# PCI DSS – value for money

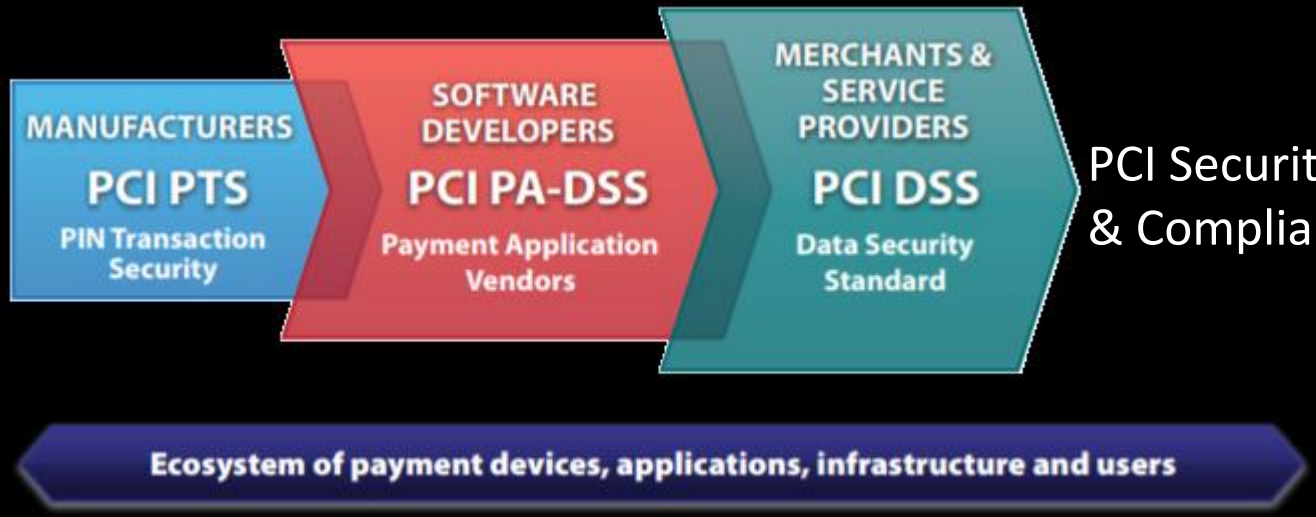
## PRACTICAL IMPLEMENTATION OF PCI DSS FOR THIRD PARTY SERVICE PROVIDERS (TPSP)

by Juliusz Idzik

# What is PCI DSS

The PCI Security Standard Council is responsible for all PCI Standards:

- ✓ PCI DS
- ✓ PA-DSS
- ✓ P2PE
- ✓ PTS



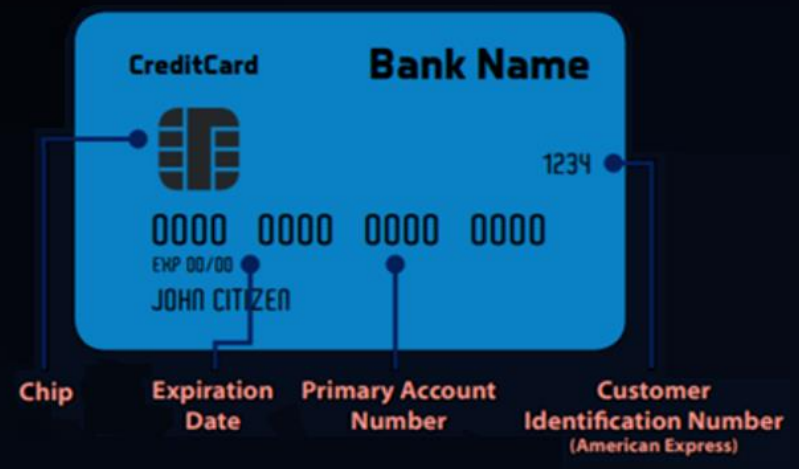

source: https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

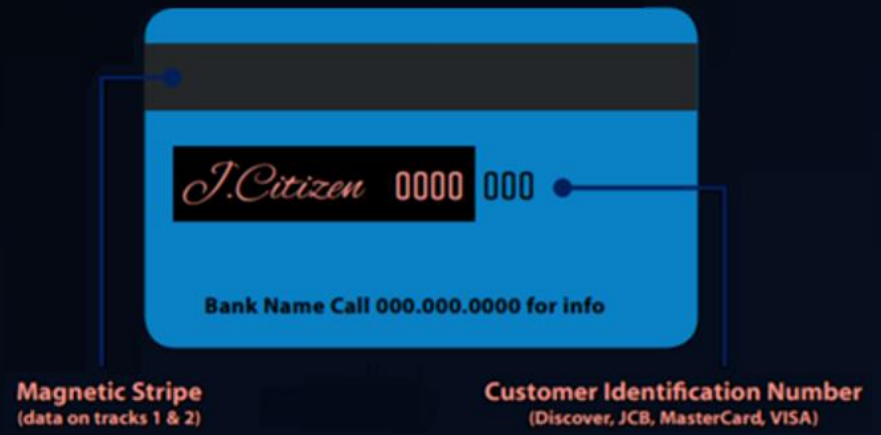
PCI Myths:

- PCI compliance will be easier with PCI compliant Service Provider
- PCI compliance is not possible in non-compliant cloud
- PCI compliance makes organisation secure
- PCI is an expensive IT project

source: https://www.pcisecuritystandards.org/pdfs/pciscc_ten_common_myths.pdf

# Why PCI DSS




https://www.pcisecuritystandards.org/documents/PCI-CyberCrime-FinalR.pdf

The Payment Card Industry (PCI) Data Security Standard (DSS) is a set of requirements designed to ensure that all organizations that store, process, or transmit cardholder data do so in a secure environment.

A credit card as defined by the Council is any card that is backed by a major card brand, including but not limited to:

- ✓ Credit
- ✓ Debit
- ✓ Pre-paid
- ✓ Virtual
- ✓ Loyalty

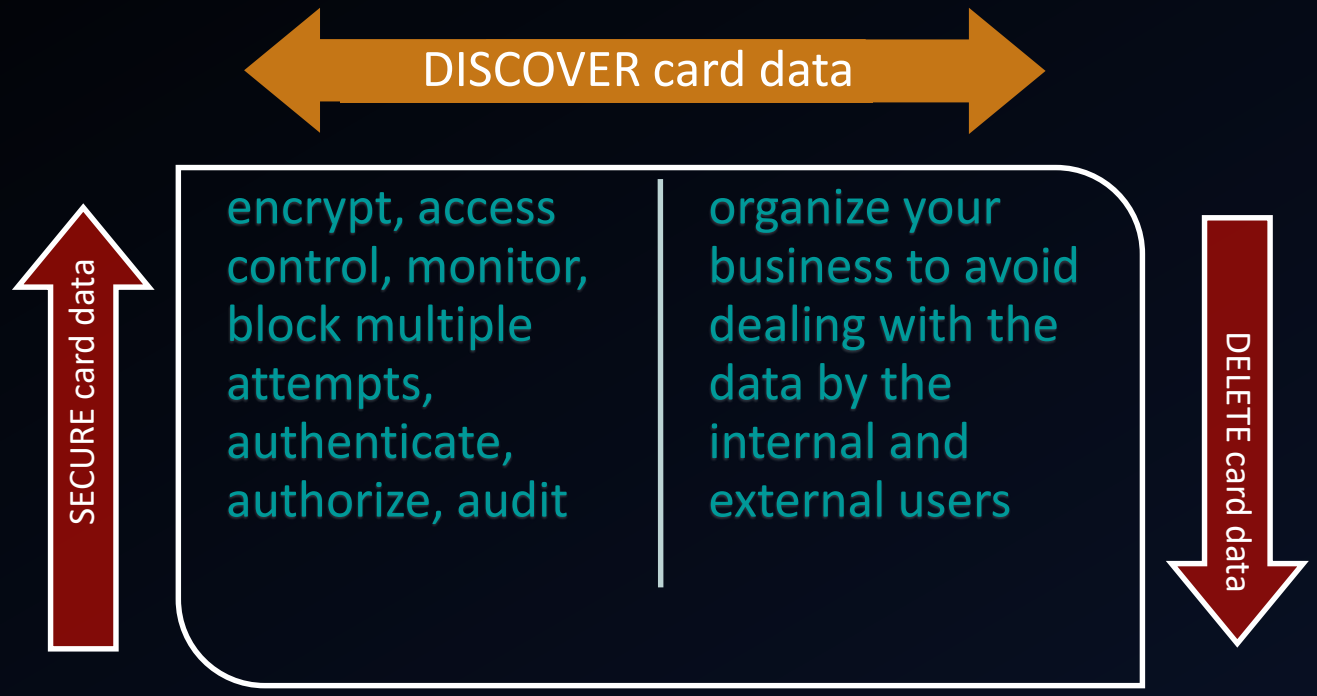
PCI FAQ 1285: one-time PAN
PCI FAQ 1286: virtual PAN

# PCI DSS 12 requirements in 6 domains

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

source: https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf

# PCI DSS implementation



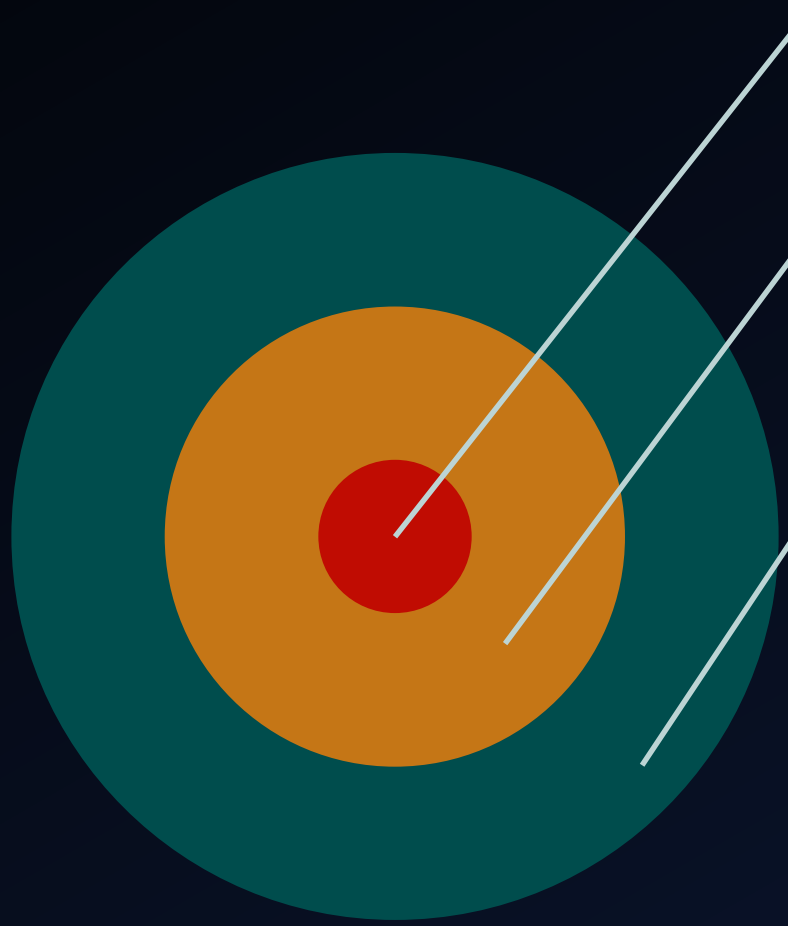

PCI prioritized approach:

- Security policies/procedures
- Network and system security
- Malware protection
- Application and web security
- Logging and monitoring
- Vulnerability scanning
- Security awareness

source: https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide

# Key implementation concept: De-Scoping

Without adequate business process segregation (least privilege, segregation of duties, etc.) the entire organisation is in scope of the PCI DSS assessment



All PCI controls

Only some PCI controls

Out of PCI DSS scope

Without adequate network segmentation (sometimes called a "flat network") the entire network is in scope of the PCI DSS assessment

source: https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf

# TPSP responsibility matrix

Organisation internal requirements:

- Scoping
- Monitoring
- Requirement 3.4: encryption of stored data
- Requirement 12.8: service providers and matrix
- Requirement A: shared hosting providers
- Verification of provider controls
- Incident response and data breaches

Clear acceptance of responsibility for “their” controls:

- Physical
- Network
- Encryption
- Key management
- System security
- Parts of application security

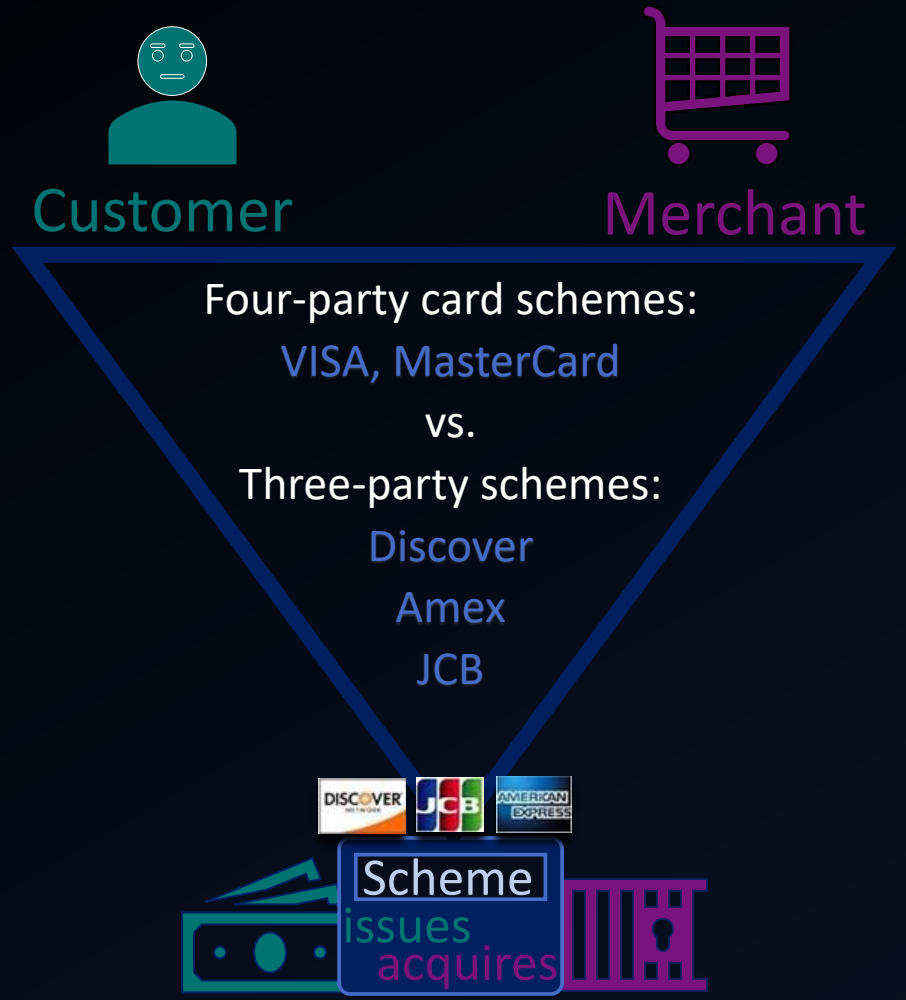
Key Risks:

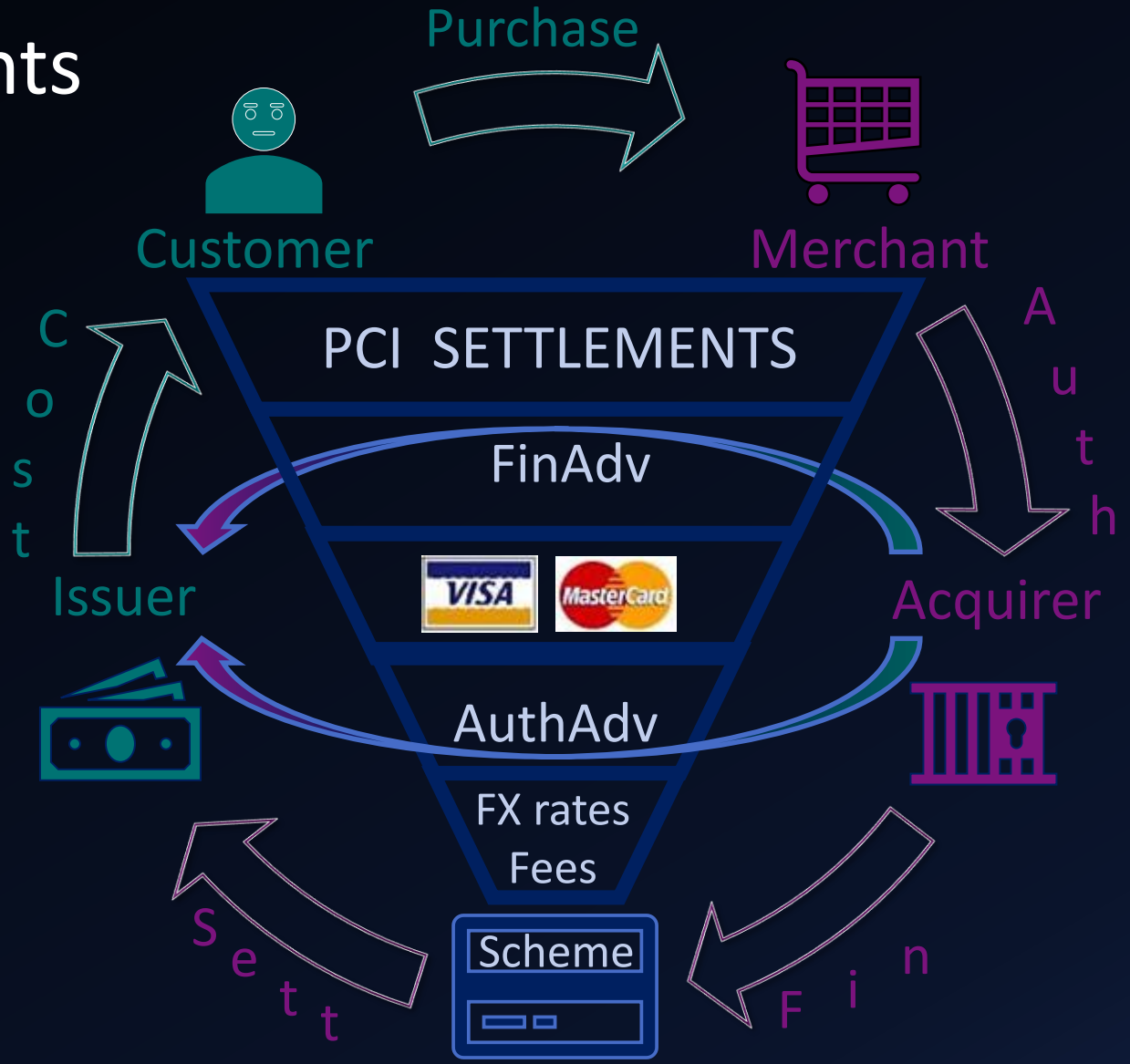
- Failure to test the provider on the ongoing basis
- Trusting the provider without evidence
- SLA failures: no escalation, evidence sharing, incident response cooperation

SLA should be as detailed as possible and approved by both information security and legal

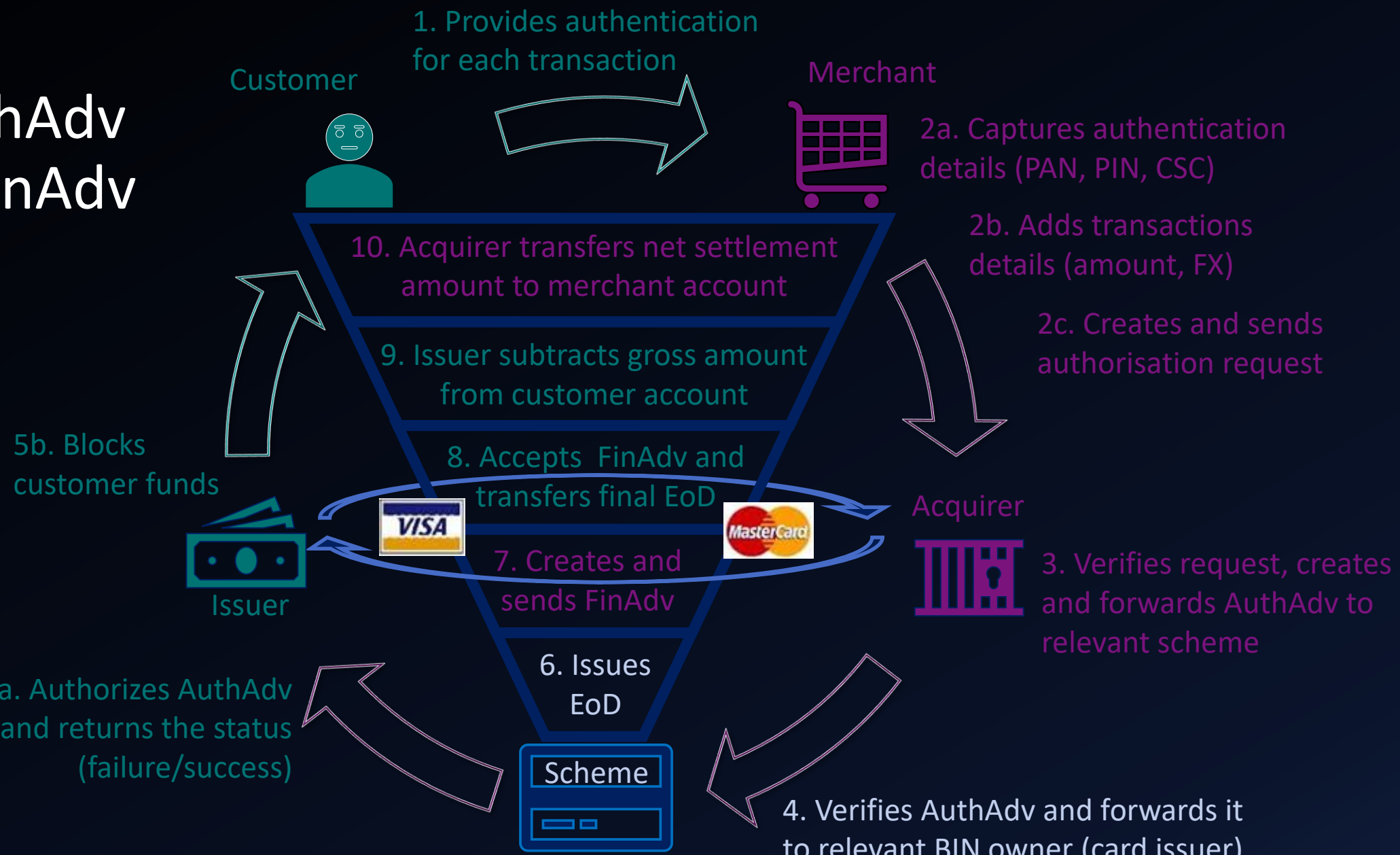
source: https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Third_Party_Security_Assurance.pdf

# PCI financial settlements



# AuthAdv & FinAdv



# Ongoing compliance with PCI DSS

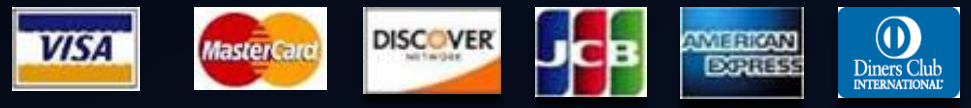
| FREQUENCY | TASK |
|---|---|
| Annually | Scope review, risk assessment, security awareness, key changes, off-site backups review, QSA assessment, Pen Test |
| Bi-annually | Network segmentation testing, review of internal controls |
| Quarterly | ASV and internal scans, wireless scans, non-critical updates and patches |
| Monthly | Critical updates and patches |
| Weekly | File integrity checking, known vulnerabilities updates |
| Daily | Log and alerts review, other operational procedures |

source: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

# Consequences of non-compliance

- Forensic investigations costs
- Fines imposed by the card brands, including damages, compensations, covers
- Limitation and restrictions of card business operations
- Damage to company reputation and bad publicity

The PCI Security Standards Council publishes and maintains PCI DSS, but the actual compliance is enforced by each card brand (Council doesn't fine anybody)




https://www.pcisecuritystandards.org/pci_security/educational_resources

# Thank you

Juliusz Idzik
https://uk.linkedin.com/in/juliusz-idzik-56058385
https://twitter.com/Idzik_L