
AZETS

Remote working, an opportunity for fraud

26 November 2020

AZETS

Today’s speakers

Martin Chapman

Partner, Forensic Accounting

E: martin.chapman@azets.co.uk

Adam Finch

Partner, Dispute Resolution

E: afinch@hcrlaw.com

Today’s agenda

- Remote working, what is the risk?
- The size of the problem
- Why fraud is committed?
- Investigating fraud
- Legal remedies
- Preventative measures

AZETS

Poll question

What do you consider to be the biggest fraud risk to you and/or your organisation?

AZETS

Remote working, what is the risk?

- Fraud is a risk to everyone of us and our businesses
- Remote working presents an increased opportunity for fraud, principally revolving around the following areas:
  - Increasing cyber crime
  - Increase in employee fraud
- Before we review the impact of remote working, we need to understand two key questions…

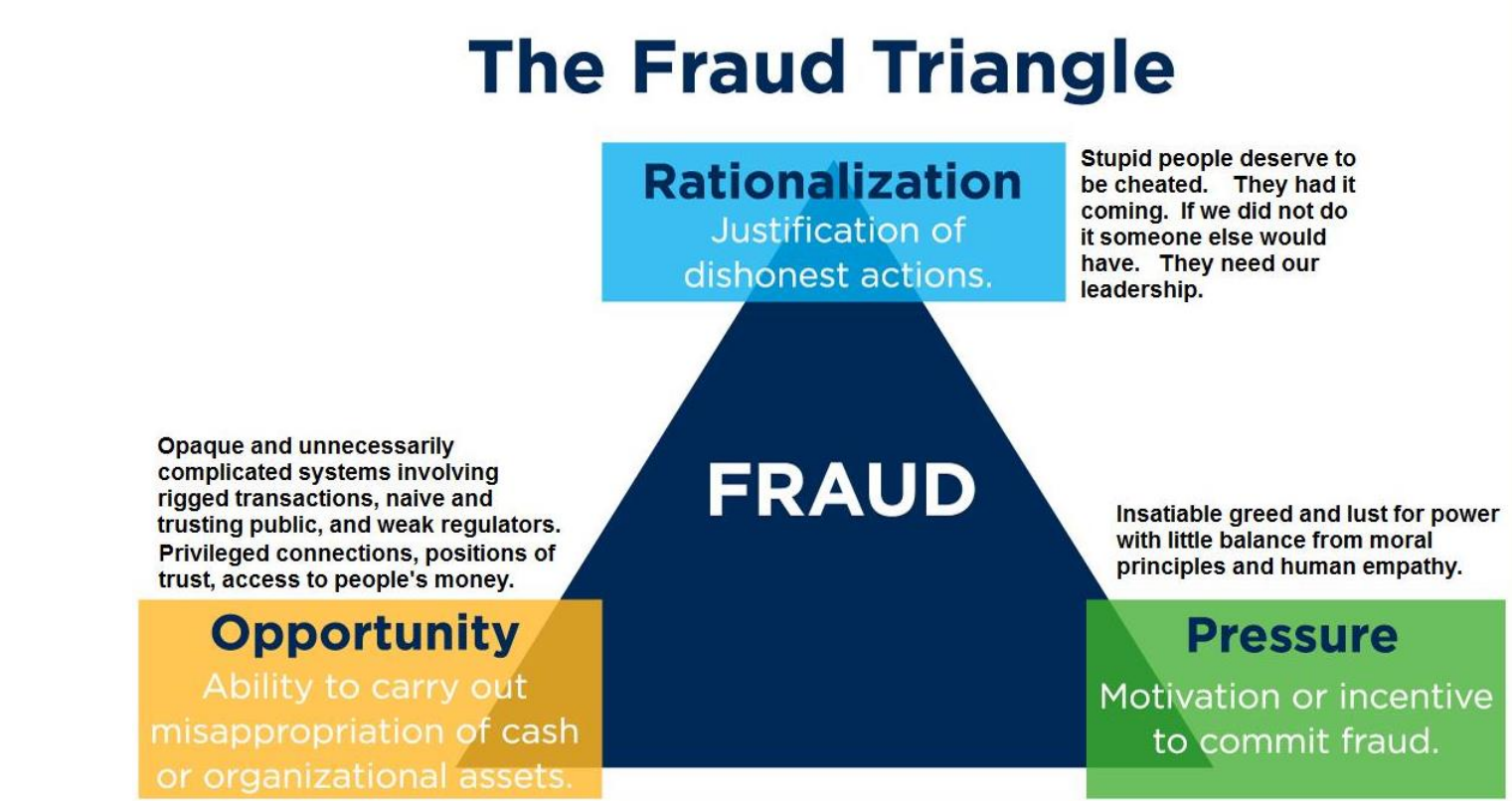
What enables a fraud to happen?

People

Process

Technology

How remote working increases the opportunity for fraud to take place



Cybercrime

What is it?

Cybercrime is an ‘umbrella’ term for lots of different types of crimes which either takes place online or where technology is a means and/or target for the attack.

Fastest growing fraud in the world

- Cybercrime costs the UK Economy £15 billion a year. Latest government report puts this at £27 billion per year
- Cybercrime is forecast to grow from $3 trillion (globally) in 2015 to $6 trillion by 2021
- One act of fraud or cybercrime is committed every six seconds in the UK

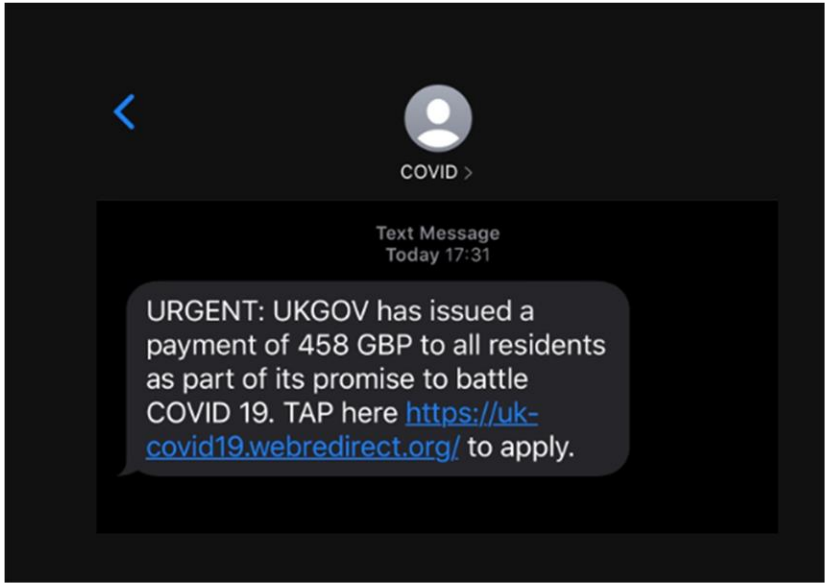
Cybercrime

What are we seeing?

Cybercrime cases on the rise: anywhere between 30 and 50% during lockdown 1.

Types (numerous)

- False donation pages
- False texts from HMRC and other agencies
- False online sales of PPE
- COVID-19 update subscriptions
- Payment diversion
- Mandate fraud
- Data breach and theft of businesses IP
- Malware



Employee fraud

Why?

Fraud Triangle – think of the three corners

- Rationalisation: I'm on reduced hours. I've not been supported
- Opportunity: Less scrutiny, working from home
- Pressure: Money is tight, I have bills to pay

New fraud's emerging as a result of the above

But…

- Old / Existing fraud is being discovered as tighter reviews are taking place of finances and systems as companies have more time

Employee fraud

What are we seeing…expect to see?

- **Diversion of funds**
  - Bank transfers intended for suppliers sent to personal accounts
  - Cheque fraud
  - Expenses fraud
  - Payroll fraud e.g. false overtime
- **Collusion with suppliers for contracts – i.e. procurement**
- **Manipulation of results…why?**
  - Make “me” or “organisation” look better
- **Data theft**

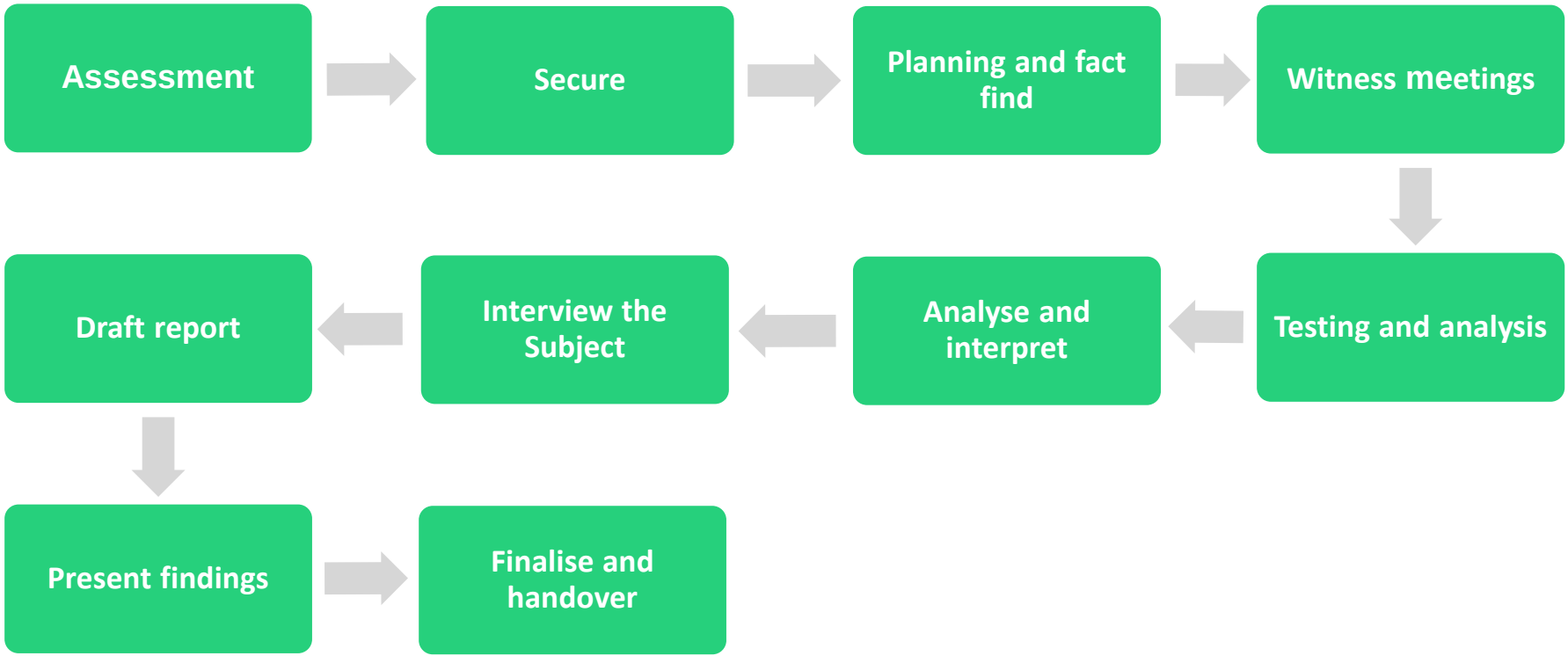
Remote working, why does this increase the level of fraud occurring?

- Less scrutiny
- Weaker / harder to manage IT security
- Concentration and application
- Easier to conceal / get away with
- Collusion easier
- Justification of existence

Investigating a fraud

- **What do you need to consider**
  - Objective: This may change but have one!
  - Planning: Vital at all stages
  - Who: Need to know -v- want to know
  - Resources: Staff, physical, technology
  - Skill set: Right people involved
  - Time: How critical is this? Does the subject know? Tipping off
  - Logistics: Where and how?
  - Evidence preservation: Email, computer records, physical evidence
  - Regulator: When to notify?
  - Insurance: Do we have cover?
  - Police: When do we notify?
  - Laws, compliance and regulations: What's applicable?
  - Action Fraud: When and how?

Investigating a fraud, typical process



Remote working, an opportunity for fraud

AZETS

Legal Remedies

- Assessing your options is a balancing exercise.
- Key issues to consider when deciding how to proceed:
  - Your objectives and priorities
  - Have they changed from your initial plan?
  - Maintaining legal privilege
  - Preserving evidence
  - The strength of your evidence
  - Are there steps to take to strengthen your claim?
  - What resources are available to pursue the fraudster?
- Criminal v Civil options available

Criminal Proceedings

Advantages:

- Sends a serious message
- Low cost option

Disadvantages:

- Lack of control
- No guarantee case will be pursued
- Speed
- Outcome

Civil Remedies

Advantages:

- Ownership
- Case can be quickly progressed
- Strong message to former and current employees

Disadvantages:

- Significant costs
- Resources required to support

What can be done?

- Injunction
- Worldwide Asset Freezing
- Search and/or Delivery Up
- Tracing of assets
- Disclosure / Norwich Pharmacal Orders / Bankers Trust Order
- Affidavit evidence
- Cross – undertaking in damages
- Claims available

Private Prosecutions

- Not brought by the crown but by an individual and / or company
- Otherwise, proceed similar to that of a crown prosecution

Advantages over a crown prosecution:

- Quicker
- More focussed
- Control

Intellectual Property and COVID-19

What is intellectual property *("IP")?*

IP is intangible property which is owned and protected by a company. Things such as a website address, brand logos, software, patents, etc.

How is COVID-19 affecting the sudden rise in IP fraud / theft?

Due to the current economic climate and the effect this has had on people's income and ability to generate profit, there has been a substantial increase in IP fraud.

What is being accessed / stolen and why:

- Businesses Internet protocol address ("**IP address**");
- A businesses logo / brand name / trademark; and/or
- Patents / designs.

Preventative measures for IP theft

- Ensure your patents, trademarks, copyrights etc are registered correctly and proof of registration retained;
- Look to include an intellectual property rights clause into your contracts of sale and employment;
- Train staff to recognise a phishing / click bait email;
- Ensure your IT support staff are actively and routinely monitoring for such attempts trying to break the firewall and updating / alerting staff to such;
- Ensure high quality malware software is installed on all electronic machinery that has access to company documentation / information including companies ensuring (and probably paying for) malware for personal items of staff such as computers, laptops, mobile phones etc if work communication is being diverted / worked on such devices;
- Ensure your IT department are actively running updates to software and malware and you are not relying on your staff to do such; and
- Consider outsourcing your security to a specialist cyber security company.

Case Study

- A recruitment agency had staff working remotely. An employee moved to a competitor. He then poached customers using a social media platform – direct contact, targeted updates to his connections and generic postings.
- Our client wanted to take steps to protect its business. It had the usual restrictive covenants in place for post termination of employment. It also had a social media policy.
- We applied for an injunction against the former employee. Not only did we seek to enforce non-solicitation of customers, we also argued that LinkedIn was used as a database for its business. Helpfully, it had an enhanced LinkedIn account and the social media policy.
- The Court determined connections generated on LinkedIn during the period of employment, belonged to our client.
- The former employee was ordered to delete all of the connections generated during the period of employment.

Practical Steps

- Limit access to confidential information
- Limit devices that employees use to what is necessary and not to use personal devices for work purposes
- Ensure company property is returned by the employee before they leave
- Hold an exit interview and reiterate their restrictive covenants
- Mine servers/emails if you suspect any breaches (check your employment contracts for permission)
- Consider instructing professionals and a forensic expert at an early stage
- Reach out to customers / suppliers – work hard to keep them
- Ask new employees to create a new LinkedIn account for work purposes when they start
- Consider a social media waiver

Remote working, an opportunity for fraud

AZETS

Cyber security

- **Think about defence in depth, many layers – all requiring security.**
  - Crown Jewels - Identify what the critical assets & key information you need to protect are
  - Files and data – Map where your data is held and restrict access appropriately Minimise the damage a security compromise can lead to
  - Software – Enable security, restrict malware, develop securely, use cloud
  - Platform – Build in resilience, think about end user devices. Bring your own device
  - Network – Ensure it is up to date, securely configured and patched
  - Users – Educate and tolerate, encourage reporting
  - Physical – Never forget how important physical security is
  - Anticipate – Rehearse responding to a data loss, investigating a data breach, restoring data from backup servers

Remember…
National Cyber Security Centre: Online guidance
https://www.ncsc.gov.uk/

Poll question

What do you think is the best preventative measure for employee fraud?

AZETS

Employee fraud: Prevention

- **Traditionally the top tip for prevention…**
  - **“Whistleblowing!”**
- **To get it right you need:**
  - Strong and accessible policies
  - Training and evaluation
  - Culture of openness and trust
- ***Your staff are your “eyes and ears”***
- ***Does being remote make this harder?***
  - Need the right culture

Other prevention tips

- **Know the areas of risk and profile them:**
  e.g. money handling, IP
- **Know the key assets and what / who protects them:**
  e.g. cash, banked funds, data, IP
- **Produce, test and retest policies and procedures**
- **Train staff**
- **Use data to analyse patterns:**
  e.g. change of bank details, leavers and joiners, holiday records

To me "Data" is the biggest help to you with remote working – control it, understand it and analyse it and you may identify fraud?!

Thank you for listening

Any questions?

AZETS

Upcoming webinar…

Customs duty and VAT : Get ready for 2021

Thursday 10 December 2020 | 12:00pm - 13:00pm

Speak to your Azets contact or email webinars@azets.co.uk

Disclaimer

The purpose of this presentation is to **give general information** on the subject matter presented.

It is **not intended to be a comprehensive analysis** of the subject matter that is being discussed or presented in written or verbal form. The information is believed to be correct as at 22 November 2020

It is **not intended to be a substitute** for formal advice from the appropriate person in the organisation to a client under the terms of a suitable signed engagement letter.

AZETS

We are an accounting, tax, audit, advisory and business services group that delivers a personal experience both digitally and at your door.

Accounting | Tax | Audit | Advisory | Technology

hello@azets.co.uk

Follow us