ControlCase
Compliance as a Service

Protecting Payments Throughout the Ecosystem

Emma Sutcliffe
Senior Director, Data Security Standards
PCI Security Standards Council

PCI Security Standards Council

- *Founded in 2006*
- *Guiding open standards for payment card security*

ControlCase
Compliance as a Service

Role of PCI SSC

Standards, Best Practices & Services

Payment **Equipment**

Payment **Software**

Merchant & Service Provider **Environments**

Validation & Qualification – Equipment, Services, Assessors, Investigators

Training – Merchants, Assessors, Acquirers, Integrators

ControlCase
Compliance as a Service

Understanding the Ecosystem

Emerging Payment Technologies

ControlCase
Compliance as a Service

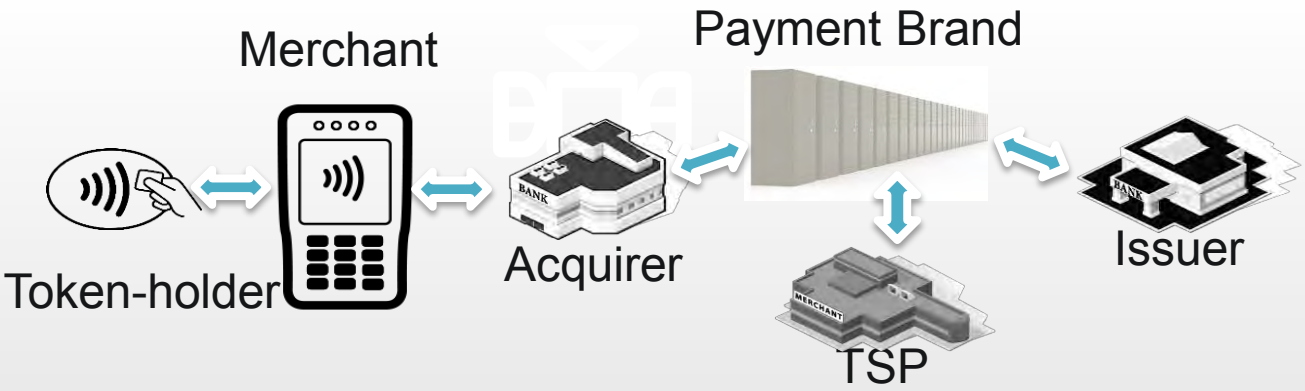
Mobile Technologies

- PCI DSS
  - Requirements applicable to mobile and other technologies as they emerge
- PA-DSS
  - Payment applications running on mobile hardware dedicated to payment acceptance
- Point-to-Point Encryption (P2PE)
  - PCI-listed P2PE solutions using PTS approved mobile PEDs

ControlCase
Compliance as a Service

Token Service Provider (TSP)

- New standard to address Token Service Provider environments
  - Requirements for securing environments where payment tokens are generated / issued
- Token Service Provider defined by EMVCo



Mobile Provisioning Security Requirements

- Addendum to the Card Production standard
- Physical and Logical Security Requirements for vendors that:
  - Perform cloud-based (host card emulation) or secure element (SE) provisioning services;
  - Manage over-the-air (OTA) personalization, lifecycle management, and preparation of personalization data; or
  - Manage associated cryptographic keys

ControlCase
Compliance as a Service

EMV Chip

- **EMV Chip reduces face-to-face counterfeit fraud**
- **EMV Chip Needs PCI**

ControlCase
Compliance as a Service

Common Goal: Devalue Data

- EMV
- Point-to-Point Encryption
- Tokenization

ControlCase
Compliance as a Service

A Holistic Approach

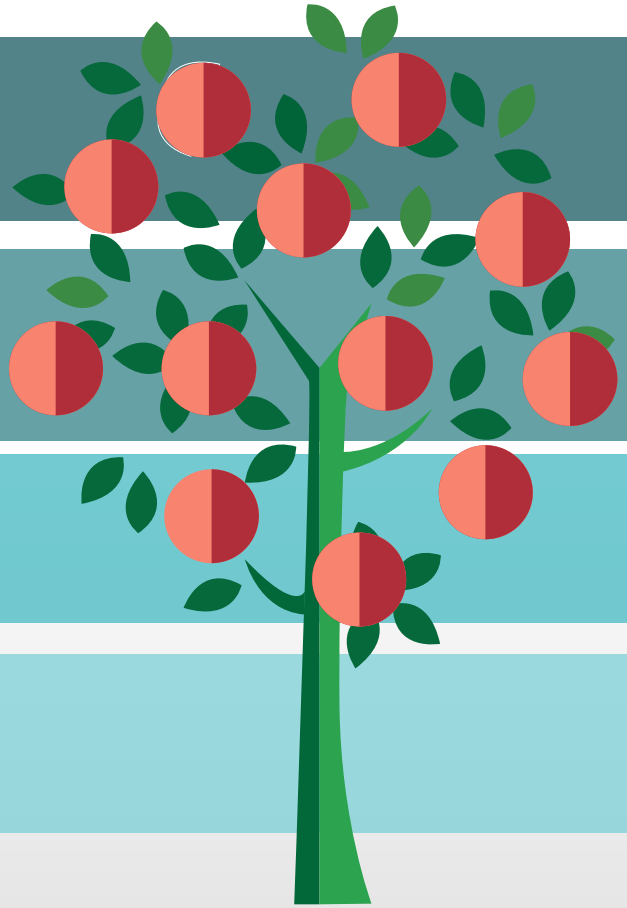
	Prevents counterfeit fraud of exposed data?	Protects data in transit?	Protects data at rest?
EMV Chip only	✓	X	X
Encryption + Tokenization	X	✓	✓
EMV Chip + Encryption + Tokenization	✓	✓	✓

ControlCase
Compliance as a Service

The Move to EMV

ControlCase
Compliance as a Service

The Security Fruit Tree

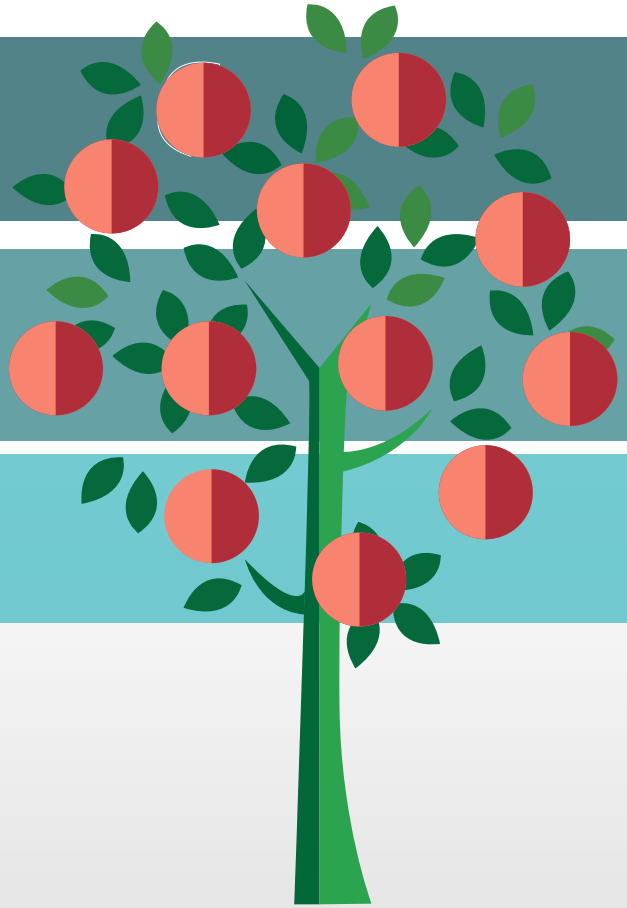


High Fruit	PCI and EMV
Bulk fruit	EMV
Low-hanging fruit	Card-Not-Present
Ground fruit	Magnetic stripe

ControlCase
Compliance as a Service

The Security Fruit Tree after EMV migration

High Fruit	PCI and EMV
Bulk fruit	EMV
Low-hanging fruit	Card-Not-Present



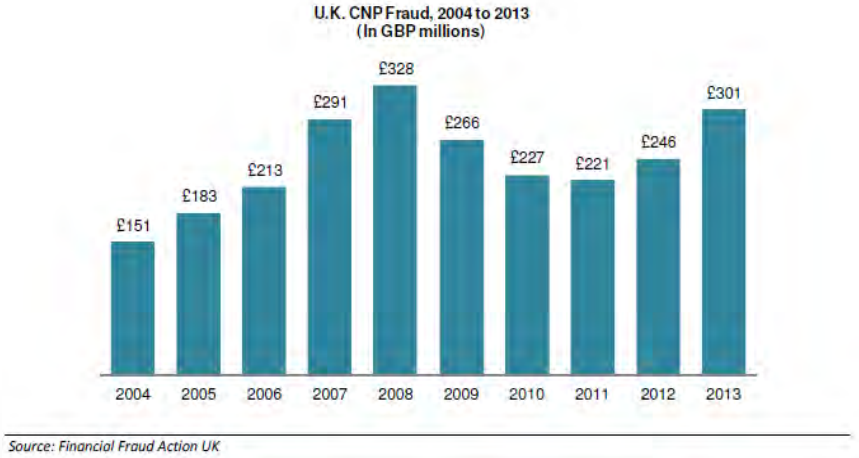
ControlCase
Compliance as a Service

Global Trends

Canada

Counterfeit and Lost/Stolen
CNP

UK



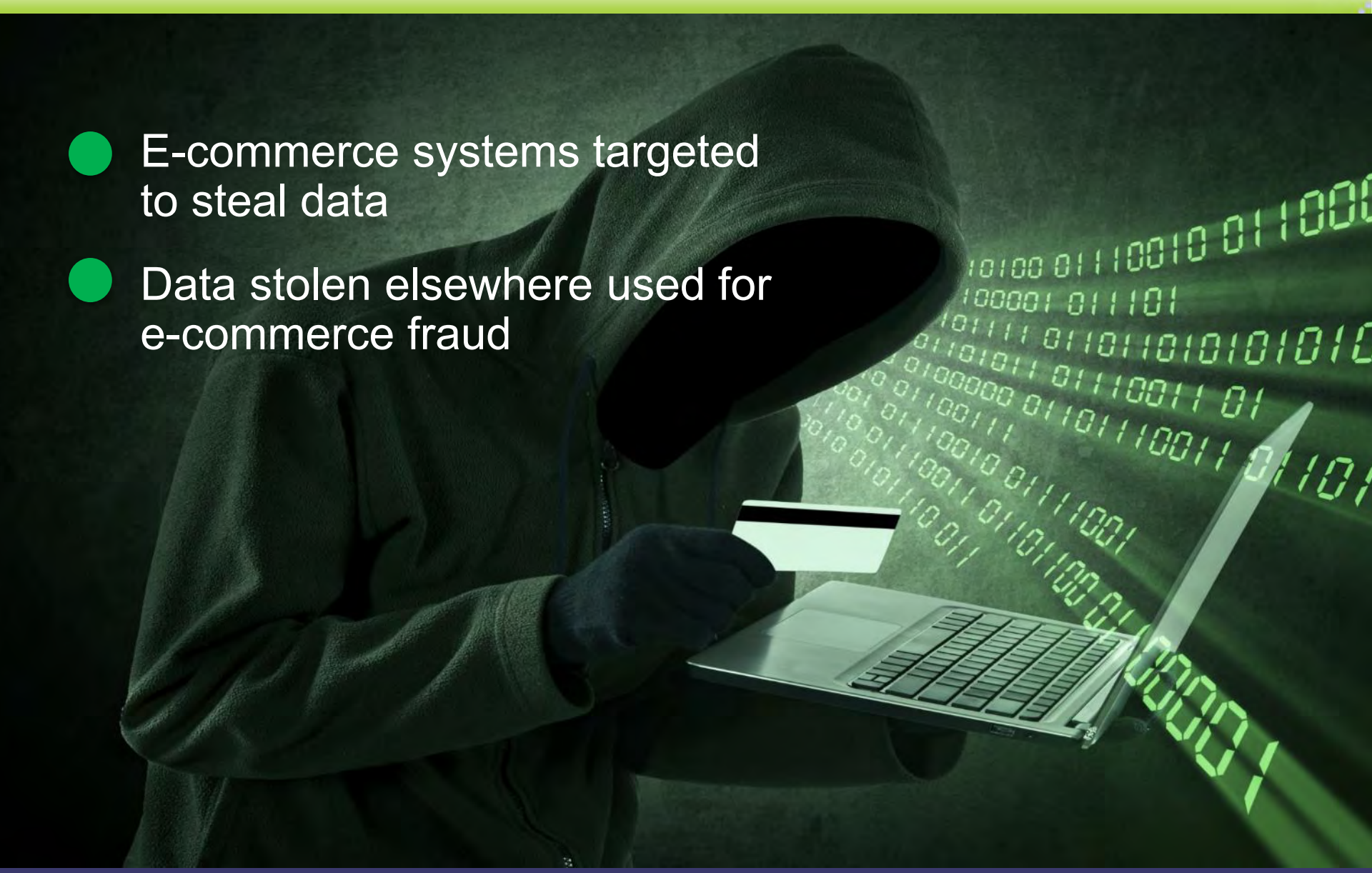
According to Aite Group, CNP fraud in the U.S. is projected to double by 2018 to $6.4 billion

ControlCase
Compliance as a Service

E-Commerce Security

ControlCase
Compliance as a Service

Threats to E-Commerce



- E-commerce systems targeted to steal data
- Data stolen elsewhere used for e-commerce fraud

Protecting E-Commerce

E-Commerce systems as a target

- Controls that prevent, detect, & respond to threats
- PCI security standards

Common Implementations

ControlCase
Compliance as a Service

PCI DSS v3.2 SAQ Updates

- Merchant web servers that perform redirect continue to be highly targeted
- Basic security controls not being applied.
- SAQs A and A-EP include new requirements to help organizations address this threat.

SAQ A	• Change default passwords and implement an incident response plan • Implement basic authentication controls, such as a unique user ID and strong password
SAQ A-EP	• Added requirements related to secure configuration of the webserver and network, access controls, authentication, and audit logs • Additional process/policy requirements

ControlCase
Compliance as a Service

Protecting E-Commerce

E-Commerce systems as a target

- Controls that prevent, detect, & respond to threats
- PCI security standards

Protecting E-Commerce

E-Commerce systems as a target

- Controls that prevent, detect, & respond to threats
- PCI security standards

E-commerce used for fraudulent transactions

- Fraud detection and modelling
- Cardholder authentication

ControlCase
Compliance as a Service

3-D Secure

- Collaboration with EMVCo
- Supports EMV® 3-D Secure 2.0 Specification
- Cardholder authentication for e-commerce and connected devices, including in-app purchases

ControlCase
Compliance as a Service

Securing Telephone Payments

ControlCase
Compliance as a Service

Telephone Recordings Containing PAN/SAD

- PCI DSS applies to audio recordings
- Methods are available to prevent storage of PAN/SAD
- Consider people, process, technology

ControlCase
Compliance as a Service

Securing Software

ControlCase
Compliance as a Service

Securing Software

- Software development is continuous
- The threat is continuous
- Application security must also be continuous

ControlCase
Compliance as a Service

Promoting a Security Mindset

ControlCase
Compliance as a Service

Compliance AND Security

- Security is a 24x7 mentality
- Not a “check-the-box” once a year and done

ControlCase
Compliance as a Service

PCI Resources

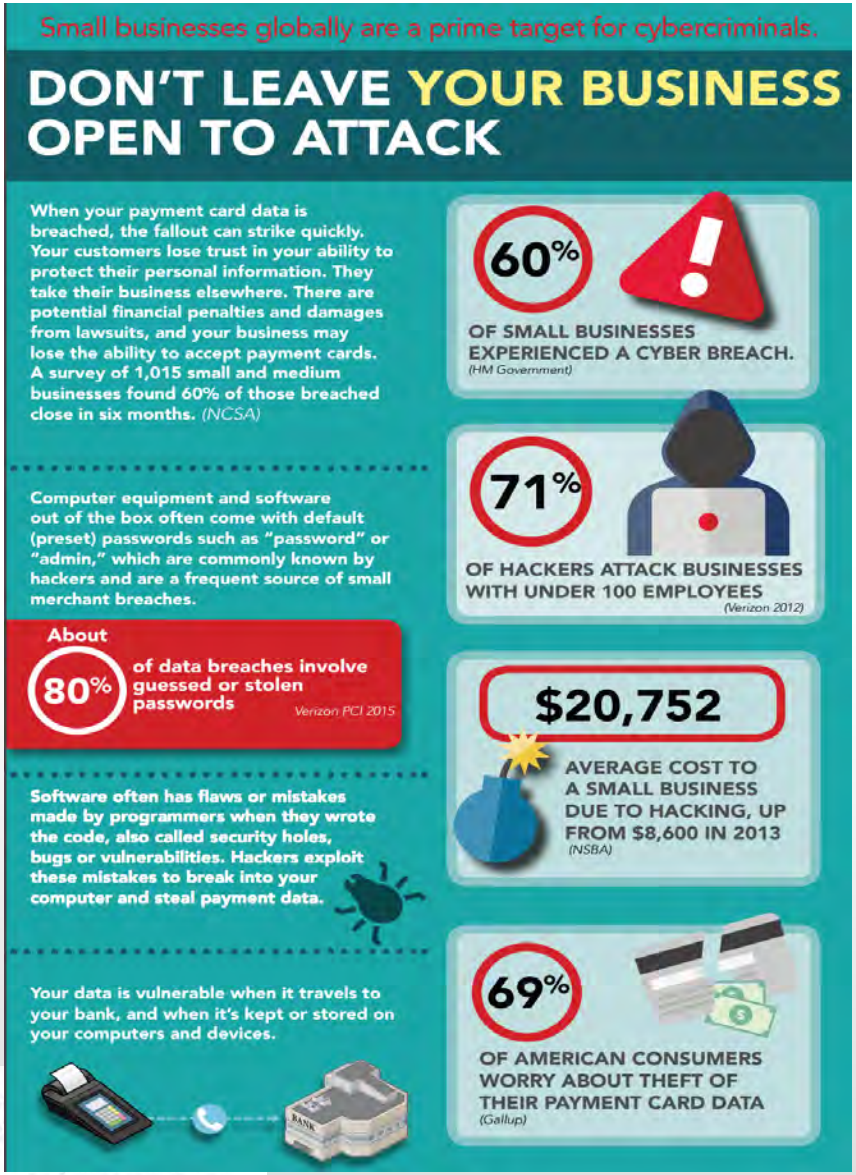
Guidance Documents

- Building a security awareness program
- Protecting against malware
- Skimming prevention
- Defending against phishing attacks
- Working with third parties
- Maintaining PCI DSS compliance
- Accepting payments with a mobile devices
- *Coming Soon:* Securing E-Commerce

Available at: www.pcisecuritystandards.org

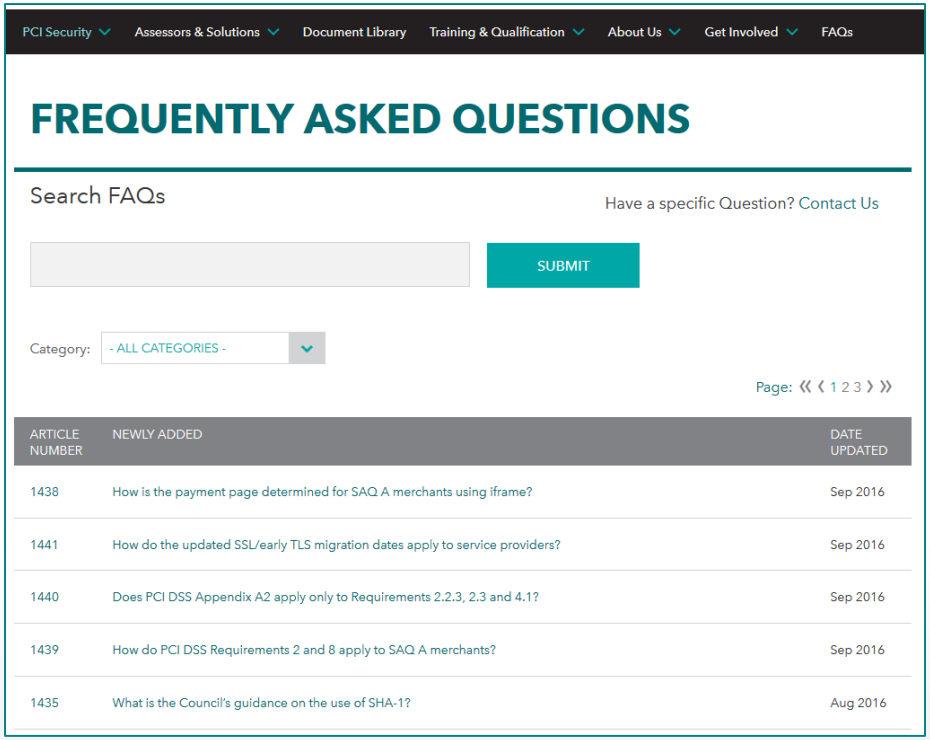
ControlCase
Compliance as a Service

Small Merchant Guidance



FAQs

- New FAQs regularly added
  - PCI DSS v3.2 transition dates
  - SAQ eligibility
  - Multi-factor authentication
  - Migration dates for SSL/early TLS
- RSS Feed available



www.pcisecuritystandards.org/faq

ControlCase
Compliance as a Service

Thank you

ControlCase
Compliance as a Service