

# Fake PCI Compliance Auditors

---

PCI Comply or Die: The Perfect PCI Compliance Scam

By Nicholas Soulliere

June 24, 2025

---

A customer I support reported an email to my organization requesting info/explanation.

Original email pretends to be some type of PCI compliance auditor, and tries to direct them to their website (phishing).

Domain in question that was cited in the email, do not visit/click:

managepci . com

Original email:

---

From: PayPal PCI Support <paypal@managepci . com>

Date: June 11, 2025 at 4:52:17 AM EDT

To: paypalFDM4 [paypalFDM4@my-customer.com](mailto:paypalFDM4@my-customer.com)

Subject: Action Required: Schedule your mandatory scan as soon as possible

PayPal Global

Merchant ID: 5MRW776K4SM8L

Forgot your password?

Your mandatory vulnerability scan(s) are overdue.

Dear My Customer Products Inc,

We reminded you recently to complete your mandatory vulnerability scan to maintain your Payment Card Industry Data Security Standard (PCI DSS) compliance. These scans run an external check on the security of your business internet connection.

As of 06/11/2025, these scans are now overdue. Your card payment acceptance set-up requires you to conduct mandatory scans every 90 days

Failure to run these scans could result in becoming non-compliant with the PCI DSS, which will leave your business vulnerable to cybersecurity risk.

Please call us as soon as you can. Your dedicated customer assistance team is available to help with your mandatory scanning tasks. If we don't hear from you soon, we will continue to reach out by phone and email to help keep your business secure.

#### Running a Network Vulnerability Scan:

To scan your business network, you'll need to provide your business network's public IP address (IP.v4). This unique identifier, made up of numbers and periods, is your business network location on the internet.

#### Finding your IP Address:

There are two main public IP address types:

Dynamic IP: This type automatically changes **from time to time**. Before each scan, you'll need **to** find your current, public IP address. You can easily do this **by** visiting [www.whatismyip.com](http://www.whatismyip.com).

Static IP: This type remains **constant**. If your business has a static public IP, you can save **it for** future scans **and** avoid needing **to** look **it** up each **time**.

Your internet service provider can confirm if your public IP address is dynamic or static.

#### Running a Website Scan

If you take payments via a website, you will need to scan your website payment pages. If you're unsure what to scan, we recommend speaking to your web developer to identify the correct domain(s) to scan.

#### Your next step:

Log in to your online portal at any time to schedule and complete your mandatory scanning activities.

Login

Need Help?

Support Phone 833-770-9555

Support Email [paypalsupport@managepci.com](mailto:paypalsupport@managepci.com)

Company Name

My Customer Products Inc

Merchant ID

5MRW776K4SM8L

Username  
paypalFDM4@my-customer.com

Your portal experience has been updated to reflect the latest requirements of the PCI DSS.  
You can find out more about PCI DSS at [here](#).

This is by far one of the best, if not THE best phishing emails I've ever seen. They've got the system down to a T, everything looks so professional.

Checking via mxtoolbox.com, looks like that while they don't have a DMARC nor their DKIM records published, they do have their SPF records aligned properly. This all adds to their authenticity and looking credible.

SuperTool

MX LookupBlacklistsDMARCDiagnosticsEmail HealthDNS LookupAnalyze Headers

SuperTool Beta9

managepci.comSPF Record Lookup

spf:managepci.comFind ProblemsSolve Email Delivery Problems

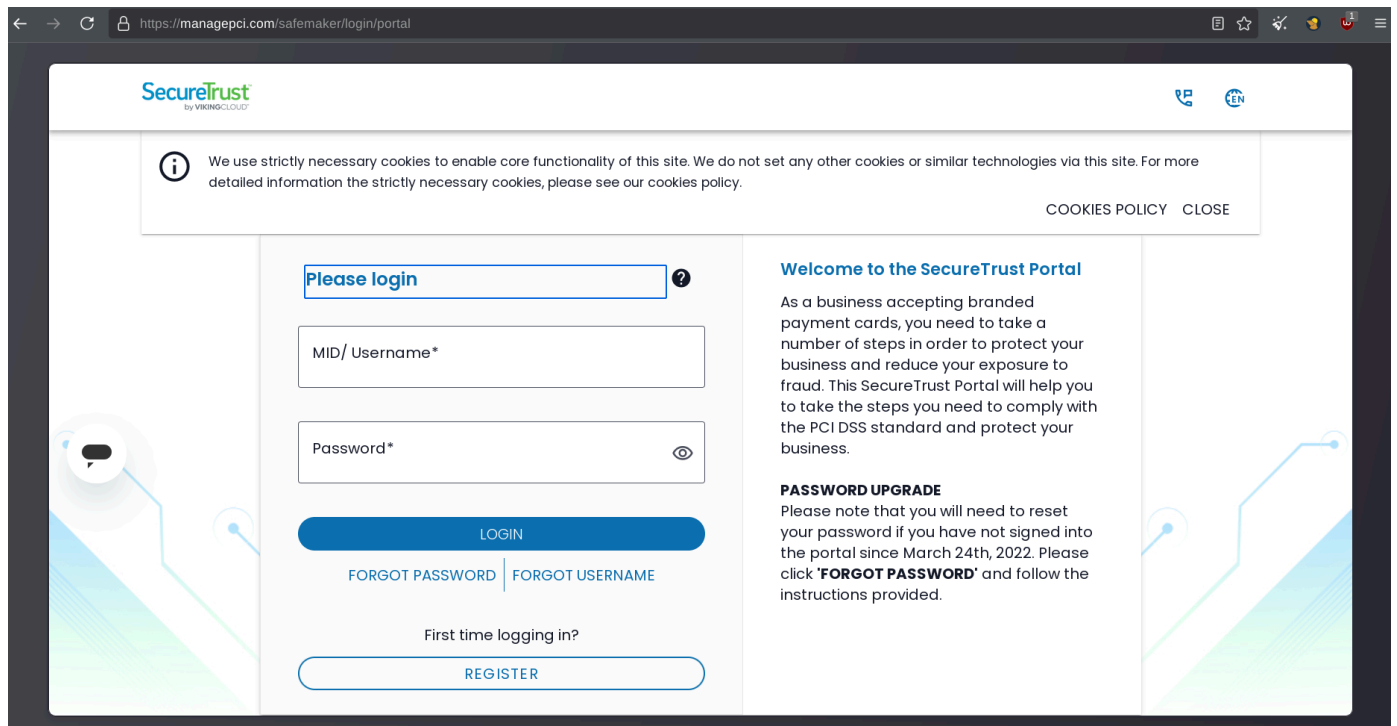
spf

v=spf1 mx include:mail.zendesk.com -all

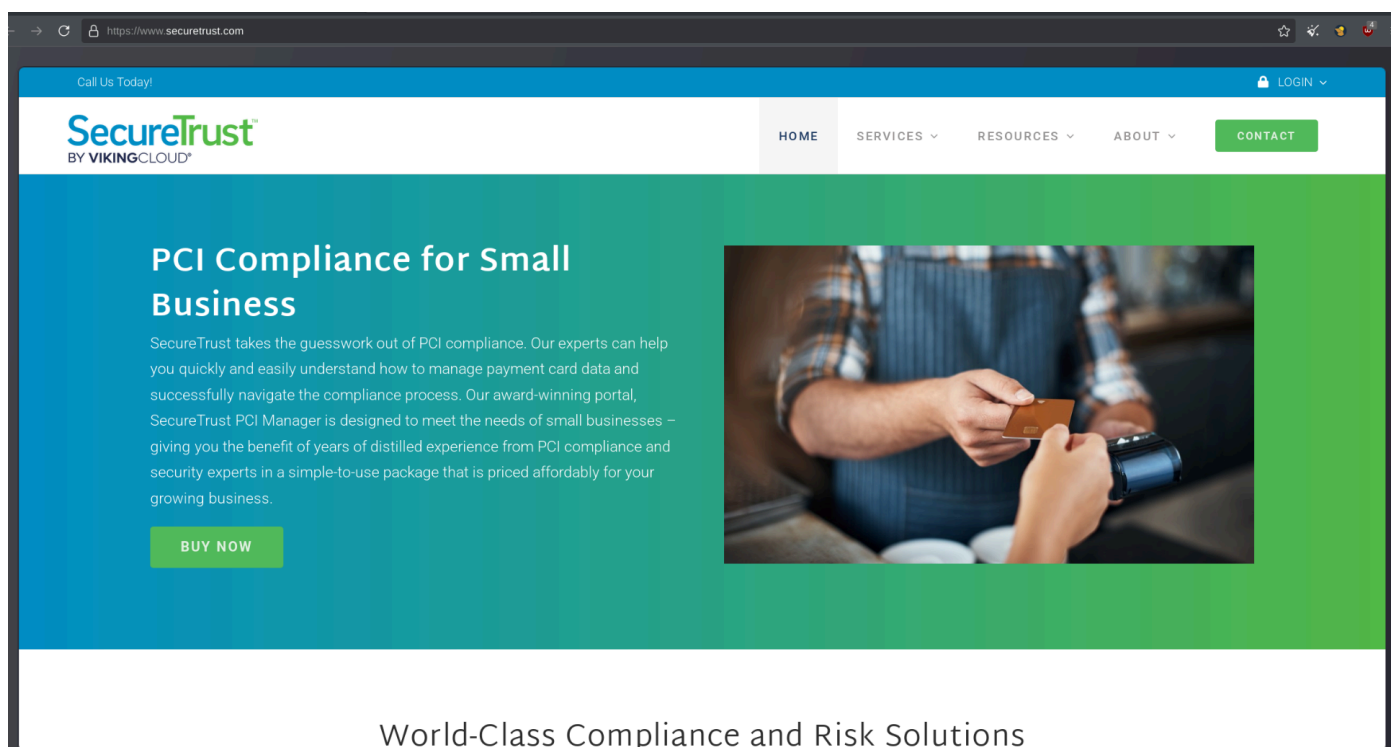
Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	mx		Pass	Match if IP is one of the MX hosts for given domain name.
+	include	mail.zendesk.com	Pass	The specified domain is searched for an 'allow'.
-	all		Fail	Always matches. It goes at the end of your record.

	Test	Result	
✖	DMARC Record Published	No DMARC Record found	<a href="#">More Info</a>
✖	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	<a href="#">More Info</a>
✔	SPF Record Published	SPF Record found	
✔	SPF Record Deprecated	No deprecated records found	
✔	SPF Multiple Records	Less than two records found	
✔	SPF Contains characters after ALL	No items after 'ALL'.	
✔	SPF Syntax Check	The record is valid	
✔	SPF Included Lookups	Number of included lookups is OK	
✔	SPF Recursive Loop	Nor Recursive Loops on Includes	
✔	SPF Duplicate Include	No Duplicate Includes Found	
✔	SPF Type PTR Check	No type PTR found	
✔	SPF Void Lookups	Number of void lookups is OK	
✔	SPF MX Resource Records	Number of MX Resource Records is OK	
✔	SPF Record Null Value	No Null DNS Lookups found	

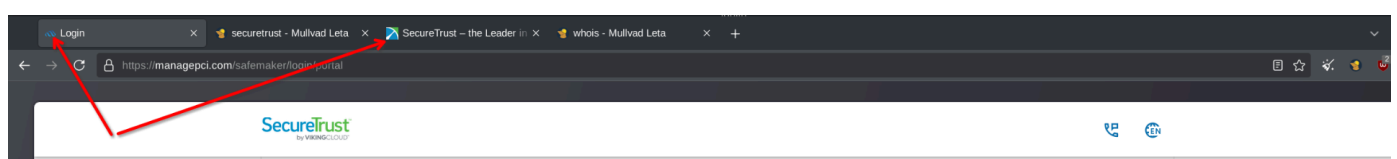
Site is very authentic and professional. SecureTrust by VikingCloud is also a legitimate PCI related entity.



And have a look at the real SecureTrust by VikingCloud:



As always, the devil is in the details. The favicon does not match, its using VikingCloud's default logo, rather than SecureTrust, which is who its pretending to be.



Inspecting the source we can also see its drastically different, fake is left, real is right:

[illegible]

Reviewed the DNS info of both, the scam site is using AWS on the east coast and the real is using Fastly Inc on the west coast.

<https://www.nslookup.io/domains/www.securetrust.com/dns-records/>

<https://www.nslookup.io/domains/managepci.com/dns-records/#cloudflare>

[illegible]

Entirely falls apart with a basic ICANN lookup as well, checkout the owner of the domain's info.

Registered to someone in the UK, with none of the info matching anything mildly legitimate, contact number, email, etc.

Contact Information

Registrant:

Handle: managepci.com-reg  
Name: On behalf of managepci.com owner  
Organization: Identity Protection Service  
Phone: tel:+44.1483307527  
Kind: individual  
Mailing Address: PO Box 786, Hayes, Middlesex, UB3 9TR  
ISO-3166 Code: GB  
Contact Uri: mailto:1c91623c-4f77-4af9-b826-21ccc478cb0a@identity-protect.org

Technical:

Handle: managepci.com-tech  
Name: On behalf of managepci.com owner  
Organization: Identity Protection Service  
Phone: tel:+44.1483307527  
Kind: individual  
Mailing Address: PO Box 786, Hayes, Middlesex, UB3 9TR  
ISO-3166 Code: GB  
Contact Uri: mailto:1c91623c-4f77-4af9-b826-21ccc478cb0a@identity-protect.org

Registrar Information

Name: Amazon Registrar, Inc.  
IANA ID: 468

<https://www.virustotal.com/gui/domain/managepci.com>

6 hits for a phishing domain is crazy, I typically only see 1-2.

managepci.com

6 / 94  
Community Score

6/94 security vendors flagged this domain as malicious

managepci.com

top-1M

Registrar  
Amazon Registrar, Inc.

Creation Date  
3 years ago

Last Analysis Date  
3 hours ago

Reanalyze Similar More

DETECTIONDETAILSRELATIONSCOMMUNITY1

Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Phishing	CRDF	Malicious
CyRadar	Phishing	Gridinsoft	Phishing
MalwareURL	Phishing	VIPRE	Malware
ArcSight Threat Intelligence	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	benkow.cc	Clean
BitDefender	Clean	Blueliv	Clean
Certego	Clean	Chong Lua Dao	Clean
CINS Army	Clean	CMC Threat Intelligence	Clean

Customer was informed of findings, and advised on cybersecurity best practices.