Publishes PCI DSS and PA-DSS Version 3.0"

[23] PCI Security Standards Council (2013, August). "Version 3.0 Change Highlights" [Online]. Available: https://www.pcisecuritystandards.org/documents/DSS_and_PA-DSS_Change_Highlights.pdf

[24] Steve Wright, "PCI DSS A practical guide to implementation", United Kingdom, 2008

[25] PCI Security Standards Council. "Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms" [Online]. Available: https://www.pcisecuritystandards.org/security_standards/glossary.php

[26] Discover. "Identifying Merchant Level" [Online]. Available: http://www.discovernetwork.com/merchants/data-security/identifying-organizations.html

[27] Visa. "Compliance validation details for merchants" [Online]. Available: http://usa.visa.com/merchants/protect-your-business/cisp/merchant-pci-dss-compliance.jsp

[28] American Express "Merchant Levels" [Online]. Available: https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=merchinfo&ln=en&frm=US&tabbed=merchantLevel

[29] Richard S. Carson & Associates, Inc. "PCI Merchant Requirements" [Online]. Available: http://www.carsoninc.com/services/PCImerchant.html

[30] PCI Security Standards Council (2013, May). "Approved Scanning Vendors" [Online]. Available: https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v2.pdf

[31] PCI Security Standards Council. "PCI DSS Self-Assessment Questionnaire (SAQ)" [Online]. Available: https://www.pcisecuritystandards.org/merchants/self_assessment_form.php

[32] PCI Security Standards Council. "Understanding the SAQs for PCI DSS v3.0" [Online]. Available: https://www.pcisecuritystandards.org/documents/Understanding_SAQs_PCI_DSS_v3.pdf

[33] Dr Keith Mason, Air Transport Management Seminar, Lisbon (January 2008). "Airline Distribution" [Online]. Available: http://recil.grupolusofona.pt/bitstream/handle/10437/2631/artg10.pdf?sequence=1

[34] Visa. "Visa International Best Practices Guides" [Online]. Available: http://visa.com.ua/ac/pdf/airline_best_practice.pdf

[35] Wikipedia. "Airline reservation system" [Online]. Available: http://en.wikipedia.org/wiki/Airline_reservations_system

[36] IATA. "Billing and Settlement Plan (BSP)" [Online]. Available: http://www.iata.org/services/finance/bsp/Pages/index.aspx

[37] IATA. "How a BSP works" [Online]. Available: http://www.iata.org/services/finance/bsp/Pages/how-bsp-works.aspx

[38] Wikipedia. "Common-use self-service" [Online]. Available: http://en.wikipedia.org/wiki/Common-use_self-service

[39] Transactionage (2011, September 22) "PCI DSS in the Airline Sector" [Online]. Available: http://www.transactionage.com/2011/09/22/pci-dss-in-the-airline-sector/

[40] IATA. " Payment Card Industry Data Security Standards (PCI DSS)" [Online]. Available: http://www.iata.org/services/finance/Pages/pci-dss.aspx

[41] PCI Security Standards Council (2008). " PCI Data Storage Do's and Don'ts" [Online]. Available: https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf

[42] PCI Security Standards Council. "Payment Card Industry (PCI) Data Security Standard Version 3" [Online]. Available: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

[43] PCI Security Standards Council (PCI SSC) "Information Supplement: Protecting Telephone-based Payment Card Data", March 2011

[44] PCI Security Standards Council (2014, January)." Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS), Glossary of Terms,

Abbreviations, and Acronyms"[Online]. Available:
https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3.pdf

[45] Wikipedia. "Computer reservations system" [Online]. Available:
http://en.wikipedia.org/wiki/Computer_reservations_system

[46] Wikipedia. "Billing and Settlement Plan" [Online]. Available:
http://en.wikipedia.org/wiki/Billing_and_Settlement_Plan

[47] IATA. "BSPlink - A Global Vision" [Online]. Available:
https://www.bsplink.iata.org/bsplink14/entrada/BSPL_E_PI.html

[48] Wikipedia. "Global Distribution System" [Online]. Available:
http://en.wikipedia.org/wiki/Global_Distribution_System

[49] IATA. "About Us" [Online]. Available: http://www.iata.org/ABOUT/Pages/index.aspx