



Welcome to the CIO Hour!

July 2021

The CIO Hour

- A new type of Webinar
- Tackling the problems and questions that are on your mind with real-world technology advice
- Featuring experts in their field with decades of real-world experience
- First Thursday of every month (except this month!)

Visit www.theCIOHour.com for upcoming topics and events.

Ground rules...

- No question is off limits!
- If the question is too specific to a particular situation, we may defer it but are happy to talk to you offline or after the event.
- This is a safe space, but we understand if you wish to remain anonymous.

Agenda

- In the News – A few highlights that might interest you
- Fast 15 min – Introduction to the topic of the month
- Q & A – 30 min – Discussion with our experts and taking your questions

Today's Panel



CHRISTIAN FADEL

Chief Financial Officer, Affinipay
cfadel@affinipay.com | 855.656.4684



Christian Fadel serves as the Chief Financial Officer at Affinipay. Christian brings more than 20 years of experience in the payments industry to his role at Affinipay. He is responsible for overseeing all of the company's financial, accounting and capital planning affairs. Prior to joining Affinipay Christian held the CFO role in several other payment related businesses. Christian is a CPA and holds a Bachelor's Degree in Business from Stephen F. Austin State University and an MBA from Georgetown University.



JAMES C. MARQUIS

Chief Information Officer, 501Works
marquis@501works.com | 703.459.9779

James C. Marquis is a seasoned senior executive with more than 30 years of experience working in technology with a wide variety of associations and nonprofits. James' work experience includes serving as CIO for a large medical association, CEO of a technology consulting organization and senior roles in product development and business consulting for for-profit and nonprofit clients. He also has designed and built multiple Internet-based business applications including Mojo Middleware™.

In the News

1. Beware the Print Spooler – Patch your Microsoft Systems

<https://us-cert.cisa.gov/ncas/current-activity/2021/06/30/printnightmare-critical-windows-print-spooler-vulnerability>

2. Kaseya Vulnerability exploited for Ransomware Attack

<https://www.zdnet.com/article/kaseya-ransomware-attack-your-questions-answered/>

3. Own your very own Festivus pole with Lego Seinfeld

<https://www.cnet.com/news/new-seinfeld-lego-set-features-jerrys-apartment-a-festivus-pole/>

4. DoD rescinds the JEDI contract

<https://www.cnn.com/2021/07/06/tech/defense-department-cancels-jedi-contract-amazon-microsoft/index.html>

Today's Topic:

PCI in July!

PCI in July – 5 Fast Facts

1. Founded September 2006 by major card providers
2. **19%** of breaches in small (<100 employees) organizations
3. In 2019 only **27.9%** of organizations were compliant
4. Requirement 11 (Testing) posted the biggest gap in compliance – organizations do not test enough
5. Experts estimate almost 4 million security positions remain unfilled globally

SOURCE: Verizon 2020 Payment Security Report

<https://enterprise.verizon.com/resources/reports/2020-payment-security-report.pdf>



On to Your Questions...



Who falls under the rules of PCI?

PCI Compliance – the impact is wide!

- “The PCI DSS applies to all entities that store, process, and/or transmit cardholder data.”

https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf?agreement=true&time=1534870826847

- You can lessen your responsibility depending on how you accept cards and manage your systems

What is the Self Assessment Questionnaire?

Self Assessment Questionnaire – the “SAQ”

SAQ	DESCRIPTION	# OF /75	VULN. SCAN
A	E-commerce website (third party) - Fully outsourced card acceptance and processing - Merchant website provides an iframe or URL that redirects a consumer to a third-party payment processor - Merchant can't impact the security of the payment transaction	24	No
A-EP	E-commerce website (direct post) Merchant website accepts payment using direct post or transparent redirect service	191	Yes
B	Processes cards via: - Analog phone, fax, or stand-alone terminal - Cellular phone (voice) or stand-alone terminal - Knuckle buster/imprint machine	41	No
B-IP	Processes cards via: Internet-based stand-alone terminal isolated from other devices on the network	86	Yes
C	Payment application systems connected to the Internet: - Virtual terminal (Not C-VT eligible) - IP terminal (Not B-IP eligible) - Mobile device (smartphone/tablet) with a card processing application or swipe device - View or handle cardholder data via the Internet - POS with tokenization	160	Yes
C-VT	Processes cards: - One at a time via keyboard into a virtual terminal - On an isolated network at one location - No swipe device	83	No
D	E-commerce website - Merchant website accepts payment and does not use a direct post or transparent redirect service Electronic storage of card data - POS system not utilizing tokenization or P2PE - Merchant stores card data electronically (e.g., email, e-fax, recorded calls, etc.)	329	Yes
P2PE	Point-to-point encryption - Validated PCI P2PE hardware payment terminal solution only - Merchant specifies they qualify for the P2PE questionnaire	33	No

- SAQ is how you attest to your compliance with PCI.
- The goal is to move to SAQ-A by using strategies to minimize PCI exposure.
- **SAQ-A = 24 Questions**
- **SAQ-D = 329 Questions**

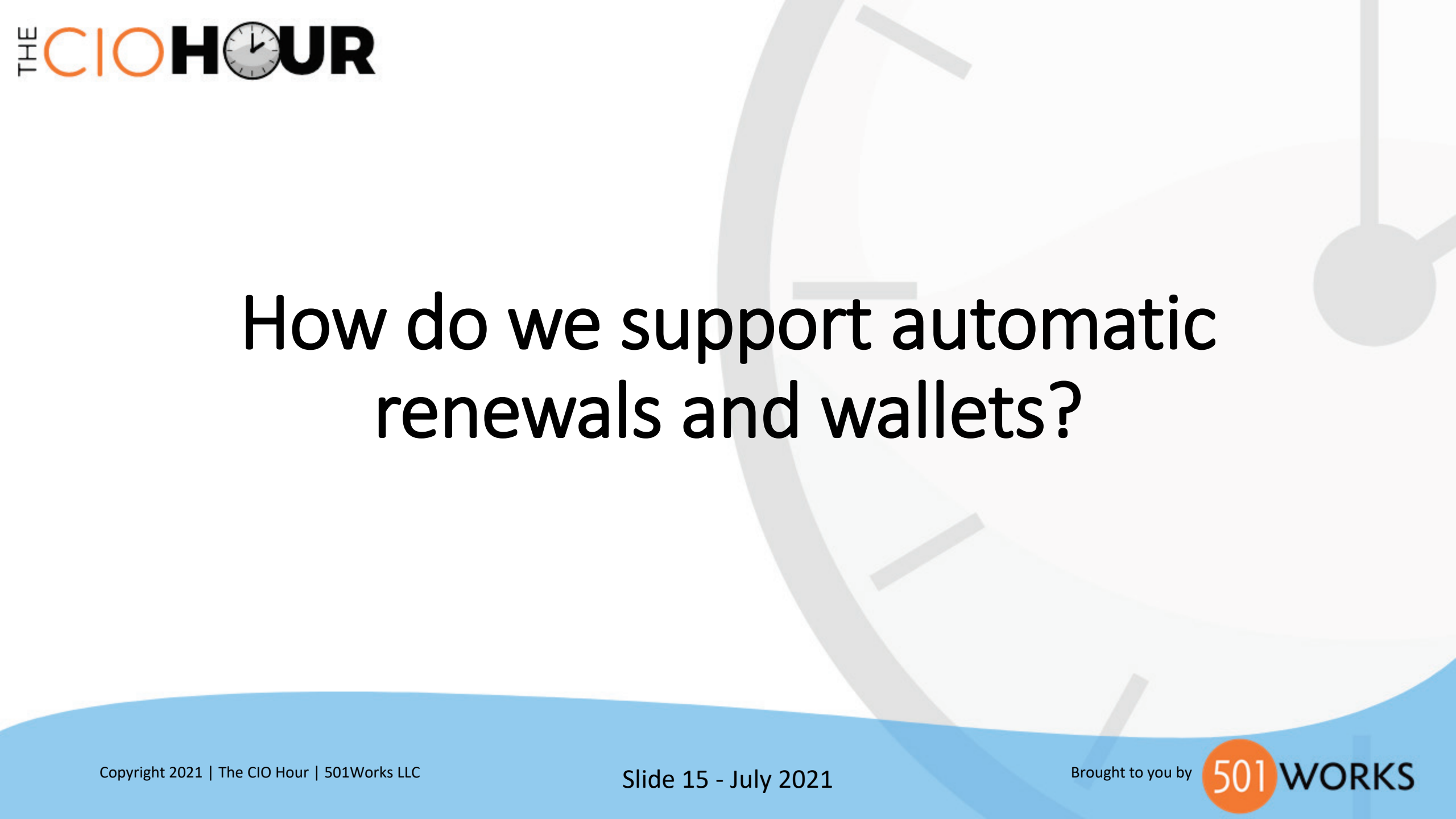
<https://www.securitymetrics.com/learn/pci-saq-overview-chart>



What are hosted fields?

Hosted Fields shift your risk...

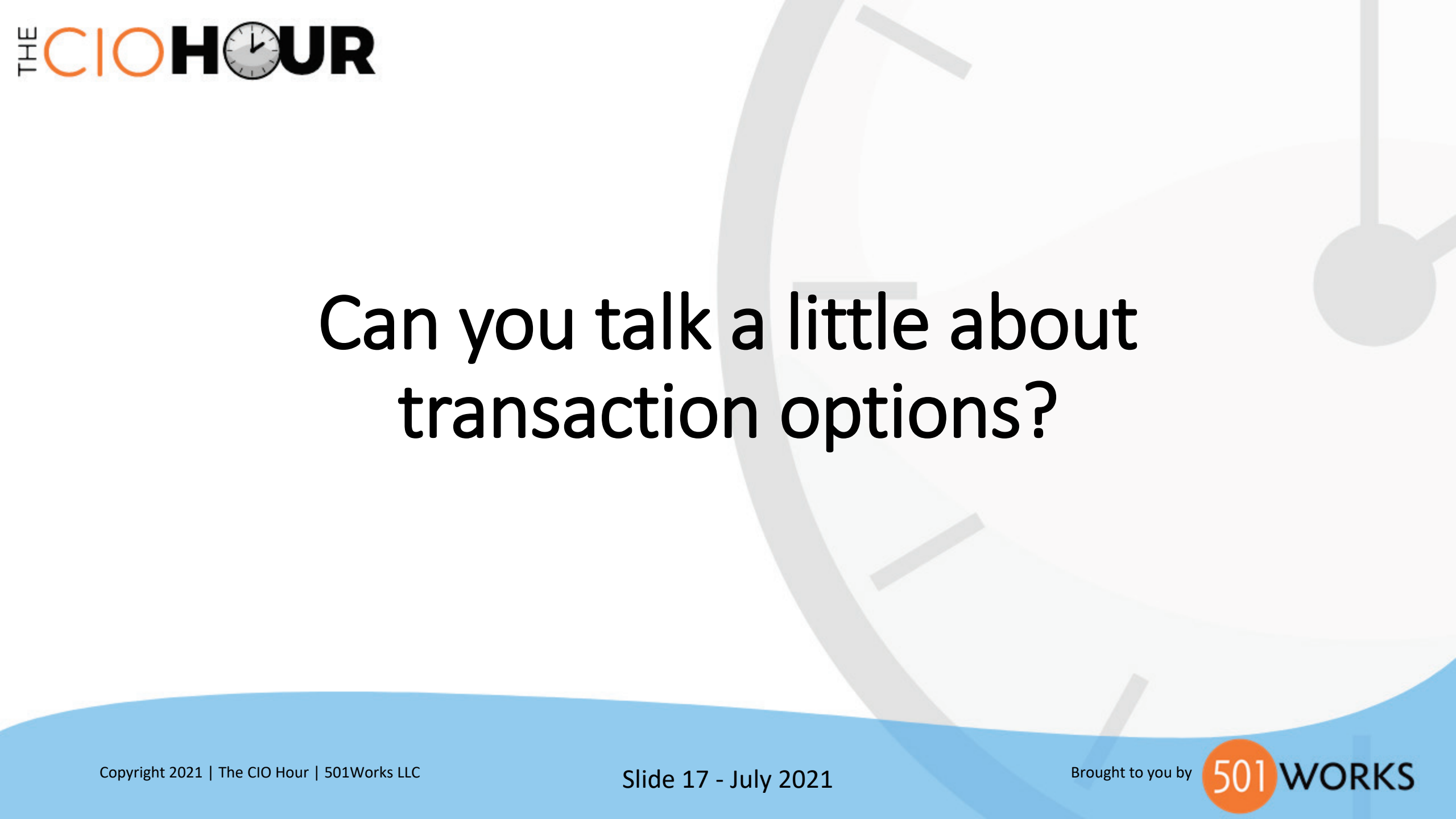
- This is a coding technique on your payment pages so that cardholder information is passed directly back to the payment processor
- Since cardholder data bypasses your system – it moves your system out of scope for PCI purposes
- Limiting scope is the name of the game
- Massachusetts CLE is a real-world example



How do we support automatic renewals and wallets?

Tokenizing cards and automatic updates...

- Not all tokens are created equal – they do not need to expire
- Protects the card holder because tokens are unique to you as a merchant.
- Accounts can be auto-updated to maintain the wallet.



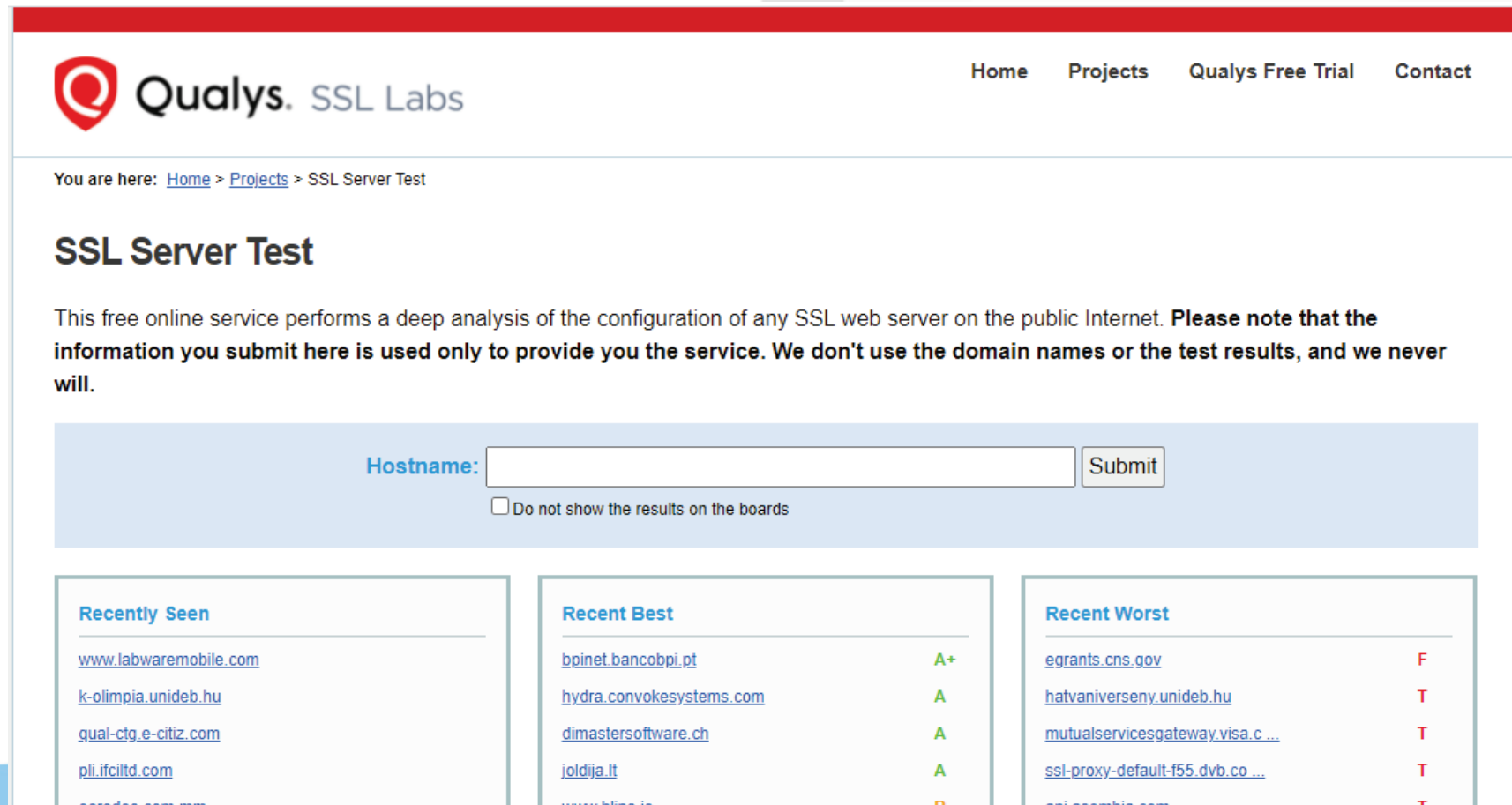
Can you talk a little about transaction options?

Smart versus dumb transactions...

- Legacy gateways do not offer a lot of flexibility with data captured during transactions.
- Modern gateways offer flexibility to include more information in the transaction stream.
 - Examples could include MemberID, OrderID, Member Name, Event Name, etc.
 - Solves issues like a corporate card being used for multiple purchases
 - Greatly improves the reconciliation process for the finance team

A simple test... check your TLS!

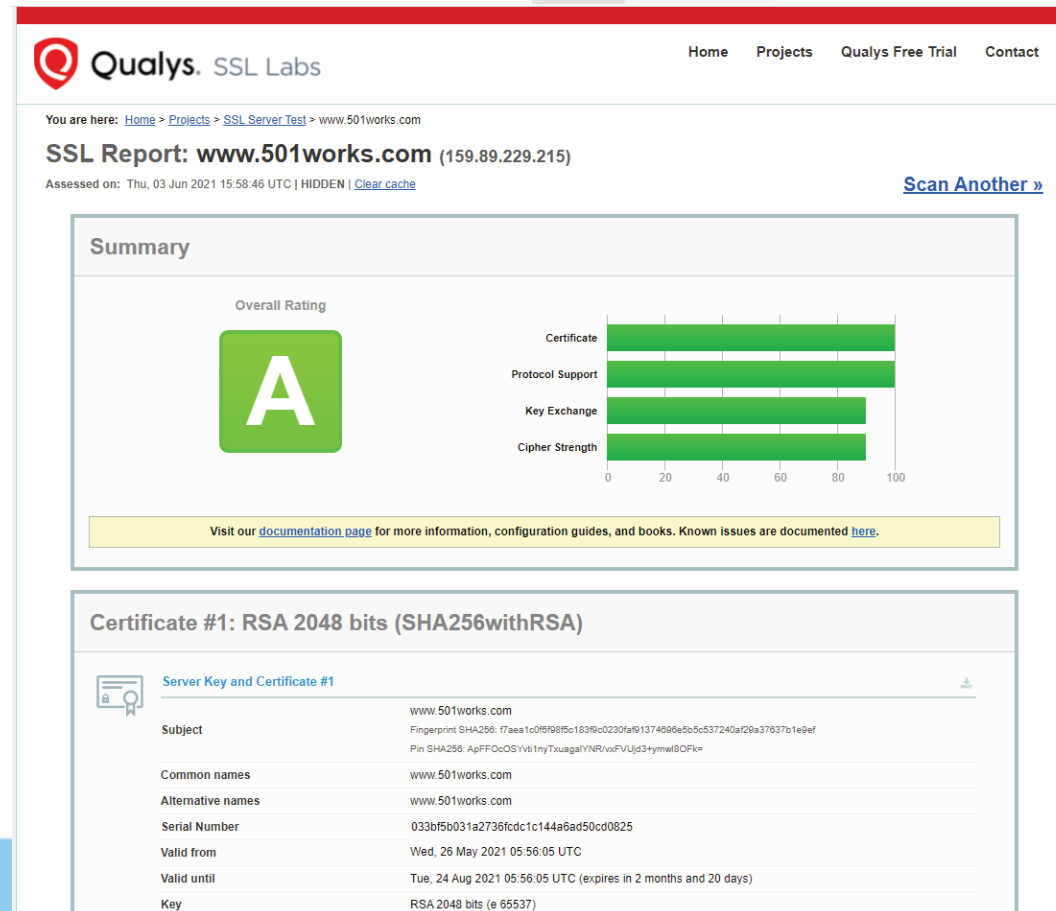
Tools you can use... Qualys SSL Labs - <https://www.ssllabs.com/ssltest/>



The screenshot shows the Qualys SSL Labs website. At the top is a red navigation bar with the Qualys logo and links for Home, Projects, Qualys Free Trial, and Contact. Below the navigation bar, a breadcrumb trail reads "You are here: Home > Projects > SSL Server Test". The main heading is "SSL Server Test". A paragraph explains that this is a free online service for analyzing SSL web server configurations, with a disclaimer that submitted information is used only for the service. Below this is a light blue form area containing a "Hostname:" label, a text input field, a "Submit" button, and a checkbox labeled "Do not show the results on the boards". At the bottom, there are three columns of results: "Recently Seen", "Recent Best", and "Recent Worst".

Recently Seen	Recent Best	Recent Worst
www.labwaremobile.com	bpinet.bancobpi.pt A+	egrants.cns.gov F
k-olimpia.unideb.hu	hydra.convokesystems.com A	hatvaniverseny.unideb.hu T
qual-ctg.e-citiz.com	dimastersoftware.ch A	mutualservicesgateway.visa.c... T
pli.ifciltld.com	joldija.lt A	ssl-proxy-default-f55.dvb.co... T
paradeo.com.mm	www.blinc.jp B	api.scombia.com T

Tools you can use... Qualys SSL Labs - <https://www.ssllabs.com/ssltest/>



Other Questions?



Thank you Affinipay for today's content expertise!



If you have additional questions, please contact Affinipay:

associations@affinipay.com



Emily Schulte



Sherry Reisman



Ask the CIO

Questions not answered? Connect with us...



703-459-9779



theCIOHour@501works.com



www.theciohour.com

Final Thoughts

- We are hitting the beach in August but will be back in September with “Back to School – Understanding SSL”
- An archive of this presentation and today’s Webinar will be posted on theCIOHour.com in a few days.
- Any suggestions for future programs? Topics you would like to see covered? Please email us: theCIOHour@501works.com