KPMG

When business as usual becomes unusual

Session 5: Managing risk in turbulent times

—

6 May 2020

KPMG

When business as usual becomes unusual

Welcome to our weekly webinar. We will be starting shortly so if you don't hear any sound, don't worry, you're not missing anything - we'll be starting in a few minutes

Introduction

- **Format of the webinar**
- **Asking questions**
- **Further webinars and updates**
- **Reference to materials / webinar playback**

Webinar presenters

Russell Kelly
Senior Partner & Moderator
russellkelly@kpmg.co.im

Elaine McCormack
Senior Manager, Advisory
emccormack@kpmg.co.im

David Watterson
Senior Manager, Advisory
davidwatterson1@kpmg.co.im

Bryan Beesley
Senior Manager, Advisory
bbeesley@kpmg.co.im

Agenda

Introduction

Regulatory risks

Fraud risk impact of COVID-19

Staying cyber secure

Wrap up and questions

KPMG

Introduction

Russell Kelly - Senior Partner

KPMG

Regulatory Risks

Elaine McCormack– Senior Manager, Regulatory Advisory

Regulatory expectations

- Regulator will always expect firms to notify them where they are experiencing difficulty in complying with requirements – this is no different to usual. Be proactive;
- Standard notification requirements should be met where practicable, if delays are necessary notifications asap thereafter;
- Significant operational issues, significant financial strains – current circumstances not appropriate to wait until a regulatory threshold or trigger breach before making notification;
- Recognition that may be difficulties with areas such as finalising audits – regulatory forbearance framework;
- Prudence in decision making – directors are ultimately responsible for managing their business. Directors should fulfil ongoing duties towards regulated entities and clients;
- Financial strain – maintain sufficient financial resources capital & liquidity. Act prudently when making decisions re dividends, upstreaming excess capital, liquidity or any other decision that could weaken the IOM regulated entity.
- Treat customers fairly – FSA have issued guidance to consumers

Regulatory Forbearance Framework

Audited Financial Statements	4 months after financial year end
– Can submit up to 6 months if 4 months is not possible	
– Submit returns electronically via password protected PDF	
– Annual Compliance Return and auditors confirmation can be submitted alongside audited financial statements	
– If fully complete prior to the 4 month deadline – submit as normal	
– If your normal deadline for submission is 6 months after the financial year end – no changes apply	
– If you can't meet the extended deadline – engage with the FSA	
– Not required to notify in advance if you are partaking in the extended deadline	
– Quarterly FRRs – if a delay to the audit means you don't have a new annual audited expenditure figure for inclusion use the figure from the previous financial year end. If this results you falling below or within 110% of your minimum regulatory requirements notify the FSA.	

Financial Intelligence Unit guidance

- Issued separate guidance;
- Expected increase in financial crime/money laundering as criminals taking advantage of situations, people and businesses in trouble conduct criminal activity to compensate for financial losses;
- MLRO function increased importance at this time – higher level of vigilance;
- Risk assessment – identify specific risks and mitigation strategies;
- SARs submitted online. Advise FIU if experiencing any delay that would prevent SARS being submitted on a timely basis.

AML/CFT guidance

Guidance is not law, but is persuasive – moving feast will be added to when appropriate

Verifying identity – vital that this continues to determine whether a customer is who they say they are.

- Consider information and documents on a case by case basis. Take into account the risk of the customer and any introducer
- 'Meet' customers through video conference, scanned/photographs of copy documents may be used and verified by video call.
- Selfies - FSA considers acceptable for address as well as ID. Clear scanned copy of document and photograph of persons face and image on ID document being held in same picture e.g. driving licence
- Statements/bills in e-format – acceptable provided show residential address, not just email address. Verify by one of the above methods.
- Section 7 Handbook - you may be satisfied customer is who they say they are without verifying all suggested components of ID e.g. address. This is acceptable provided signed off by SM.
    - If a decision is made to implement change for class of customers document in BRA.

AML/CFT guidance

- Training – must be conducted annually – Authority will take pragmatic approach, expect to see proactive measures – looking to undertake via webinar

- Signatures – Consider whether wet signature is required or whether an electronic signature is acceptable legally and consider arrangements for witnessing signatures where relevant.

- Handbook allows CDD to be obtained electronically, but authenticity of documented must be verified appropriate.ly. If moving from wet to electronic signatures, entities should undertake and document in business and technology risk assessment where appropriate.

- Not specifically COVID related - sector specific guidance issued for banking and money lenders and also consultation papers and responses for insurers

Practical steps you can take

Consider regulatory expectations – what do you need to let the regulator know?

Consider material outsourcing, review arrangements as part of your business continuity planning – what alternative arrangements do you have in event that the outsourced party is unable to provide outsourced services.

What changes have you made to business processes in light of recent events – do you need to update your business risk/technology risk assessment. Consider additional risks , changes to your risk appetite, customer risk assessments etc.

Consider your business continuity plan – what has worked, what hasn't. Where do you need to make changes.

Think about compliance and control procedures, these still need to continue.

Document decision making - particularly where exceptions to the 'norm' are made.

Consider any Data Protection issues, particularly where there may be change in processes with WFH

KPMG

Fraud risk impact of COVID-19

David Watterson – Senior Manager, Advisory

Fraud risk impact of COVID-19

"Fear brings out the best in some people and the worst in others. It's a test of character, for individuals and nations."

Source: David Ignatius, Washington Post, 16 October 2014

Fraud risk impact of COVID-19

Source: Mtaylor848, wikimedia.org, CC-BY-SA-4.0, 8 March 2020

Fraud risk impact of COVID-19

Coronavirus latest: Warning against fake Covid-19 'miracle cures' sold across the UK

Unlicensed medicine could pose a risk to your health, the UK's medicine regulator has cautioned

Source: iNews.co.uk, 5 April 2020

Coronavirus: UK forces hundreds of scam Covid-19 shops offline

Source: bbc.co.uk, 21 April 2020

Fraudsters exploiting Covid-19 fears have scammed £1.6m

Criminals are escalating activity that targets the vulnerable, analysts have said

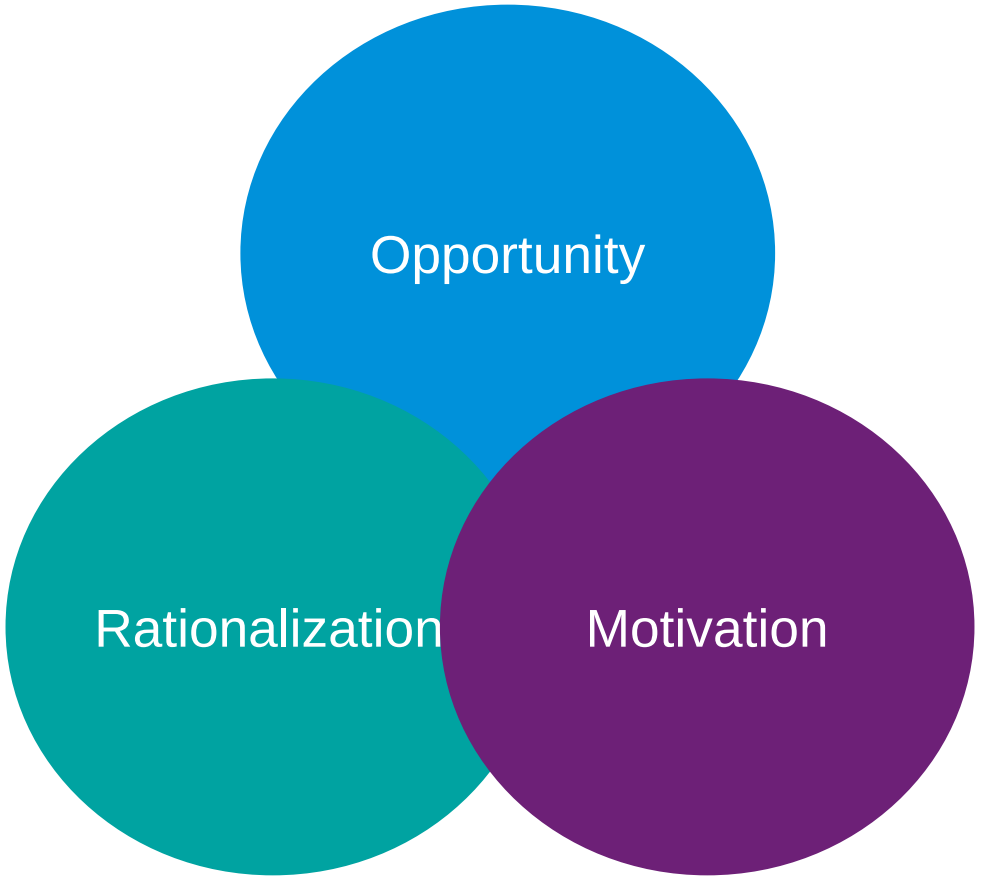
Source: theguardian.com, 4 April 2020

Captain Tom Moore: Just Giving blocks copycats over fears scammers are 'cashing in' on £28m NHS fundraising campaign

Exclusive: As the war veteran's effort passes £28m, online fundraising sites monitor new pages closely

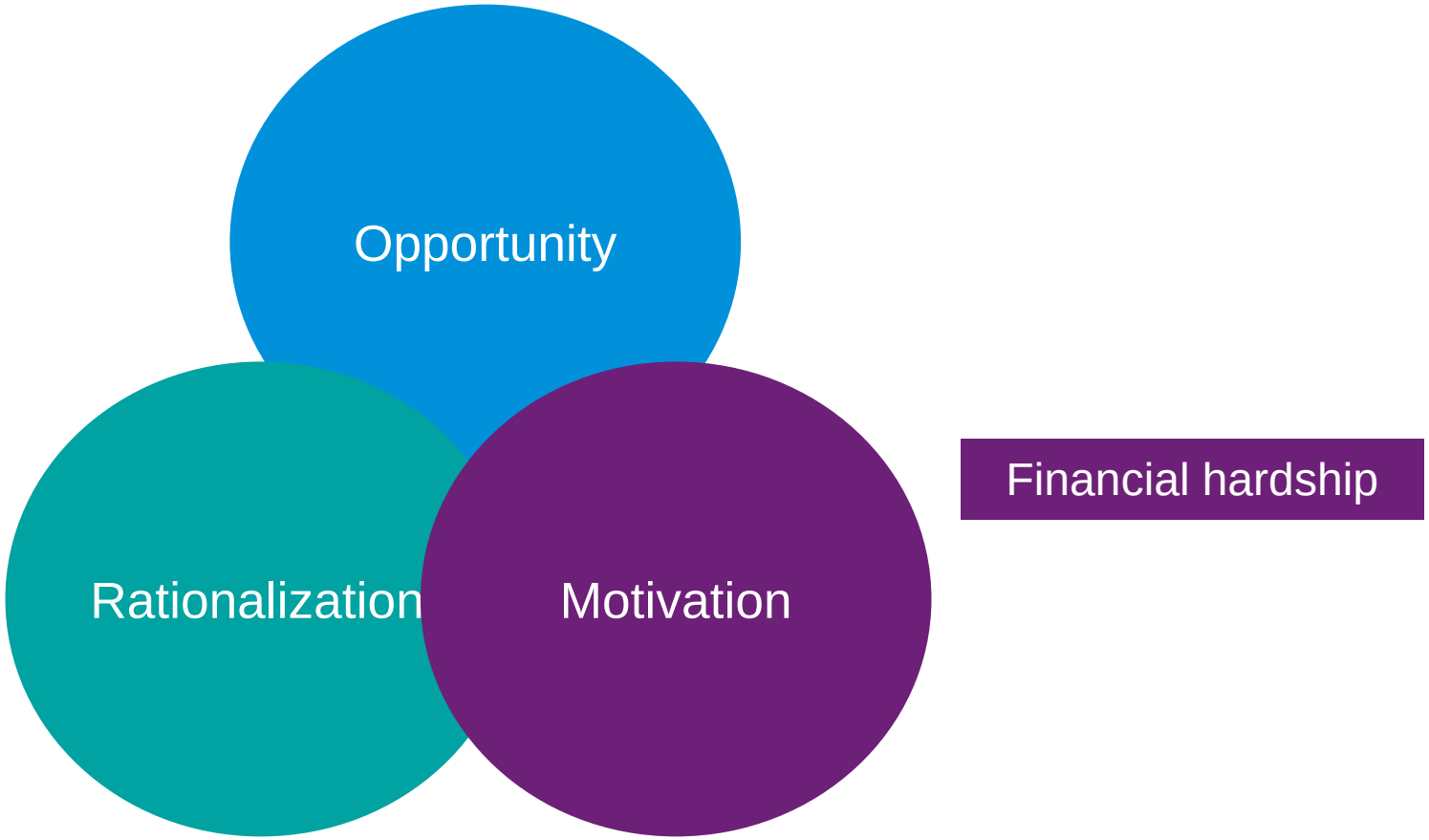
Source: iNews.co.uk, 22 April 2020

The Fraud Triangle



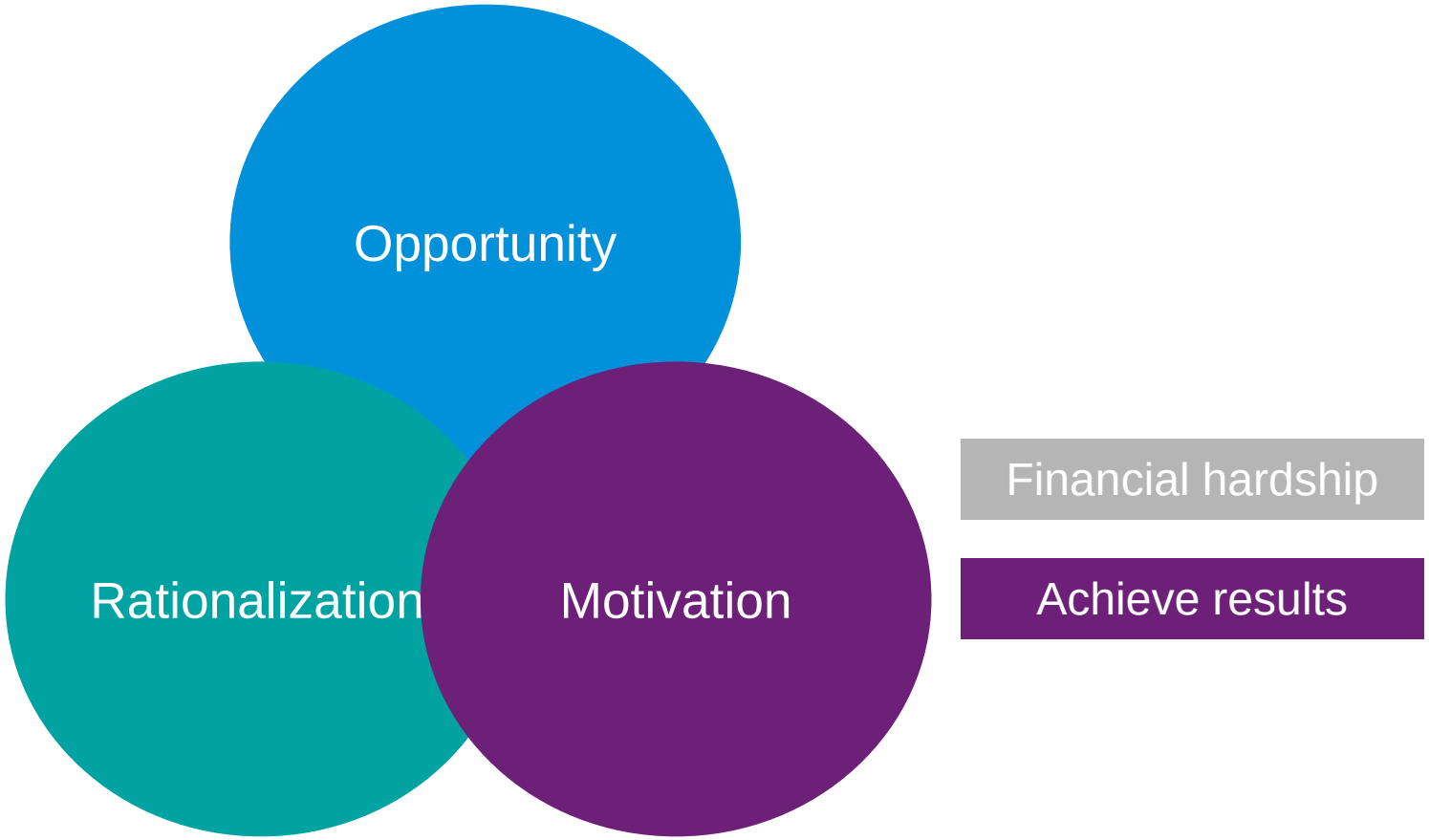
Source: Donald Cressey, 1953

The Fraud Triangle



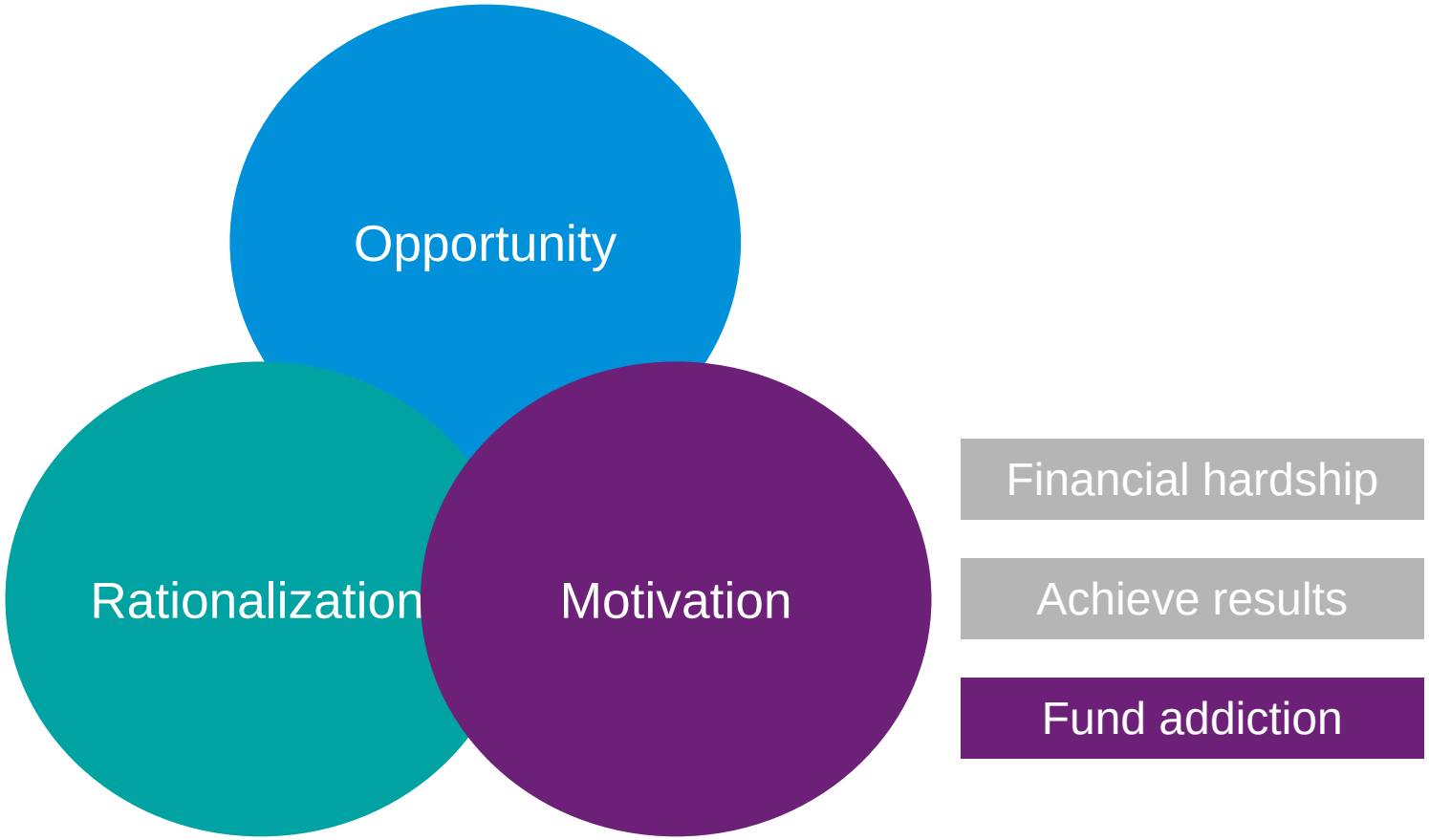
Source: Donald Cressey, 1953

The Fraud Triangle



Source: Donald Cressey, 1953

The Fraud Triangle



Source: Donald Cressey, 1953

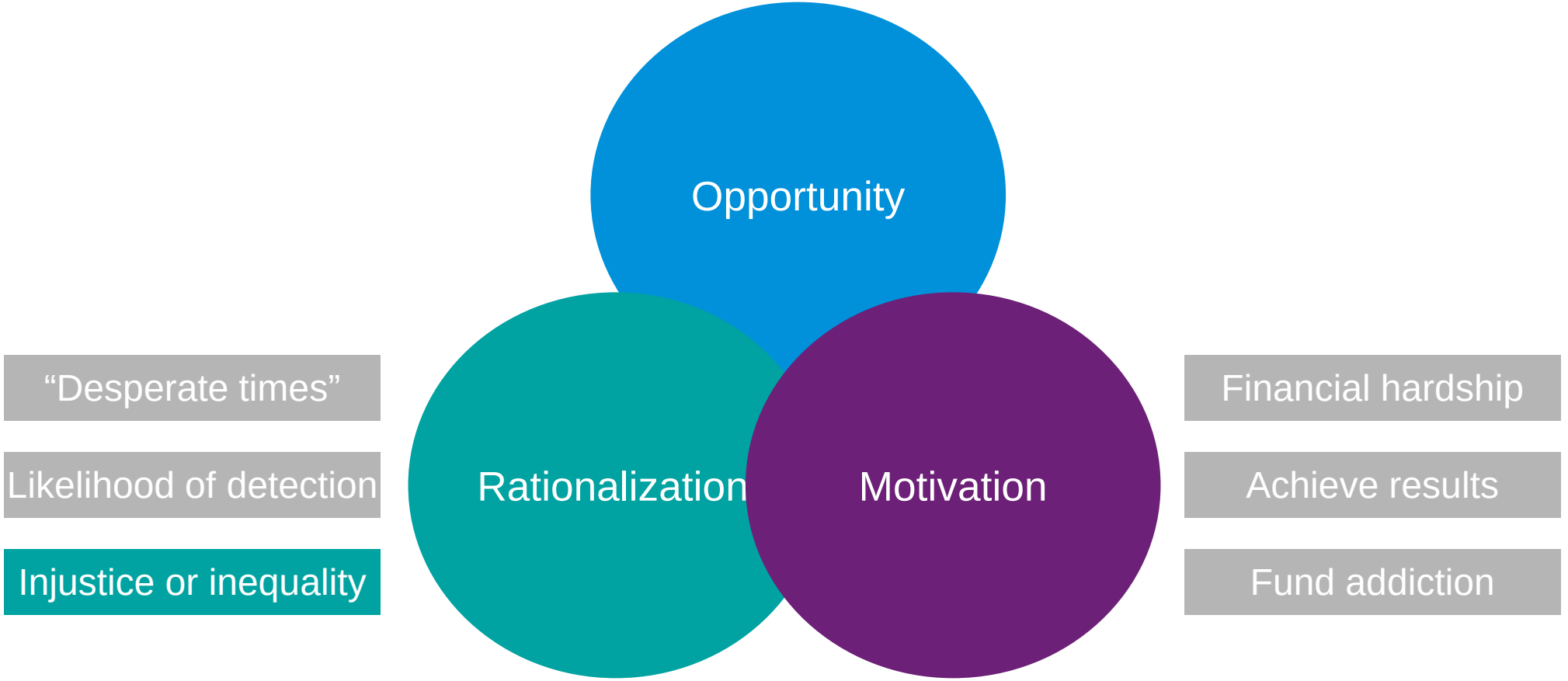
The Fraud Triangle

Source: Donald Cressey, 1953

The Fraud Triangle

Source: Donald Cressey, 1953

The Fraud Triangle

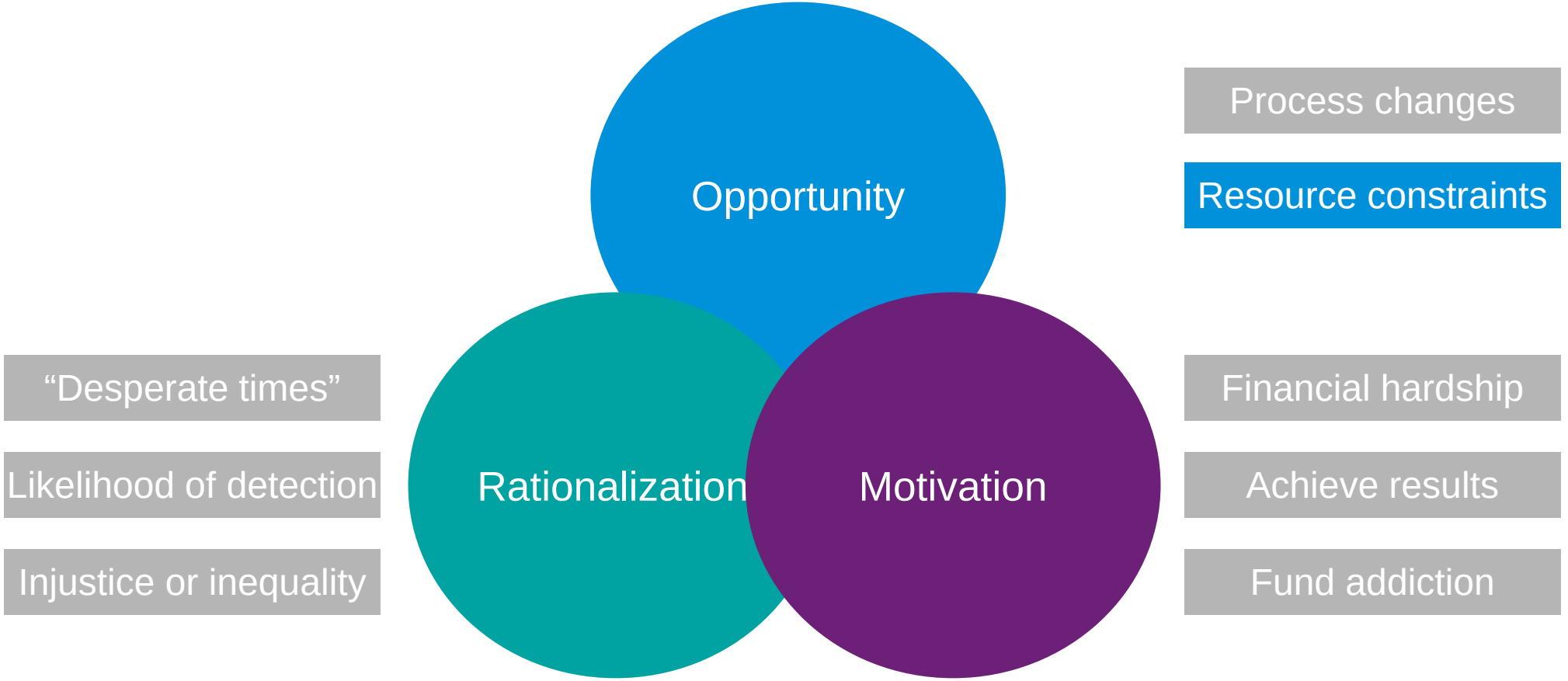


Source: Donald Cressey, 1953

The Fraud Triangle

Source: Donald Cressey, 1953

The Fraud Triangle



Source: Donald Cressey, 1953

The Fraud Triangle

Source: Donald Cressey, 1953

The Fraud Triangle

Source: Donald Cressey, 1953

Suggested steps

- **Review existing fraud risks and identify new ones**
- **Identify controls that have been rendered ineffective**
- **Revise or replace controls where needed**

KPMG

Staying cyber secure

Responding and maintaining amidst COVID-19

Bryan Beesley – Senior Manager, Advisory

Emerging threats

Fake sites selling Coronavirus key supplies

Trojanised Coronavirus maps and resources

Masquerade as health organisation (E.g. WHO or CDC)

Masquerade as government providing tax and benefits advice

Setup fake Coronavirus information sites

Fake charitable collections for health workers

15,000

sites in last week

Ransomware

CEO/BEC Fraud

Crypto currency frauds

O365 credential theft

Cyber Safety During Pandemic

There have been multiple reports of increasing number of scams and online phishing attacks relating to the coronavirus. Whilst we are all trying to stay safe from the real virus, please also watch out for potential phishing attacks trying to infect your computer with computer virus.

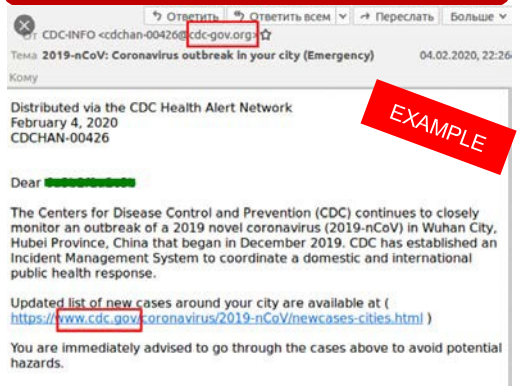
Types of attacks seen so far

1

Email phishing attacks using malicious coronavirus themed websites

.coronavirusstatus[.]space
.coronavirus-map[.]com
.coronavirus[.]zone
.cdc-gov[.]org

.....and many more.



2

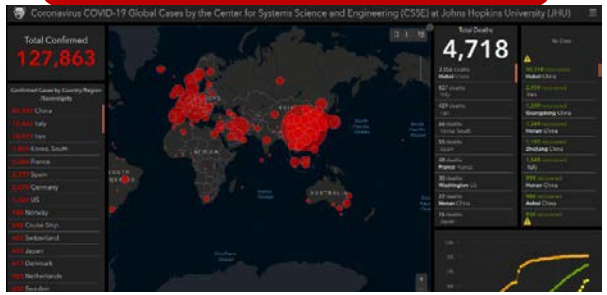
Email phishing attacks with malicious office file attached

Malicious file attached in email claiming to have the latest information about the virus contains malware targeting Microsoft office applications

3

Malicious "Live Coronavirus Map" application

A malicious application claimed to have a live map of Coronavirus contains password stealing malware



Tactical actions to remain safe

Aspects to consider:

- Remote access infrastructure
- Secure adoption of BYOD
- End point security
- Identity & Access Management
- Collaboration platforms
- Shadow IT & Cloud SaaS services proliferate
- Cloud brings capacity but security challenges
- Testing security controls

Thinking more strategically the new normal

Within the CISO function

— Key personnel

— Virtual war rooms

— Dependence on key suppliers

— Augmentation

— Disruption of security operations

Beyond the CISO function

— Securing the digital footprint

— Security for a new normal

— Working in regulated industries

Technology and resilience... looking beyond cyber

Three key challenges our clients are facing from an IT service delivery and resilience perspective...

1

Third Parties

2

Service Delivery

3

Change Management

Wrap up and questions

Russell Kelly - Senior Partner

Dates for your diary

Join us every Wednesday at 10:00 for our webinar:

13 May - Tax update

KPMG

Thank you

Russell Kelly
Senior Partner
KPMG in the Isle of Man
T: +44 (0) 1624 681013
E: russellkelly@kpmg.co.im

Elaine McCormack
Senior Manager, Advisory
KPMG in the Isle of Man
T: +44 (0) 1624 681024
E: emccormack@kpmg.co.im

David Watterson
Senior Manager, Advisory
KPMG in the Isle of Man
T: +44 (0) 1624 681063
E: davidwatterson1@kpmg.co.im

Bryan Beesley
Senior Manager, Advisory
KPMG in the Isle of Man
T: +44 (0) 1624 681042
E: bbeesley@kpmg.co.im