Adeft
Associazione
NO PROFIT

# PCI - DSS Forensics
# Soggetti, strumenti e metodi dell'investigazione digitale

**Avv. Giuseppe Serafini**

# About me.

- **Avvocato del Foro di Perugia;**
- **Perfezionamento UNIMI digital forensics '10 - '14;**
- **BSI ISO/IEC 27001:2013 Lead Auditor;**
- **Federprivacy Master Privacy Officer;**
- **E.C.C.E. - European Certificate on Cybercrime Evidence;**
- **UNIPG.IT /Giuris / Informatica;**
- **Comm. Informatica SOS Ordine Avvocati Perugia;**
- **D.F.A. - Digital Forensics Alumni;**
- **C.S.A. - Cloud Security Alliance;**
- **C.S.I.G. - Centro Studi Informatica Giuridica - Perugia.**

# Payment Card Industry - Data Security Standard

## Generalitá.

Insieme di prescrizioni di “sicurezza” - *che trovano applicazione in riferimento a strumenti tecnologici, logici e fisici (POS, PA-DSS) e risorse umane (QSA, ASV, PFI)* - da **attuare e documentare**, attraverso il ricorso all'opera di terzi autorizzati, in base a regole proprie dello standard medesimo, in caso di attivitá di elaborazione (**stores, processes, or transmits**) di dati relativi a pagamenti effettuati con carte di credito/debito.

# Payment Card Industry - Data Security Standard

## Origine.

Nasce nel 2004 dall'esigenza, condivisa dei principali operatori del circuito di pagamento a mezzo carte di credito e di debito (Visa, MasterCard, American Express, Discover, JCB), di **“quantificare e misurare”** il livello di sicurezza da applicare alle negoziazioni avvenute con tali strumenti, al fine di prevenire frodi e/o di accertare responsabilitá, ed in caso, di comminare “sanzioni contrattuali”, per l'inosservanza delle sue prescrizioni - V.3.1 - 15 Aprile 2015.

# Payment Card Industry - Data Security Standard

**Vincolativitá.**

Salvo eccezioni, al momento tre stati U.S.A., lo *standard* non é imposto agli operatori (ad es.: ***esercenti***) per effetto della immediata applicazione di disposizioni di legge, ma, in forza dell'**adesione contrattuale, (... piú o meno libera e consapevole ...) del soggetto "obbligato"**, alle regole dello *standard* medesimo.

# Payment Card Industry - Data Security Standard

**Cartasí**

**E-commerce.**

**Area download**

- Regolamento Esercenti convenzionati con CartaSi
- Regolamento Esercenti abilitati alle vendite e-commerce
- Verified by VISA e MasterCard SecureCode - istruzioni e regole
- Elenco merci e servizi per cui è vietata la vendita a distanza
- Regolamento in materia di trattamento dei dati personali dei Titolari
- Vademecum vendite on-line

**Art. 8 Trattamento dei dati del Titolare**

L'Esercente si impegna a trattare i dati dei Titolari delle Carte nel rispetto degli obblighi previsti dalla vigente normativa in materia di trattamento e protezione dei dati personali e delle disposizioni dei Circuiti Internazionali (consultabili nel Portale Esercenti del sito www.cartasi.it e richiedibili al Servizio Clienti di CartaSi), che l'Esercente dichiara di conoscere e accettare. L'Esercente si impegna altresì a trattare tali dati in maniera lecita, sicura, riservata e limitatamente alle finalità connesse al presente Contratto. L'Esercente si impegna inoltre a certificare la propria organizzazione secondo gli standard PCI DSS (Payment Card Industry Data Security Standards), utilizzando, se necessario, una società riconosciuta dai Circuiti Internazionali per la valutazione delle problematiche di sicurezza e a mantenere tale certificazione valida nel tempo, secondo le modalità di volta in volta richieste, e a fornire a CartaSi la documentazione comprovante la soddisfazione degli standard di sicurezza previsti dalla certificazione. I requisiti per ottenere tale certificazione sono pubblicati sul sito www.cartasi.it.

L'accesso ai dati deve essere consentito solo al personale addetto e autorizzato "mediante appropriati meccanismi di autenticazione" al fine di garantire che i dati stessi non vengano distrutti o persi anche in modo accidentale, ovvero utilizzati in maniera illegittima o non conforme alle finalità di raccolta e per evitare l'accesso a tali dati da parte di terzi non autorizzati. I dati dei Titolari delle Carte non possono essere trasmessi, salvo per eventuali esigenze di carattere giudiziario, a terze parti diverse da CartaSi e dalla Banca e/o da soggetti dalle stesse designati. La trasmissione dei dati ai soggetti autorizzati deve essere comunque effettuata in modo sicuro. In caso di uso illecito dei dati, anche da parte di terzi, derivante dal mancato rispetto delle norme in materia di trattamento e conservazione dei dati previste dal presente Contratto, l'Esercente è soggetto al pagamento di una penale, prevista dai Circuiti Internazionali. In conformità a quanto previsto dai Circuiti Internazionali, qualora i danni generati dall'illecito utilizzo dei dati siano superiori al valore della sanzione sopra indicata, CartaSi si riserva il diritto di rivalersi nei confronti dell'Esercente, addebitando multe e sanzioni.

# Information Security & PCI DSS

## Art. 31

## Obblighi di sicurezza

In dati personali sono custoditi e controllati anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla **natura dei dati** ed alle specifiche caratteristiche del trattamento etc..

| | | |
|---|---|---|
| **A.18 Compliance** | | |
| **A.18.1 Compliance with legal and contractual requirements** | | |
| Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements. | | |
| A.18.1.1 | Identification of applicable legislation and contractual requirements | *Control*<br>All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization. |
| A.18.1.2 | Intellectual property rights | *Control*<br>Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products. |
| A.18.1.3 | Protection of records | *Control*<br>Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements. |
| A.18.1.4 | Privacy and protection of personally identifiable information | *Control*<br>Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable. |
| A.18.1.5 | Regulation of cryptographic controls | *Control*<br>Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations. |

# Payment Card Industry - Data Security Standard

## Overview.

| | |
|---|---|
| **Sviluppo e gestione di una rete sicura** | 1. Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta<br>2. Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione |
| **Protezione dei dati di titolari di carta** | 3. Proteggere i dati di titolari di carta memorizzati<br>4. Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche |
| **Utilizzo di un programma per la gestione delle vulnerabilità** | 5. Utilizzare e aggiornare regolarmente il software o i programmi antivirus<br>6. Sviluppare e gestire sistemi e applicazioni protette |
| **Implementazione di rigide misure di controllo dell'accesso** | 7. Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario<br>8. Assegnare un ID univoco a chiunque abbia accesso a un computer<br>9. Limitare l'accesso fisico ai dati dei titolari di carta |
| **Monitoraggio e test delle reti regolari** | 10. Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta<br>11. Eseguire regolarmente test di sistemi e processi di protezione |
| **Gestione di una politica di sicurezza delle informazioni** | 12. Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale |

# Payment Card Industry - Data Security Standard

| REQUISITI PCI DSS | PROCEDURE DI TEST | ISTRUZIONI |
|---|---|---|
| **10.2.2** Tutte le azioni intraprese da un utente con privilegi di utente root o amministratore | **10.2.2** Verificare che siano registrate tutte le azioni intraprese da un utente con privilegi di utente root o amministratore. | Account con maggiori privilegi, come di "amministratore" o "root", hanno il potenziale di influire in modo significativo sulla sicurezza o sulla funzionalità operativa di un sistema. Senza un registro delle attività eseguite, un'organizzazione non è in grado di ricondurre ogni questione risultante da un errore amministrativo o dall'uso improprio di privilegi all'individuo o all'azione specifici. |
| **10.2.3** Accesso a tutti gli audit trail | **10.2.3** Verificare che l'accesso a tutti gli audit trail sia registrato. | Gli utenti non autorizzati spesso cercano di modificare i log di audit per nascondere le loro azioni e con la registrazione degli accessi un'organizzazione può ricondurre eventuali incongruenze o potenziali manomissioni dei registri ad un singolo account. Il potere accedere ai registri che identificano modifiche, aggiunte ed eliminazioni consente di ricostruire i passaggi intrapresi dal personale non autorizzato. |
| **10.2.4** Tentativi di accesso logico non validi | **10.2.4** Verificare che siano registrati i tentativi di accesso logico non riusciti. | Gli utenti non autorizzati sulla rete spesso eseguono più tentativi di accesso sui sistemi di destinazione. Vari tentativi di accesso non riusciti possono rappresentare un'indicazione dei tentativi di accesso di un utente non autorizzato facendo ricorso a "forza bruta" o cercando di indovinare una password. |
| **10.2.5** Uso e modifiche dei meccanismi di identificazione e autenticazione (compresi, a titolo esemplificativo, creazione di nuovi account, incremento dei privilegi, ecc.) e tutte le modifiche, le aggiunte e le eliminazioni agli account dell'applicazione con privilegi root o di amministratore. | **10.2.5.a** Verificare che l'uso dei meccanismi di identificazione e autenticazione sia registrato. | Se non è possibile sapere chi erano gli utenti presenti al momento in cui si è verificato un incidente, non è possibile identificare gli account che potrebbero essere stati utilizzati. Inoltre, gli utenti non autorizzati possono tentare di manipolare i controlli di autenticazione per cercare di superarli o di spacciarsi per un account valido. |
| | **10.2.5.b** Verificare che l'aumento dei privilegi sia stato registrato. | |
| | **10.2.5.c** Verificare che siano registrate tutte le modifiche, le aggiunte o le eliminazioni a qualsiasi account con privilegi di utente root o amministratore. | |

# Payment Card Industry - Data Security Standard

## Processo di valutazione PCI DSS

1. *Confermare l'ambito della valutazione PCI DSS.*
2. *Eseguire la valutazione PCI per l'ambiente, seguendo le procedure di test per ogni requisito.*
3. *Se necessario, eseguire la correzione per eventuali elementi non a norma.*
4. *Compilare il rapporto applicabile per la valutazione (ad esempio, il Questionario di autovalutazione*, SAQ, o il Rapporto sulla conformità, ROC) compresa la documentazione di tutti i controlli compensativi, in base alle istruzioni PCI applicabili.
5. *Completare per intero l'Attestato di conformità per i provider di servizi o per gli esercenti, come applicabile. Gli attestati di conformità sono disponibili sul sito Web PCI SSC.*
6. *Inviare il questionario di autovalutazione o il rapporto sulla conformità e l'Attestato di conformità, insieme ad eventuale altra documentazione richiesta (ad esempio, i rapporti delle scansioni dei fornitori di prodotti di scansione approvati) al proprio acquirente (per gli esercenti) o al marchio di pagamento o ad altra entità richiedente (per i provider di servizi).*

# Payment Card Industry - Data Security Standard

**0 IN TEN YEARS**

Of all the companies investigated by our forensics team over the last 10 years following a breach, not one was found to have been fully PCI DSS compliant at the time of the breach.

| Level / Tier | Merchant Criteria | Validation Requirements |
|---|---|---|
| 1 | Merchants processing over 6 million Visa transactions annually (all channels) or Global merchants identified as Level 1 by any Visa region | • Annual Report on Compliance ("ROC") by Qualified Security Assessor ("QSA")<br>• Quarterly network scan by Approved Scan Vendor ("ASV")<br>• Attestation of Compliance Form |
| 2 | Merchants processing 1 million to 6 million Visa transactions annually (all channels) | • Annual Self-Assessment Questionnaire ("SAQ")<br>• Quarterly network scan by ASV<br>• Attestation of Compliance Form |
| 3 | Merchants processing 20,000 to 1 million Visa e-commerce transactions annually | • Annual SAQ<br>• Quarterly network scan by ASV<br>• Attestation of Compliance Form |
| 4 | Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually | • Annual SAQ recommended<br>• Quarterly network scan by ASV if applicable<br>• Compliance validation requirements set by acquirer |

*** Verizon 2015 - PCI COMPLIANCE REPORT Pag. 12 - www.verizon.com - {sito consultato e verificato in data 13.04.2015}**

# Payment Card Industry - Data Security Standard

**Payment Card Industry (PCI)**
**Standard di protezione dei dati**

## Questionario di autovalutazione C
## e Attestato di conformità

---

**Esercenti con sistemi di pagamento connessi a Internet, nessuna memorizzazione elettronica dei dati di titolari di carta**

**Versione 3.0**

Febbraio 2014

# Payment Card Industry - Data Security Standard



## Security Rules and Procedures

Merchant Edition

5 February 2015

**What To Do If Compromised**

**Visa Europe Data Compromise Procedures**

**January 2015**

**Version 7.0 (Europe)**

# MASTERCARD Security Roles & Procedures

- Within seventy-two (72) hours, engage the services of a PCI SSC Forensic Investigator (PFI) to conduct an independent forensic investigation to assess the cause, scope, magnitude, duration, and effects of the ADC Event or Potential ADC Event. The PFI engaged to conduct the investigation must not have provided the last PCI compliance report concerning the system or environment to be examined. Prior to the commencement of such PFI's investigation, the Customer must notify MasterCard of the proposed scope and nature of the investigation and obtain preliminary approval of such proposal by MasterCard or, if such preliminary approval is not obtained, of a modified proposal acceptable to

# VISA Europe What to do if compromised

13. If a forensic investigation is required, the acquirer must ensure that a PCI SSC listed Forensic Investigator (PFI) is engaged to perform the forensic investigation: https://www.pcisecuritystandards.org/approved_companies_providers/pfi_companies.php

14. **Visa Europe reserves the right to insist upon a forensic investigation if deemed necessary, irrespective of the number of accounts at risk.**

15. If a PFI forensic investigation is required, members must identify the **PFI within seven (7) business days** of initial notification of a suspected compromise.

16. Ensure that the PFI is engaged (or the contract is signed) **within ten (10) business days** initial notification of a suspected compromise.

17. The PFI must be onsite to conduct a forensic investigation **within five (5) business days** from the date the contract agreement is signed.

18. The Visa Europe member must ensure that there is **no conflict of interest** for the PFI and must ensure that the PFI did not certify any of the Payment Applications being used by the compromised entity or having undertaken the PCI DSS audit for the compromised entity. Visa Europe has the right to engage a PFI to perform a forensic investigation as it deems appropriate and will assess all investigative costs to the member in addition to any fine that may be applicable.

# PCI - PFI

| PCI Forensic Investigator (PFI) | | |
|---|---|---|
| PCI Forensic Investigator (PFI) Program Guide | Aug 2014 | English<br>Download |
| Supplemental Requirements for the PCI Forensic Investigators (PFI) v 2.0 | Dec 2012 | English<br>Download |
| PFI Preliminary Incident Response Report Template | Aug 2014 | English<br>Download |
| PFI Final Incident Report Template v1.1 | Mar 2015 | English<br>Download |
| PFI PIN Security Requirements Report Template | Aug 2014 | English<br>Download |
| PFI Remote Final Incident Report Template v1.1 | Mar 2015 | English<br>Download |

## 2.4 PCI Forensic Investigators

PCI Forensic Investigators ("PFIs") are companies, organizations or other legal entities that are in compliance with all PFI company requirements (defined in the *PFI Supplement*) and have been approved as PFIs by PCI SSC (or another Approving Organization, as described in the *PFI Supplement*) for purposes of performing PFI Investigations.

Only PFIs approved by an Approving Organization and who are in PFI Good Standing are permitted to perform PFI Investigations, and then only in the specific PFI Regions for which they have been approved by PCI SSC. All approved PFIs are listed on the Website with applicable PFI Region(s).

***Note:*** *Not all QSAs are PFIs. In order to be approved as a PFI, an entity must already be qualified as a QSA, and then must satisfy additional requirements applicable to PFIs as set forth in the PFI Supplement.*

# Appendix A: Forensic Investigation Guidelines

In accordance with applicable Industry Rules, a Compromised Entity that stores, processes, or transmits payment card data and is the subject of a Security Issue must ensure that only a PCI Forensic Investigator approved under the PCI SSC PFI Program is engaged to perform a forensic investigation thereof. All PFIs are required to adhere to the following forensic investigation guidelines in all PFI Investigations. Compromised Entities can also use these guidelines to monitor the work of the PFI.

PFI Investigations must be conducted using the following scope and methodology:

1. The PFI will determine the scope of the forensic investigation and relevant sources of electronic evidence. This includes, but is not limited to:
    - Assessment of all external and internal connectivity points within each location involved.
    - Assessment of network access controls between compromised system(s) and adjacent and surrounding networks.
2. The PFI will acquire electronic evidence from the Compromised Entity's host and network-based systems.
    - If the forensic investigation is conducted onsite at the Compromised Entity's premises, both hard drive and volatile memory acquisition must be performed by either recognized law enforcement agencies or the PFI.
    - If the forensic investigation is being done remotely, the PFI must assess the Compromised Entity's environment to determine whether connectivity allows for acquiring evidence over the Internet. If evidence is to be collected remotely the PFI must use a secure connection (secure tunnel only back to the PFI's IP address). If remote evidence acquisition is not possible the PFI must instruct the Compromised Entity to ship evidence to the PFI. The PFI must ensure the Compromised Entity follows defined preservation guidelines so as not to corrupt the evidence.
3. All potential electronic evidence must be preserved on a platform suitable for review and analysis by a court of law, if applicable.
4. Forensically examine electronic evidence to find cardholder data and establish an understanding of how the compromise or other Security Issue may have occurred.
5. Verify that cardholder data is no longer at risk and/or has been removed from the environment.
6. Verify that the Compromised Entity has contained the incident.
7. The PFI must use the PCI SSC-approved PFI Report templates for each PFI Investigation and provide all required reports to all applicable parties as required in accordance with the *PFI Program Guide*. Additionally, the PFI must make all draft PFI Reports and PFI Investigation work papers available to affected Participating Payment Brands upon request.

### 1.4 *Executive Summary of Findings*

| | |
|---|---|
| ▪ Summary of environment reviewed<br>*Details must be documented under "Findings" section below.* | |
| ▪ Was there conclusive evidence of a breach? | ☐ Yes<br>☐ No |
| *If yes* (there is conclusive evidence of a breach), complete the following: | |
| ▪ Date(s) of intrusion | |
| ▪ Cause of the intrusion<br>*List applicable attack vectors as per Appendix C.* | |
| ▪ Has the breach been contained? | ☐ Yes<br>☐ No |
| ▪ *If yes*, specify how the breach has been contained. | |
| ▪ Is there evidence the cardholder data environment was breached?<br>*Provide reasons for Yes or No under "Findings" section below* | ☐ Yes<br>☐ No |
| *If no* (there is no conclusive evidence of a breach), complete the following: | |
| ▪ Were **system** logs available for all relevant systems? | ☐ Yes<br>☐ No |
| ▪ Were **network** logs available for all relevant network environments? | ☐ Yes<br>☐ No |
| ▪ Did the available logs provide the detail required by PCI DSS Requirement 10? | ☐ Yes<br>☐ No |
| ▪ Were the log files in any way amended or tampered with prior to your investigation starting? | ☐ Yes<br>☐ No |
| ▪ Were changes made to the environment prior to your investigation starting? | ☐ Yes<br>☐ No |
| ▪ Was data pertaining to the breach deleted prior to your investigation starting? | ☐ Yes<br>☐ No |

Grazie per l'attenzione.