



PCI-DSS Security Awareness

What you need to know
to protect your customers' data

PCI DSS – What is it?

Payment Card Industry,
Data Security Standard

Developed by the five major card brands, to address potential areas of vulnerability and guide organizations in best practices to maintain the integrity of cardholder data.



The Cost of Noncompliance

- Fines, penalties, and increased fees
- Lost revenues, customers, jobs
- Negative market image
- Cost of reissuing credit cards
- Lawsuits, insurance claims
- Average cost of each stolen card or record = **\$141***
- Global average cost of a data breach = **\$3.62 million***

Data breach Chronology

- 2005 – CARDSYSTEMS – 40-Million Credit Cards stolen
- 2007 – TJ MAXX – 49-Million Credit Cards stolen
- 2009 – HEARTLAND PS – 130-Million Credit Cards stolen
- 2013 – TARGET – 110-Million Credit Cards stolen
- 2014 – HOME DEPOT – 56-Million Credit Cards stolen

- 2020 – TWITTER – 130 Accounts hacked
Including social media accounts of Barack Obama, Kanye West, Elon Musk, Joe Biden and Bill Gates - scammers netted **\$100,000** from people who had no reason to question why a celebrity would tweet: "I'm giving back to the community. All bitcoin sent to the address below will be sent back doubled! If you send \$1000, I will send back \$2000. Only doing this for 30 minutes."

- 2021 - Colonial Pipeline – paid **\$5-Million** ransom to hackers

Attacks on Businesses Like Yours

58% of all malware attacks target small businesses

- Verizon DBIR study

\$84,000 – \$148,000
Is the average cost of an attack on a small business

- UPS Capital study

60% of small businesses close within 6 months of an attack

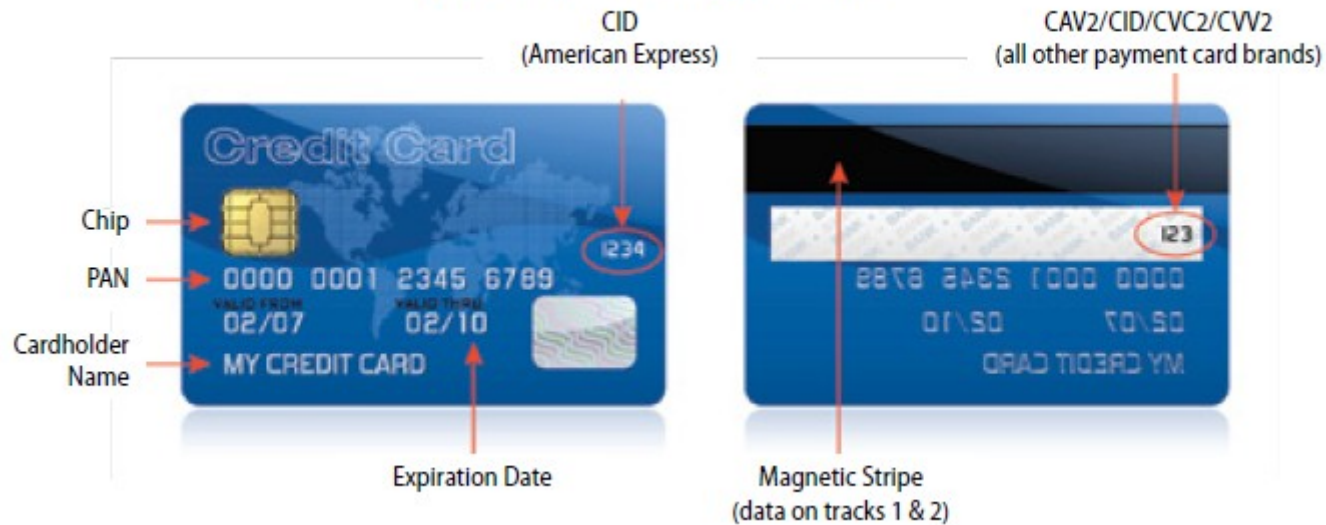
- UPS Capital study

2 in 3 do not have tools in place to prevent a cyber attack

- Ponemon Institute study

Verify Card Elements & Security Features

Types of Data on a Payment Card



When processing a credit card transaction...

Verify the following:

- * The card is signed.
- * The expiration date has not passed.
- * The signature on the receipt matches the card signature.
- * The receipt does not show the full 16-digit account number or card validation code.



Focus on:

Implementing Strong Access Control Measures which Include:

Restricting physical access to cardholder data.



Restrict physical access to cardholder data

- Periodically inspect all credit card devices for tampering or substitution.
- Never allow direct physical access to the credit card device, without supervisor approval.
- Be aware of suspicious behavior.
- Immediately report tampering or evidence of "skimming" or any breach to your supervisor.

Periodically inspect all credit card devices for tampering or substitution

Tampering / Substitution – What to look for



Your credit card terminal will have a sticker on the back that provides the serial number for the device.

Regularly check for altering or tampering. If the numbers do not match, the terminal may have been replaced.

Periodically inspect all credit card devices for tampering or substitution.

Tampering / Substitution – What to look for

Be aware of all access points to the inside of the device.

A skimming device has been added to the inside compartment of this device.



Periodically inspect all credit card devices for tampering or substitution.

Tampering / Substitution – What to look for



In the bottom picture, the cord has been replaced, this could allow capture of credit card data, if left unnoticed.

Never allow direct physical access to the credit card device without owner/manager approval.



Never allow access to credit card terminals without owner/manager approval.

Always verify with your supervisor the identity of any third-party claiming to be repair or service personnel.

Be aware of suspicious behavior.

Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).



Immediately report tampering or evidence of skimming or any breach to your owner/manager.



If you become aware of evidence of tampering, replacement, or any other breach of credit card data, **contact your owner/manager immediately.**

Phishing Emails

- Be wary of suspicious email messages.
- Don't open email attachments unless you are expecting them.
- E-mails may include viruses or misleading links to web pages which ask for personal information.
- Don't click on URLs that people send you unless it is a known "safe" site.
- Report suspicious email to your owner/manager.

Website Safety

- Malicious websites can be infected with spyware or malware and can infect your computer when you visit them.
 - Stay away from unknown sites or sites that anti-virus software warns against.
- Be aware of "pop-ups" that could contain spyware.
- Use known sites that are secure "https" for personal business.
- Spyware and malware could allow an opening to steal confidential information.

It's Not Only Electronic Data

- Protect information in all its forms.
- Keep printed confidential information out of site.
- Use locks on cabinets and offices appropriately.
- Shred documents when they are no longer required.
- When speaking about a confidential matter, be sure that your conversation will not be overheard.

Ways to Protect Cardholder Data

- Never share your password with anyone!
- Keep your desk clear of any sensitive materials.
- Always properly dispose of paper records with cardholder data, using cross-cut shredders or approved shredding bins.
- Don't allow unauthorized individuals around PCI devices
- Be alert! If you're unsure about what could be a security risk, ask your owner/manager.

PCI DSS Requirements

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	<ol style="list-style-type: none">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	<ol style="list-style-type: none">3. Protect stored cardholder data4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none">5. Protect all systems against malware and regularly update anti-virus software or programs6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none">7. Restrict access to cardholder data by business need to know8. Identify and authenticate access to system components9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data.11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none">12. Maintain a policy that addresses information security for all personnel.

Maintain a Vulnerability Management Program



Protect all systems against malware and regularly update anti-virus software or program



Develop and maintain secure systems and applications

Build and Maintain a Secure Network

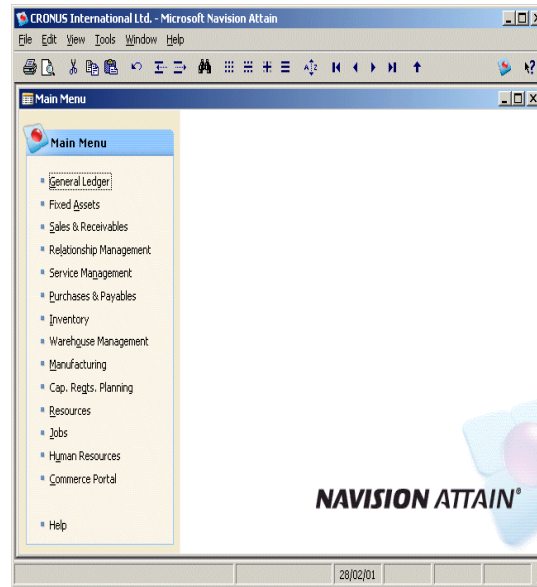


Install and maintain a firewall configuration to protect data



Do not use vendor-supplied defaults for system passwords and other security requirements

Avoid Missing or Outdated Security Patches



Password Protection

- Establish password protocols
- Use strong ones
- Change default passwords
- Enforce confidentiality

It's time to change your password

Are you still using the default password that came with your point of sale (POS) terminal? Or, using 12345 or password1? If so, you need to change it right away to protect your customers' confidential payment card data. Passwords are an easy way for criminals to sneak in to access information if not updated from the default or, if passwords are too simple, it can also make it easy for data thieves to break in.

The idea of changing your passwords may be overwhelming. You want it to be something easy for you and for your employees to remember, while also keeping unwanted predators out. Complex passwords don't have to be complicated.

Look at the chart below:



Password time to crack

burger = instantly



Burger1 = 14 minutes

(uppercase, lowercase, number)



burger1 = 19 seconds



123burger = 7 hours
(8 characters)



Burger123 = 39 days
(9 characters)



hamburger123 = 37 years
(12 characters with numbers)



Burger&fries = 64,000 years
(13 characters with one character)



Burger&fries1 = 26,000,000 years
(13 characters, mix of characters)



Burger123fries = 98,000,000 years
(13 characters)



As you can see, just adding a number or capitalization, or both, can make a huge difference. Take one step closer to protecting payment card data and change your passwords now.

Implement Strong Access Control Measures



Restrict access to cardholder data by business need to know



Assign a unique ID to each person with computer access



Restrict physical access to cardholder data

Regularly Monitor and Test Networks



Track and monitor all access to network resources and cardholder data



Regularly test security systems and processes

Maintain an Information Security Policy



Maintain a policy that addresses information security for all personnel

PCI Compliance Audit: Self Assessment or QSA?

Category	Criteria	Requirement
Level 1 Merchants	More Than Six Million Visa/ MasterCard/American Express/ Discover Transactions per Year Across channels	Annual Onsite PCI Data Security Assessment
	Any Merchant that Has Suffered a Hack or an Attack that Resulted in an Account Data Compromise	Quarterly Network Scan
Level 2 Merchants	One Million to Six Million Transactions Across All Channels per Year	Quarterly Network Scan / Annual Self-Assessment
Level 3 Merchants	20,000 to One Million e-commerce Transactions per Year	Quarterly Network Scan / Annual Self-Assessment
Level 4 Merchants	Less Than 20,000 e-commerce Transactions Annually	Quarterly Network Scan Annual Self-Assessment

SAQ—Self Assessment

Where can I find the PCI SAQ?
https://www.pcisecuritystandards.org/pci_security/completing_self_assessment

Which SAQ do I use?

An Attestation of Compliance is a required part of the SAQ

Understanding the SAQs for PCI DSS version 3

The PCI DSS self-assessment questionnaires (SAQs) are validation tools intended to assist merchants and service providers report the results of their PCI DSS self-assessment. The different SAQ types are shown in the table below to help you identify which SAQ best applies to your organization. Detailed descriptions for each SAQ are provided within the applicable SAQ.

Note: Entities should ensure they meet all the requirements for a particular SAQ before using the SAQ. Merchants are encouraged to contact their merchant bank (acquirer) or the applicable payment brand(s) to identify the appropriate SAQ based on their eligibility.

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS validated third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. <i>Not applicable to face-to-face channels.</i>
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. <i>Applicable only to e-commerce channels.</i>
B	Merchants using only: <ul style="list-style-type: none"> • Imprint machines with no electronic cardholder data storage; and/or • Standalone, dial-out terminals with no electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>
B-IP*	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>
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. <i>Not applicable to e-commerce channels.</i>
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>
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. <i>Not applicable to e-commerce channels.</i>
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.

* New for PCI DSS v3.0

PCI Compliance Checklist

- Identify your merchant category
- Limit your PCI scope using network segmentation and tokenization/hosted payments
- Document your systems and procedures
- Contract with an ASV to perform quarterly scans
- Identify who will perform the audit (you or a QSA)
- Perform the audit
- Remediate
- Submit your attestation of compliance to your processor

PCI DSS – helpful links

- *PCI DSS: <https://www.pcisecuritystandards.org/>
- *American Express: www.americanexpress.com/datasecurity
- *Discover: www.discovernetwork.com/fraudsecurity/disc.html
- *JCB International: <http://partner.jcbcard.com/security/jcbprogram>
- *MasterCard: www.mastercard.com/sdp
- *Visa Inc: www.visa.com/cisp

CardConnect & Secure Trust

- The PCI Wizard and task-tracking To Do List to help you complete the process easily.
- Vulnerability scanning of your Web site (if required) to identify network weaknesses.
- The Security Policy Advisor to help you design your own set of security policies — a requirement of PCI compliance.

- Easy-to-use online Security Awareness Education courses for front-line employees.
- Access to the SecureTrust Endpoint Protection to detect sensitive data storage and provide ongoing compliance monitoring.
- Expedited support by phone or e-mail, as well as online help, tutorials, and education.

















Concierge Service

SecureTrust will contact you to:

- Discuss your PCI status + explain the PCI Concierge service
- Schedule an appointment
- Schedule follow-up appointments (as needed)

Features Include:

- One-on-one walk through with SecureTrust PCI Analyst
- Fully-supported SAQ completion
- Scan setup (if applicable) + Endpoint Security download
- Support for completing PCI Attestation of Compliance (AOC)

	BBB	BBB Complaints (last 3 years)	Google
	★★★★★	1	★★★★★
	★★★☆☆	233	★★★☆☆
	★★★★★	32	★★★★★
	★★★★★	6,520	★★★★★
	★★★★★	3,597	★★★★★
	★★★★★	1,655	★★★★★
	★★★★★	5,653	★★★★★
	★★★★★	297	★★★★★
	★★★★★	253	★★★★★
	★★★★★	4,388	★★★★★
	★★★★★	25,911	★★★★★
	★★★★★	61	★★★★★
	★★★★★	28	★★★★★
	★★★★★	3,613	★★★★★
	★★★★★	5,472	★★★★★
	★★★★★	546	★★★★★

Thank you for attending

Call Dan Arndt 480.289.6304 for more details

Dan Arndt
480.289.6304
Dan@fdisp.com
charge-it-now.com
Power Point Training at;
charge-it-now.com/PCI-Training



- ✓ Free PCI Support
- ✓ 25% lower rates.
- ✓ FREE EMV CHIP CARD MACHINE.*
- ✓ Personal Service and Support.
- ✓ 100% satisfaction guarantee.
- ✓ Cancel at anytime.

See messages from our happy clients below:

"I was skeptical at first, I have heard all the promises of lower rates. Cardconnect has come thru with what they said they would do. They have reduced my CC fee's by over 50%. That puts more money in my pocket. Dan was not pushy and the IT people were easy to deal with. Had a problem with my existing equipment and they replaced it within 24 hours. The ability to process over the internet just adds that extra back up when equipment fails. Highly recommend!"

– David Siress, D&D Automotive

"Absolutely the best service and best credit card processing platform I've seen. Not only do they offer the best rates in the market they give us access to everything we need to get accurate information, accept credit cards remotely and options to run recurring charges for customers who do a lot of business with us. You can talk to a live person who is right here locally any time you need help and they get right on any issues. Highly recommended!"

– Jimmy Alauria, 3-A Automotive Service

*Free machine offer is for shops processing over \$42,000 per month. Shops processing less than that receive below wholesale price of \$295 less \$100 instant rebate or \$195 plus tax. Free equipment remains the property First Data ISP and must be returned in working order if account is discontinued.