



PCI DSS Positioning

White paper

Table of Contents

Introduction – Why should we care about protecting data in the first place?	4
<i>UK Background Information</i>	4
<i>US background Information</i>	4
Common denominators in US & EU legal and industry data security frameworks	5
Data Breach and Non-Compliance Costs	5
<i>Data at rest vs Data in motion</i>	6
I have identified the type of data I need to protect – but where is it?	7
An introduction to PixAlert Critical Data Auditor – “PixAlert Auditor”	9
<i>Introduction to PixAlert Auditor Scanning Process</i>	9
<i>Corrective Action - What do PixAlert Auditor scan results allow me to do to comply with PCI DSS</i> ..	10
Benefits of Using PixAlert as part of your PCI DSS tool set.....	10
<i>PixAlert Monitor beyond PCI DSS Compliance</i>	11
Case Study - PixAlert Monitor for Security Assessors.....	12
Appendix A – Analysis of Bob Russo’s and PCI SSC officials opinions on storing credit cardholder data and reducing PCI DSS Scope.....	13
So what does it mean for merchants and how can PixAlert Auditor help?.....	13
Appendix B - PCI DSS Overview and PixAlert Compliance Assist Capabilities	14
<i>Consequences of non Compliance with PCI DSS</i>	15
<i>Focus on Cardholder Data Storage</i>	15
<i>PixAlert Compliance Assistance Capabilities</i>	18
Requirement 3 – Protect stored data	18
Requirement 6 – Develop and maintain secure systems and applications	19
Requirement 7 – Restrict access to data on a business need to know.....	20



Requirement 11 – Regularly test security systems and processes	20
Appendix C - PixAlert Auditor Scanning Process.....	21
Step 1 – Prepare Scanning Rules.....	21
Step 2 – Select Target Components.....	21
Step 3 –Scan Target Components	22
Step 4 – Review Phase	22
Step 5 – Report Production.....	22
Appendix D - Graphical Representation of PixAlert Auditor’s scanning process.....	24

Introduction – Why should we care about protecting data in the first place?

“Too many data breaches involving sensitive and personal data as well as massive credit card breaches are forcing governments and industry bodies to regulate the market”

UK Background Information

Over the past five years there have been no shortages of data breaches in Europe or in the US. The UK has been badly hit with a string of multiple data leakage issues involving major financial institutions and government departments such as HM Customs ending up with losing two unencrypted disks containing details of 25m citizens. The UK Data Protection Act 1998 includes 8 principles which are aimed, amongst other objectives, at ensuring that sensitive information held by businesses and government on their customers/citizens is obtained fairly, for clear purposes only, maintained up to date, maintained securely and is not provided to third parties if the data owner has not agreed to it and that data is not transferred outside the EU unless the country receiving the information has at least the same level of data protection as in the EU. It is also worth noting that the recent changes to the UK Data Protection Act empower the Information Commissioner to impose fines of up to £ 500,000.00 and whilst he has indicated that fines would take into account the size of the organization breached and the type of breach, SMEs can expect a steep rise in the average fine such that ICO fines will impact their P&L.

US background Information

In the US, there has been a significant number of high-profile data breach cases over the past few years. For instance, in 2007 TJX Companies Inc., the global conglomerate that includes T.J. Maxx, T.K. Maxx, Marshalls and Winners, lost at least 45 million credit cards after systems were penetrated by hackers. In 2009 Networks at Heartland Payment Systems were hacked, exposing data on 130 million credit card users. In fact Convicted TJX hacker Albert Gonzalez was sentenced in March 2010 to 20 years and a day, and fined \$25,000 for his role in breaches into Heartland Payment Systems, 7-Eleven and other companies. He apparently nicknamed the credit card hack “Operation Get Rich or Die Tryin”¹.

In 2009, the Network Solutions data security breach exposes a half-million credit card numbers. In addition, breaches in the US must be reported in 45 US States and Federal Breach Disclosure law is on its way. It is also worth noting that the State of Massachusetts has just enacted MA 201CMR

¹ <http://news.softpedia.com/news/New-Conviction-in-TJX-Breach-Case-137369.shtml>

17.00 which requires any organization holding personal information on Massachusetts residents to put in place a Written Information Security Program (WISP) which is a set of policies and procedures aimed at safeguarding personal information which can be a combination of name and credit card holder data. It also requires staff to go through an awareness training program, requires that a Data Security Co-ordinator be appointed to take overall responsibility for security and requires that vulnerability management be performed on a regular basis.

The State of Nevada has also enacted legislation making PCI DSS a legal requirement under certain conditions and requiring that sensitive card holder data be encrypted.

Common denominators in US & EU legal and industry data security frameworks

All legal and industry data security frameworks require that a single person be designated as ultimately responsible for securing sensitive personal data and credit card holder data. All of them require a mix of policies and procedures governing how data is to be acquired, processed, transmitted and, for most of them, discarded or decommissioned. All of them require security solutions such as firewalls, encryption, back-up and IDS to be implemented on networks. A vast majority require staff to be trained so that they fully understand the value of sensitive information and credit card holder data.

They all one key thing in common – they require your business to know where your sensitive data is!

Data Breach and Non-Compliance Costs

There are various fines and costs associated with non-compliance with legal and industry frameworks, especially in the event of a breach. For instance most merchants would be at level 3 & 4 for PCI DSS² and consequences for non complying with PCI DSS in the EU are as follows³:

- €10,000 for the initial breach (rising to €25,000 for subsequent breach)
- €5,000 for each additional month while remedial work is undertaken
- All remedial costs such as replacement cards (€50 per card is common)

² See Appendix B - PCI DSS Overview in this White Paper

³ <http://www.rbsworldpay.com/pcidss/index.php?page=penalties&l=4>

- All costs associated with fraud on the cards as a result of negligence
- Termination of ability to accept card payments

It is also worth noting that should entities be breached while they are not in compliance with the standard this will result in automatic elevation to a Level 1 merchant with all the associated fines and requirements.

In terms of Data Protection Act compliance, most EU Information Commissioners or Data Protection Commissioners also have the powers to seize IT systems and printed documentation as well as to impose fines, whose levels depend on the Member States.

Data at rest vs Data in motion

It is worth considering the fact that both legal and industry security frameworks make the distinction between data at rest and data in motion, in other words the difference between data which is stored on an organization's network -paper based information as well as hardware assets such as laptops, desktops, PDAs, multifunctional printers with hard drives - and data that is being transmitted between two physical or logical locations whether they belong to the organization or are made between the organization and third parties.

When data is held either physically or logically (i.e. electronically) by an organization on premise, it tends to be protected by a mix of policies and procedures and technical solutions. A number of legal and industry security frameworks started looking at data in motion around 2005, to ensure that data being transferred both physically (i.e paper based or on hardware moved from one location to another) or logically over public networks such as the Internet be subject to higher security standards such as those included in the payment card Industry data Security Standards (PCI DSS).

I have identified the type of data I need to protect – but where is it?

Most organizations collect data from multiple sources such as e-mail, web forms and web services. However when asked how information is collected and where the data resides once it is collected most organizations are unable to demonstrate to security auditors that appropriate security measures are in place to protect data throughout its lifecycle in the organization. This is a key problem especially with regards to credit card holder data for PCI DSS compliance which states that organizations need to protect cardholder data in the in-scope cardholder data environment.

Cardholder data (“CHD”) is described by the PCI DSS Council as follows:

“Full magnetic stripe or the PAN plus any of the following:

- Cardholder name
- Expiration date
- Service Code”⁴

Cardholder data environment is described as follows:

“Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment”⁵

So the key for your organization is to map out where cardholder data resides on your systems. In order to identify where CHD is, you need to map out your organization’s ecosystem. How many business units are involved in either processing, transmitting or storing CHD? What third parties are involved in the process, if any, and if so, what CHD can they see and how? Where is CHD located on your systems.

It is important to note that PCI DSS applies to all network components⁶ which are used to either transmit, store or process CHD so this will include file servers, mail servers, desktops, laptops and potentially PDAs. USB based memory keys are typically not used to transmit store or process CDH,

⁴ http://selfservice.talisma.com/display/2/_index1.aspx?tab=glossary&r=0.5681133

⁵ http://selfservice.talisma.com/display/2/_index1.aspx?tab=glossary&r=0.5681133

⁶ http://selfservice.talisma.com/display/2/_index1.aspx?tab=glossary&r=0.9984323

however if they are used for that purpose in your environment, then they are regarded as a network component with regards to PCI DSS compliance and are in scope.

Once you have documented your ecosystem, you need to document the network structure through accurate network diagrams showing how in scope network components are protected. It is also useful to show how the whole network is protected and to demonstrate how CHD network and non CHD networks are segregated.

The next step is to document CHD data flow. What happens to CHD once it is on your network interacting with various actors belonging to your ecosystem. Mostly, your organization needs to demonstrate that it is in full control over where CHD is. The next challenge is to address the discovery and continuous monitoring of CHD within your environment and this is where PixAlert can help.

It also worth considering that the Data Protection Act 1998 is based on the EU Data protection directive of 1995 which makes distinction between data controllers who are ultimately responsible for ensuring that data is processed by anyone in the organization according to the Directive's guidelines, and data processors who may be anyone within the organization with access rights to work on data protected by the Directive. This means that organizations do not only have to classify data itself but also means that they need to map out who has access to what data and for what purpose. This also covers third parties who may be allowed access to data for business purposes. Third parties are regarded as data processors and they must maintain security around the data they process, however the overall responsibility for the data always remain with the data controllers. This is a concept that is evolving with the Article 29 working party which is primarily made of all the information commissioners in the EU. They are currently revising the definitions of data controllers and processors and have published more detailed information on the differences between controllers and processors which Security Officers need to be familiar with⁷.

⁷ <http://www.huntonprivacyblog.com/2010/03/articles/european-union-1/article-29-working-party-issues-opinion-on-the-concepts-of-controller-and-processor/index.html>

An introduction to PixAlert Critical Data Auditor – “PixAlert Auditor”

PixAlert Auditor scans network data at rest. It helps your organization map out where CHD is located on network components focusing especially on mail servers (lotus/Domino/Exchange), file servers, users computers hooked to the network (laptops/desktops).

PixAlert Auditor is able to perform a CHD discovery audit in a non-intrusive mode which means that it searches for CHD without disrupting systems or affecting performance. PixAlert auditor can out of the box look for PANs, expiry dates, PIN numbers, CVVs.

Custom expressions can also be built to look for specific CHD components mixes, for instance PAN + CVV only.

Introduction to PixAlert Auditor Scanning Process

PixAlert follows a well defined process aimed at ensuring that it can help organizations map out their CHD and ensure that no CHD is located in the parts of the network that are not in scope for PCI DSS. This process is made of five key steps⁸.

Step 1 –Prepare Scanning Rules

Step 2 –Select Target Components

Step 3 –Scan Target Components

Step 4 – Review Results

Step 5 – Produce Report

The outcome of this process is a detailed report which allows organizations to take corrective action towards achieving and maintaining PCI DSS compliance.

⁸ More detailed information about each step of the process is available in Appendix D of this White Paper.



Corrective Action - What do PixAlert Auditor scan results allow me to do to comply with PCI DSS

PixAlert allows your organization to perform extensive and intelligent Data Mapping to understand the scope of PCI DSS applying to your environment. By using PixAlert Auditor, entities can discover where CHD actually resides and compare findings with their current documentation work. PixAlert Auditor provides accurate and organized information that allows entities to get full visibility over the extent of their CHD. Coupled with existing diagrams and data flows, the CHD information included in the reports produced by the PixAlert Auditor scans provide CSOs, Security Staff and IT administrators with the information they need to understand where CHD is Stored on their network components and identify components they did not include in the scope of internal preparation for for PCI DSS before Qualified Security Assessors do.

As a result, entities can fully document where CHD is located and perform an updated risks assessment. This process involves updating existing policies & procedures governing how CHD flow is being protected and it needs to include a regular data mapping exercise as well as a requirement to perform CHD discovery on a regular basis, ideally every 30 days.

Technical corrective action is typically required after the first PixAlert Auditor scan is performed because it tends to identify components storing unencrypted CHD and/or CHD elements which need to be better protected.

PixAlert security consultants also highly recommend that customers incorporate PixAlert Auditor scans in their Continuous Compliance strategy which are aimed at ensuring that PCI DSS compliant remain compliant and revalidate compliance. As such PixAlert Auditor scans allow entities to continually monitor the in-scope and out-of-scope networks for new instances or CHD or CHD elements. This is a key component of any ongoing security strategy since environments always change

Benefits of Using PixAlert as part of your PCI DSS tool set

At the community meeting for Participating organizations of the PCI DSS Council in Las Vegas, US , in 2009, Troy leach, CTO of PCI DSS SSC, insisted on “cardholder data to be mapped out in such a way that assessors can understand your organization’s data flow and assess security around it according to the controls of PCI DSS 1.2”

The ability to be able to discover and map CHD is of great benefits to entities. It allows them to gain or regain control over how CHD is being stored, transmitted or processed. Having 100% control over



CHD on your cardholder environment allows entities to properly implement the technical, procedural and skills transfer controls required by PCI DSS.

Reducing the Scope of PCI DSS is also one of the key recommendations made by the PCI DSS Council. It advises entities not to store information if this information is not absolutely required for business purposes. PixAlert Auditor is a key enabling technology for PCI DSS scope reduction by allowing organisations to discover data for classification. Once classified the data can be protected or removed.

PixAlert PCI Compliance Assistance Capabilities

The PixAlert Critical Data Auditor product can discover unprotected credit card information on the corporate network. This has particular relevance to the following PCI capability requirements listed in the summary table below:

Requirement	How we help
3	We can detect that data is stored unprotected
6	We can detect if systems leave an unwanted foot print that might compromise security (e.g. transaction log)
7	We can detect data in unexpected places (e.g. a business unit unrelated to PCI)
11	We can be one of the security assessment tools

Please see Appendix C for the full requirements outline describing the PixAlert Critical Data product assistance capabilities for PCI compliance.

PixAlert Monitor beyond PCI DSS Compliance

Most organizations who need to comply with PCI DSS also have to comply with either US and/or EU data privacy and data protection regimes. PixAlert Auditor’s capabilities extend beyond PCI DSS and the ability to discover and map out CHD.

PixAlert Auditor allows your organization to discover and map out UK social Security Numbers (UK SSN), US Social security Numbers (US SSN), Irish PPS numbers.

This allows organizations to use PixAlert Auditor as part of their tool set to ensure compliance with US state privacy laws such as MA 201 CMR 17.00, UK Data Protection Act 1998, Irish Data Protection



Act 2003 and US Higher Education Act Opportunity (HEAO), all of which require organizations to map out specific data sets so as to protect them according to specific security guidelines.

It is also worth noting that ISO 27001 requires organizations to classify and map out its physical and logical assets which typically include sensitive information, CHD and any type of Personally Identifiable Information.

Case Study - PixAlert Monitor for Security Assessors

Qualified Security Assessors (QSAs) who conduct on-site security assessments for Level 1 merchants now need to be more thorough than ever. This is due to the fact that a Quality Assurance (QA) process has been put in place in 2009 to ensure that all assessments were conducted using the same level of security expertise and experience however it is also aimed at ensuring that assessments do not leave out any aspect of CHD security which may have been overlooked under previous rules.

Using PixAlert Auditor's CHD discovery and mapping capabilities allows QSAs to ensure that their assessment is fully comprehensive and thoroughly checks that all CHD is indeed in the in-scope part of the cardholder environment as presented to them by the entity. Running a PixAlert Auditor scan on the whole network also allows QSAs to ensure that the scope is well defined and enables them, as trusted security advisors, to help entities reduce the scope of PCI DSS which is a win-win situation for both the assessor and the organization being assessed.

Appendix A – Analysis of Bob Russo’s and PCI SSC officials opinions on storing credit cardholder data and reducing PCI DSS Scope

Bob Russo is the General Manager of the PCI Security Standards Council. As such he oversees all activities related to PCI DSS, PA-DSS and PTS. He is also the spokesperson for PCI SSC worldwide.

Russo understands that the card data security standards are often hard to understand especially for small merchants. In numerous blogs, testimonies and articles he has explained that PCI SSC is “concerned about where credit card data is being collected and stored”.⁹

This message is echoed by other members of the Council such as Amex rep Seana Pitt: “PCI Security Standards Council officials say organizations, especially those still in the initial phases of addressing compliance, should make their priority eliminating the storage of unnecessary information, known as track data. This includes the data contained on the magnetic strip of the card, including the PIN and credit card verification codes. The message: Don't store it if you don't need it.”¹⁰

In fact the PCI SSC commissioned in 2009 a study conducted by Price Waterhouse Coopers. The goal of the study, which was presented both at the at the PCI Security Standards Council's Community Meetings in the US and in Europe respectively in September 2009 and October 2009, was to identify a number of technologies that merchants may be able to leverage to reduce their scope in complying with the Payment Card Industry Data Security Standard.

So what does it mean for merchants and how can PixAlert Auditor help?

PixAlert Auditor allows your organization to search for and map out where cardholder data is located on your environment. By knowing where this data is you can align your cardholder data storage strategy with the advice of PCI SSC officials and pro-actively ensure that you only store cardholder elements you are allowed to store only if you have a business requirement to do so.

In doing so your organization is able to re-organize its in-scope cardholder environment to minimize it and therefore reduce the scope of PCI DSS which is fully aligned with the advice provided by Bob Russo and his team.

PixAlert Auditor allows you to regain control of your cardholder environment and PCI DSS scope!

⁹ http://news.cnet.com/8301-27080_3-10448197-245.html

¹⁰ <http://www.scmagazineus.com/cover-story-protecting-credit-card-numbers-has-a-positive-impact-on-business/article/35307/>

Appendix B - PCI DSS Overview

PCI DSS was created in December 2004 by Visa, MasterCard, Discover, Amex and JCB as were coming under pressure from merchants, payment service providers and acquiring banks to standardize their individual brand security accreditation with one single benchmarking document. To do so they created PCI DSS which is administered by the PCI Security Standards Council.

“The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.”¹¹

PCI DSS applies to any entity processing, transmitting or storing credit cardholder data. As such it typically applies to merchants of all sizes from corner shops to multi-national retail organizations, payment service providers & gateways as well as acquiring banks.

PCI DSS is one of three standards created by the PCI Security Standards Council. PA-DSS, Payment Application Data Security Standard, applies to payment applications which are commercialized, primarily for payment service providers, payment gateways, applications running on point of sale device but also for merchants if their in-house payment application is sold to third parties. PTS stands for PIN Transaction Security and typically applies to hardware security of Point-Of-Sales devices.

In terms of PCI DSS, there are four levels for merchants. The most onerous level is level 1 for merchants with over 6 million credit card transactions annually, then level 2 with merchants with between 1 million and 6 million credit card transactions annually, then level 3 for merchants with between 20,000 and 1 million credit card transactions annually and finally level 4 merchants with less than 20,000 credit card transactions annually. The transaction count covers all type of transactions whether through point of sale device, e-commerce or phone/mail order.

Level 1 merchants must be assessed annually by a Qualified Security Assessor¹² and must perform a quarterly scan of their external facing IPs linked to the cardholder data environment. Level two merchants. Level two merchants need to complete a Self Assessment Questionnaire and quarterly scans, level 3 merchants need to complete a Self Assessment Questionnaire and quarterly scans, level 4 merchants need to complete a Self Assessment Questionnaire and quarterly scans. Scans have to be performed by an Approved Scanning Vendor (ASV)¹³ and Self Assessment Questionnaires

¹¹ https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

¹² https://www.pcisecuritystandards.org/qa_asv/index.shtml

¹³ https://www.pcisecuritystandards.org/qa_asv/index.shtml

are typically sent to the acquiring banks or payments service providers who then report on their merchants compliance to the brands. However, please note, that some validation requirements vary by country and by brand. For full information check directly with your brand. The following site also offers guidance on validation mechanisms for all brands:

https://www.pcisecuritystandards.org/qa_asv/index.shtml

Consequences of non Compliance with PCI DSS

If merchants are breached they are automatically moved up to level 1 which means that they will have to have an onsite QSA audit every year, notwithstanding having to have a forensic investigation performed and the fact that they will more than likely have to pay for legal fees.

Additional items for considerations by merchants are as follows:

- Increase in Fraud Levels
- Harm to your business
- Card Re-issuance Costs (Costs passed to the merchant)
- Fines might be imposed on your business by the brands and by banks
- Inconvenience to customer & loss of consumer Confidence
- Adverse Publicity for your organization
- Name & shame
- Brand & Reputation Damage
- Legislative Interest – Threat of Governmental Regulation:
 - Already have PCI DSS into Law in Nevada & Minnesota
 - This will become federal Law in the US with 5 years & EU will follow

Focus on Cardholder Data Storage

PCI DSS applies if PAN is stored, transmitted or processed. If not, it does not apply. However best practice security as well as some US state and federal law and EU law require that personal

information such as the association of cardholder name and expiration date or cardholder name and service code be protected from a security view point.

Official guidance from PCI DSS is as follows¹⁴:

	Data element	Storage Permitted	Protection Required	PCI DSS Req 3.4
Card Holder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name	Yes	Yes	Yes
	Service Code	Yes	Yes	No
	Service Code	Yes	Yes	No
	Expiration Date	Yes	Yes	No
Sensitive Authentication Data	Full Magnetic Stripe Data	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

Please note that additional information on PCI DSS applicability and storage guidance is available in the PCI DSS Requirements and Security Assessment Procedures, v1.2.1. This table provides basic information only.

Organizations are asked to be able to map out where they keep cardholder data and which data elements they keep and how they keep them secure according to PCI DSS controls.

The standard is divided into 12 sections covering 6 key goals and is structured in requirements (grouped by heading) as follows:

Build and Maintain a Secure Network

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

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

¹⁴ PCI DSS Requirements and Security Assessment Procedures, v1.2.1

Protect Cardholder Data

Requirement 3: Protect Stored Data

Requirement 4: Encrypt transmission of cardholder and sensitive information across public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and Maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7: Restrict Access to Data by Business Need to know

Requirement 8: Assign a unique ID to each person with Computer Access

Regularly Monitor and Test Networks

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

Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors

Each requirement has a set of specific controls which can be categorized as policies and procedures, technical controls and skills transfer requirements. There are over 200 controls in PCI DSS v1.2.1 and each control is associated with a testing procedure.

Appendix C – PixAlert PCI Compliance Assistance Capabilities

The PixAlert Critical Data Auditor product can discover unprotected credit card information on the corporate network. This has particular relevance to the detailed requirements as outlined in the PCI standard and described in the remainder of this document on how the PixAlert Critical Data Auditor product can:

Requirement 3 – Protect stored data

Requirement	Comment
3.1 Keep cardholder information storage to a minimum. Develop a data retention and disposal policy. Limit your storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.	PixAlert Critical Data Auditor can be used to discover information that may be identified as exceeding business retention requirements.
3.2 Do not store sensitive authentication data subsequent to authorization (not even if encrypted):	
3.2.1 Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data	PixAlert Critical Data Auditor can discover log files that may contain full stripe data (CC number + Name + Date Expired ...). It can do this across desktops, file servers and email.
3.2.2 Do not store the card-validation code—(Three-digit or four-digit value printed on the front or back of a payment card (e.g., CVV2 data or CVC2 data)) used to verify card-not-present transactions	PixAlert Critical Data Auditor can discover files and email that may contain CVV numbers as well as credit card numbers It can do this across desktops, file servers and email.
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block	PixAlert Critical Data Auditor can detect files and emails that may contain PIN numbers as well as credit card numbers It can do this across desktops, file servers and email.
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).	PixAlert Critical Data Auditor can detect files and emails that contain Credit Card numbers that may have been saved from a software system which should instead contain only masked numbers. It can do this across desktops, file servers and email. PixAlert Critical Data Auditor itself masks any

	CC numbers in its own internal reports.
<p>3.4 Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:</p> <ul style="list-style-type: none"> ▪ Strong one-way hash functions (hashed indexes) ▪ Truncation ▪ Index tokens and pads (pads must be securely stored) ▪ Strong cryptography with associated key management processes and procedures. <p>The MINIMUM account information that needs to be rendered unreadable is the PAN</p>	<p>PixAlert Critical Data Auditor can detect files and emails that contain Credit Card numbers that should be encrypted and are not and are therefore vulnerable to anyone with appropriate levels of network access.</p> <p>It can do this across desktops, file servers and email.</p>
<p>3.5 Protect encryption keys against both disclosure and misuse</p>	<p>PixAlert Critical Data Auditor can detect PVK and PFX files associated with the storage of private keys.</p>
<p>3.5.1 Restrict access to keys to the fewest number of custodians necessary.</p>	<p>PixAlert Critical Data Auditor can detect presence of PFX and PVK files in unexpected locations.</p>
<p>3.5.2 Store keys securely in the fewest possible locations and forms.</p>	<p>PixAlert Critical Data Auditor can determine if PVK and PFX files are duplicated in many places and wither keys are password protected.</p>

Requirement 6 – Develop and maintain secure systems and applications

<p>6.3.4 Production data (real credit card numbers) are not used for testing or development.</p>	<p>PixAlert Critical Data Auditor can determine if Information resources associated with IT (as opposed to payment processing) contain Credit Card numbers.</p> <p>It will know about test card numbers (industry standard)</p>
<p>6.5 Develop web software and applications based on secure coding guidelines such as the <i>Open Web Application Security Project Guidelines</i>. Review custom application code to identify coding vulnerabilities.</p> <p>Cover prevention of common coding vulnerabilities in software development</p>	<p>PixAlert Critical Data Auditor can determine if sensitive information is left unsecured in temporary internet files.</p>

processes, to include the following:

[6.5.1 to 6.5.10]

Requirement 7 – Restrict access to data on a business need to know

7.2 Establish a mechanism for systems with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.

PixAlert Critical Data Auditor can help determine if Credit Card information exists on resources other than those sanctioned by need-to-know.

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 (e.g., new system component installations, changes in network topology, firewall rule modifications, product upgrades). Note that external vulnerability scans must be performed by a scan vendor qualified by the payment card industry..

PixAlert Critical Data Auditor perform scans of all network resources of the company or business units concerned with PCI compliance.

Appendix D - PixAlert Auditor Scanning Process

PixAlert follows a well defined process aimed at ensuring that it can help organizations map out their CHD and ensure that no CHD is located in the parts of the network that are not in scope for PCI DSS. This process is made of five key steps.

Step 1 – Prepare Scanning Rules

PixAlert Auditor provides “put of the box” rules for scanning for CHD, and some other commonly held data like Passport numbers, Health Insurance numbers. It also provides a rules engine that enables you to scan for random data. Defining the data that you are searching for is a most important step in order to ensure accurate results...

Step 2 – Select Target Components

PixAlert Auditor allows you to define “target components” on the network, which in this case are the CHD network components. On the one side it enables you to check what type of CHD and where it is kept on what is believed to be the in-scope network by the entity which needs to comply with PCI DSS. On the other side, it checks that no CHD is located on any of the other parts of the network which is believed to be outside of PCI DSS scope. This allows entities to ensure that they have appropriately documented where CHD is and the full extent of the scope of PCI DSS.

When auditing IT Assets with PixAlert Auditor, it is recommended to adhere to the following guidelines:

- Scan all available IT assets wherever possible in order ensure no prejudice; if this is part of an larger audit programme ensure that the programme covers all IT resources and can be targeted in a random manner
- Use the same scan configuration settings on all IT assets being audited to ensure no prejudice.
- If only a subset of a user’s file system data is being audited, ensure the same settings are applied to all users.

Step 3 – Scan Target Components

Once target components are defined, connectivity with target components is then checked. Following that, each target component is then scanned in non intrusive mode by PixAlert Auditor. Scan results, which are stored in encrypted in the PixAlert Auditor database, show a number of items which are extremely important for PCI DSS compliance.

Each scan is created and saved, with corresponding scan results, under a separate name to allow users the option to review and report on each scan separately or together.

Please note that a graphical representation of PixAlert Auditor’s scanning process is available in Appendix E in this White Paper.

Step 4 – Review Phase

At that stage the user in charge of the audit get an opportunity to analyse the results and preview the report. During this preview stage, users have an option to exclude some scans results that from the final report to tailor the report for specific purposes.

Specific training is available from PixAlert on how to classify scan results and how to interpret each result or groups of results, include or exclude them before the final report is produced.

Step 5 – Report Production

- Overall report showing the total number of target components scanned per type along with the number of scanned files for CHD per target components and the number of target components where CHD was found
- PixAlert Auditor also classifies information found based on its incident severity rating engine. It provides three categories:
 - Highly Confidential Breach
 - For instance if a PAN and the credit cardholder name are found together on the same file or targeted components
 - Policy Breach
 - For instance if unencrypted PANs are found on the same file or targeted components

- Poor Work Practice
 - For instance if an unencrypted file containing names and expiry dates is found on targeted components
- PixAlert also allows entities to see the source of data found as part of the scan. For instance data may be found in emails or in files. This allows entities to locate data in an easier way.
- The report also provides information showing data owners for each type of information. This allows entities to see which users' machines are linked to which type of non compliant CHD storage practice.
- PixAlert Auditor can also provide history of access for each file it has scanned. Thus it allows entities to see when CHD files on selected target components have been accessed last.

Appendix E - Graphical Representation of PixAlert Auditor's scanning process

