

PCI Council Small Merchant Security Resources

4 August 2016

Sylvia Auyeung, Director, Merchant Risk
Lester Chan, Director, Merchant Security



VISA

Disclaimer

The information or recommendations contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

Agenda

- Global Data Compromises
- PCI Council Small Merchant Taskforce and Materials
- Guide to Safe Payments
- Common Payment Systems
- Questions to Ask Your Vendor
- Key Takeaways

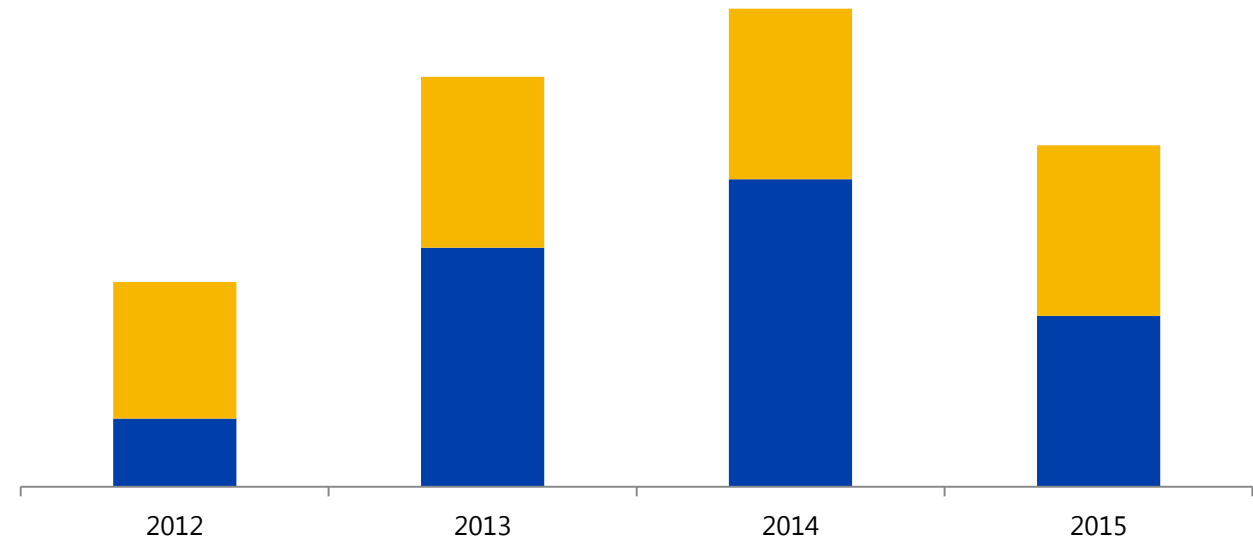
Global Data Compromises

Breach trends by merchant level

Entity Type		2012	2013	2014	2015
		%	%	%	%
	Level 1	<1%	1%	1%	<1%
	Level 2	<1%	1%	1%	<1%
	Level 3	1%	4%	4%	5%
	Level 4	95%	92%	93%	92%
Agent		<1%	1%	1%	2%
Other		2%	<1%	0%	0%
Total		100%	100%	100%	100%

- As a proportion of the total number of breach events, L4s remain the vast majority of compromise cases (93% in 2014-2015)
- At-risk accounts in 2015 were largely attributed to L4 merchants
- Level 4 merchants outnumber L1s in the US

Large breach events (levels 1 & 2)



- Fewer level 1 and 2 breaches in 2015
- Threat actors are targeting smaller interconnected merchants in large numbers
- Restaurants and “other retail” make up the biggest portion of total known breaches
- Quick service restaurants, supermarkets, and lodging make up the other top MCCs

Small Merchant Taskforce as a Merchant Resource

Formed to help improve payment data security for small businesses



Purpose

- Communicate unique small business security challenges
- Simplify understanding of PCI DSS
- Provide educational materials that relates to small businesses

Participants

- Collaboration from dozens of small merchant owners and franchisees
- Co-chaired by Barclaycard and National Restaurant Association

Products

- Materials that are easy to understand
- Tips for improved security implementation
- Small merchant resources

1 – Guide to Safe Payments

Infographic with easy-to-understand guidance on data security basics



Understanding Your Risk



Protecting Your Business with These Security Basics



Where to Get Help

Helping Small Merchants Understand Risk

Diagrams and illustrations to explain security basics

The impact of breaches to small businesses

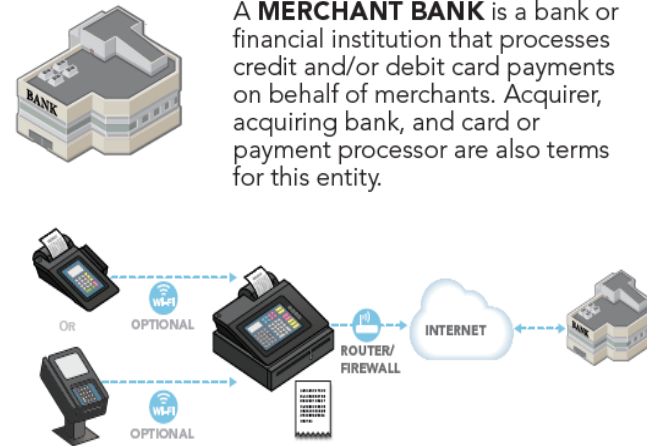
\$20,752
AVERAGE COST TO A SMALL BUSINESS DUE TO HACKING, UP FROM \$8,600 IN 2013 (NSBA)

69% OF AMERICAN CONSUMERS WORRY ABOUT THEFT OF THEIR PAYMENT CARD DATA (Gallup)

What's at risk?
 Understanding data on a payment card

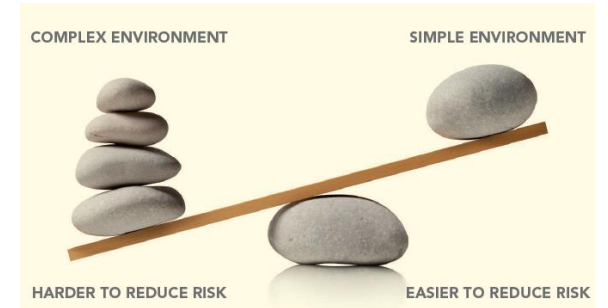


Common payment terms and types of POS terminals



A **PAYMENT SYSTEM** encompasses the entire process for accepting card payments in a retail location (including stores/shops and e-commerce storefronts), and may include a payment terminal, an electronic cash register, other devices or systems connected to a payment terminal (for example, Wi-Fi for connectivity or a PC used for inventory), servers with e-commerce components such as payment pages, and the connections out to the merchant bank.
















































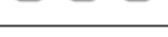
Different risk for different environments and payment systems



Simple payment system for in-shop purchases

Protect Your Small Business

Easy security controls with costs, ease, and risk mitigation scores

How to Safeguard your Business Against Breaches	Cost	Ease	Risk Mitigation
 Use strong passwords and change default ones			
 Protect your card data and only store what you need			
 Inspect payment terminals for tampering			
 Install patches from your vendors			
 Use trusted business partners and know how to contact them			
 Protect in-house access to your card data			
 Don't give hackers easy access to your systems			
 Use anti-virus software			
 Scan for vulnerabilities and fix issues			
 Use secure payment terminals and solutions			
 Protect your business from the Internet			
 For the best protection, make your data useless to criminals			

Where to Get Help?

Resources and links

PCI Council Listings		
Resource	Link	URL
List of Validated Payment Applications	PCI Council's Validated Payment Applications	https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement
List of Approved PTS Devices	PCI Council's Approved PTS Devices	https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices
List of Approved Scanning Vendors	PCI Council's Approved Scanning Vendors	https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors
List of Qualified Integrators / Resellers	PCI Council's Qualified Integrators Resellers	https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers
List of P2PE Validated Solutions	PCI Council's P2PE Validated Solutions	https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

Payment Brand Lists		
Resource	Link	URL
Lists of Compliant Service Providers	MasterCard's List of Compliant Service Providers	https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html
	Visa's Global Registry of Service Providers	http://www.visa.com/splisting/
	Visa Europe's Registered Member Agents	https://www.visaeurope.com/receiving-payments/security/downloads-and-resources

PCI DSS and Related Guidance		
Resource	Link	URL
More about PCI DSS	How to Secure with PCI DSS	https://www.pcisecuritystandards.org/pci_security/how
PCI DSS Self-Assessment Questionnaires	Self-Assessment Questionnaires	https://www.pcisecuritystandards.org/pci_security/completing_self_assessment
Guide: Skimming Prevention: Overview of Best Practices for Merchants	Skimming Prevention: Overview of Best Practices for Merchants	https://www.pcisecuritystandards.org/documents/Skimming_Prevention_At-a-Glance_Sept2014.pdf

2 – Common Payment Systems

Detailed resource on payment system types and how to secure them

- 1** Before protecting payment card theft, understand how to accept payments
- 2** Understand equipment, vendors, partners and how they all fit together
- 3** Using diagrams and visuals to identify the type of payment system used
- 4** Understand the type of associated risks with each type of payment system
- 5** Understand the security steps and controls to protect them

Identify which visual most closely represents the merchant's payment system



Protect card data and merchant business with security basics

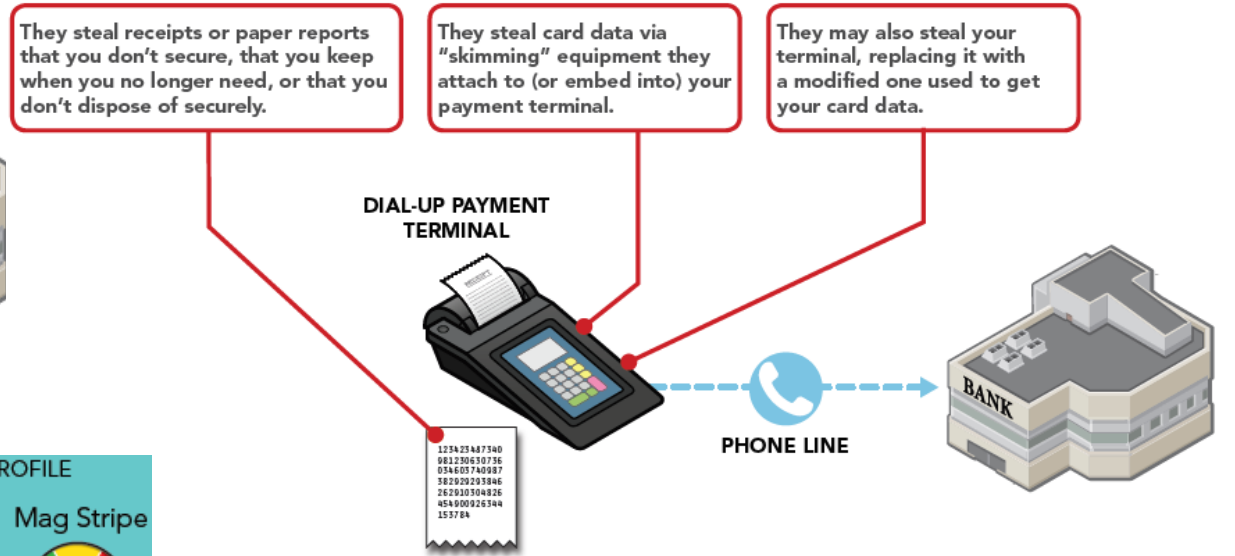
Identify risks and threats

Dial-Up Payment Terminal Diagram (Simple Model)

OVERVIEW



THREATS



RISKS

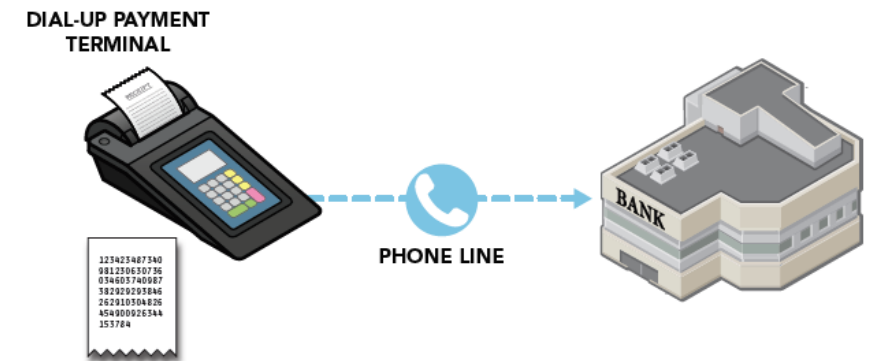
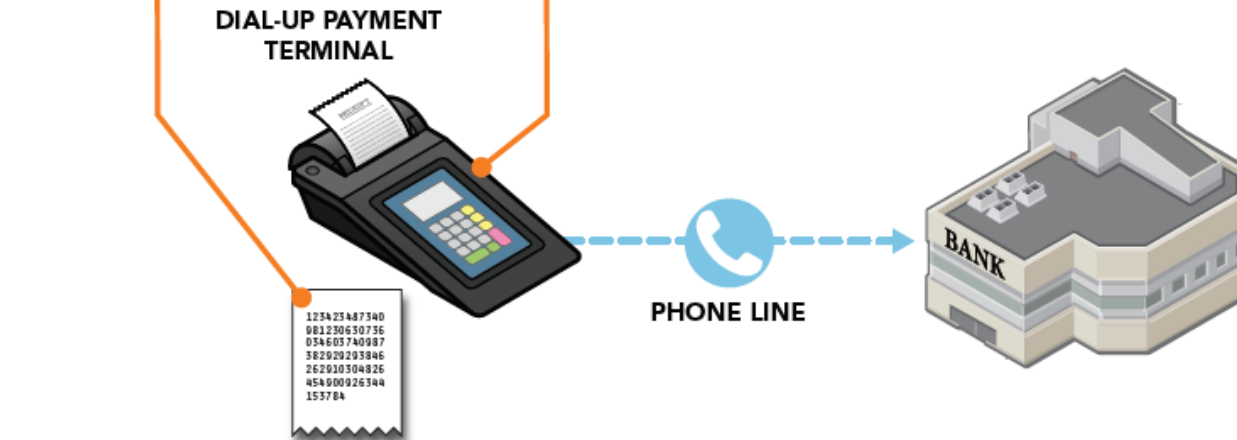


PROTECTIONS

- Protect card data and only keep what you need
- Inspect your payment terminals for damage or changes
- Ask your vendor partners for help if you need it

Hardcopy card data, for example on paper receipts or reports

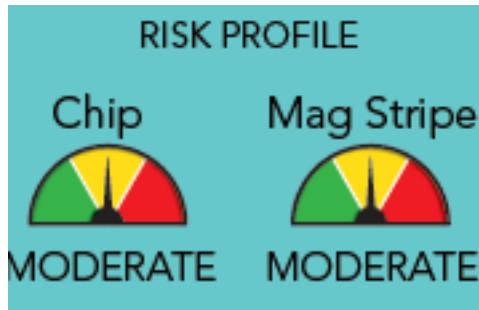
Electronic card data inside payment terminal



Secure Card Reader Diagram (Sophisticated Model)

Descriptions of more complex point of sale environments

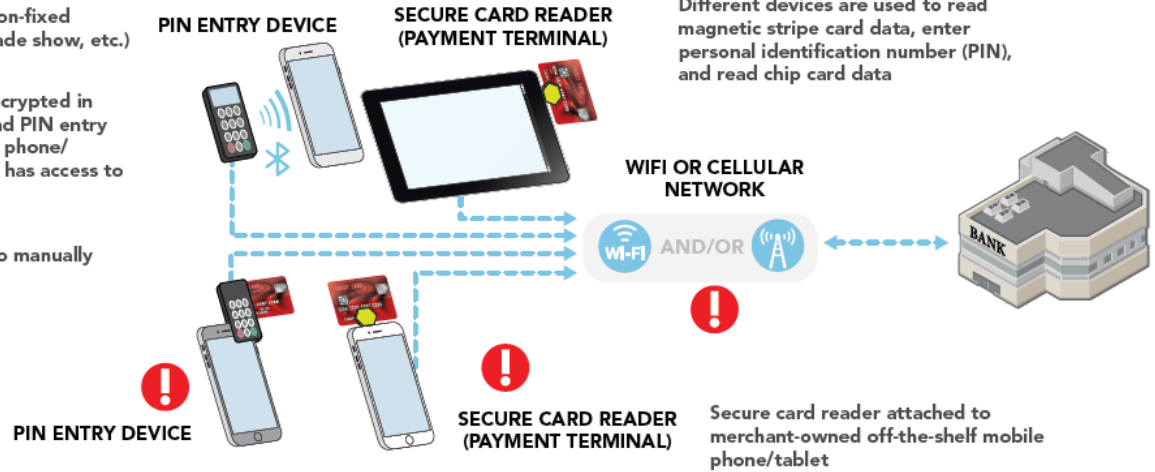
With thorough explanations of risk, threats and controls to protect these more complex environments



For merchants when at non-fixed locations (flea market, trade show, etc.)

Card data and PIN are encrypted in the secure card reader and PIN entry device before sending to phone/tablet; phone/tablet only has access to encrypted card data

Merchant has no ability to manually enter card data



Use strong passwords



Inspect your secure card readers and PIN entry devices for damage or changes



Install patches from your payment terminal vendor



Ask your vendor partners for help if you need it



Protect in-house access to your card data



Limit remote access for your vendor partners - don't give hackers easy access



Use anti-virus software



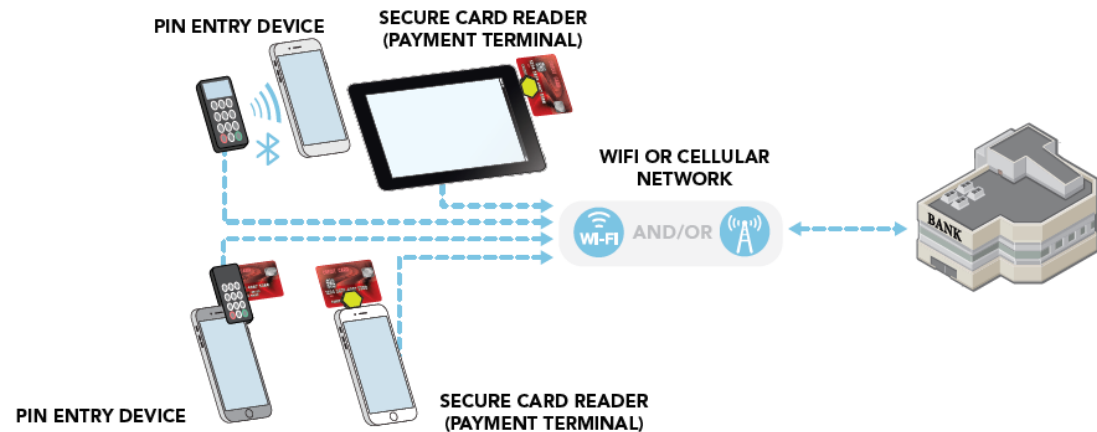
Use a secure card reader and PIN entry device



Protect your business from the Internet



Make your card data useless to criminals



3 – Questions to Ask your Vendors

Helps small merchants know what is needed from vendors and service providers

- Explains the function of vendor or service provider
- Depending on the type, the applicable PCI standard or program
- Includes what to look for and helpful links to card brand programs
- 12 simple questions to ask

TYPE OF VENDOR/ SERVICE PROVIDER	FUNCTION	PCI STANDARD OR PROGRAM	LOOK FOR:
Payment application vendor	Sell and support applications that store, process, and/or transmit cardholder data.	Payment Application Data Security Standard (PA-DSS)	Application is on the List of PCI PA-DSS of Validated Payment Applications .
Payment terminal vendor	Sell and support devices used to accept card payments (e.g., payment terminal).	PIN Transaction Security (PTS)	Payment terminal is on the List of PCI Approved PTS Devices .
Payment processors, e-commerce hosting providers/processors	Store, process, or transmit cardholder data on your behalf. May also host and manage your e-commerce server/website and/or develop and support your website.	PCI Data Security Standard (PCI DSS)	Ask for their PCI DSS Attestation of Compliance and whether their assessment included the service you are using. Service provider is on one of these lists: MasterCard's List of Compliant Service Providers Visa's Global Registry of Service Providers Visa Europe's Registered Member Agents
Providers of software as a service	Develop, host and/or manage your cloud-based web application or payment application (e.g., online ticketing or booking application).	PCI DSS	Ask for their PCI DSS Attestation of Compliance and whether their assessment included the service you are using. Service provider is on one of these lists: MasterCard's List of Compliant Service Providers Visa's Global Registry of Service Providers Visa Europe's Registered Member Agents
Integrators/resellers	Install PA-DSS validated payment applications on your behalf.	Qualified Integrators and Resellers (QIR)	Ask whether vendor is a PCI Qualified Integrator or Reseller (QIR). Vendor is on the List of PCI QIRs .
Providers of services that satisfy PCI DSS requirement(s)	Manage/operate systems or services on your behalf (e.g., firewall management, patching/AV services).	PCI DSS	Ask for their PCI DSS Attestation of Compliance and whether their assessment included the service you are using. Service provider is on one of these lists: MasterCard's List of Compliant Service Providers Visa's Global Registry of Service Providers Visa Europe's Registered Member Agents

Sample Vendor Q&A

Includes desired answer and recommended action based on responses



CATEGORY: How secure is your product?	
QUESTION: Does your product/solution protect payment card information using strong encryption?	
DESIRED ANSWER FROM VENDOR	RECOMMENDATION ACTION
<p>YES</p> <p>Encryption is a way of securing information so it is less likely to be stolen. If you can, select from the List of PCI P2PE Validated Solutions, where card data is secured as soon as you receive it and is protected as it travels through your network.</p>	<p>If NO, consider another vendor or solution.</p>

Key Takeaways

Easy-to-use toolkit to help small merchants with payment system security

- Small merchant breaches continue to occur
- Simplified PCI DSS validation exercises
- Taskforce formed to address the needs of small businesses and franchisees
- Focused on protecting customer's cardholder data rather than IT and security
- Guide focuses on risk and includes diagrams, costs, and ease of implementation matrix
- Payment diagrams designed to show data flows from simple to complex systems
- Q&A resource for working with vendors
- Glossary to help with payment terms and information security definitions
- Links for additional references and where to look for help

Resources

Upcoming Webinars – Training page on www.visa.com/cisp

- Protect the Payments System From Account Testing and Fraudulent Authorizations – August 9, 2016
- Guarding Against Card Not Present Fraud – August 24, 2016

Visa Data Security Website – www.visa.com/cisp

- Alerts, Bulletins
- Best Practices, White Papers
- Webinars
- Visa Global Registry of Service Providers – <http://www.visa.com/splisting/>

PCI Security Standards Council Website – www.pcissc.org

- Small Merchant Resources - https://www.pcisecuritystandards.org/pci_security/small_merchant
- Data Security Standards – PCI DSS, PA-DSS, P2PE, and PTS
- Programs – QSA, ASV, PA-QSA, PFI, ISA, PCIP, and QIR
- Fact Sheets – ATM Security, Mobile Payments Acceptance, Tokenization, Cloud Computing, and many more...

Thank you for attending!

