TenInsight

TenIntelligence
London | Dubai

www.tenintel.com

Due Diligence | Investigations | Protection

Issue 011 | January 2021

A new year ahead often means new resolutions, challenges, projects and plans. This year should be no different. For us, each team member will start to set out their ideas and plans for their personal development, which is a vital component to improving their working life.

At TenIntelligence, we have an initiative called Ten% time, which allows every team member the opportunity to dedicate time to personal development and individual projects.

Now more than ever, business leaders and employers must recognize that increasing stimulus and recognition in an individuals professional life will help with strengthening their mental health too. My colleague, Rae, has highlighted her thoughts from a personal journey on page 5. This edition also focuses on the tolerance of fraud in different cultures; a focus on COVID-19 fraud; brand protection cases from Dubai, examples of red flags found in recent background checks; and our 10-Point Plan on how to deal with a data breach.

Stay safe everyone!

Neil Miller, CFE | Founder
neil.miller@tenintel.com

COVID-19 Fraud: Don't Let Fraudsters Take Advantage of a Tough Situation

*In 2020 the UK Government implemented various relief and economy-boosting schemes as part of its coronavirus strategy. Yet, fraudsters have eyed up an opportunity, as Analyst **Jake Durham** reports:*

Over the last few months, the team at TenIntelligence have been raising awareness and supporting the recent COVID-19 anti-fraud campaign and anonymous hotline initiatives led by CrimeStoppers, the Cabinet Office and HMRC.

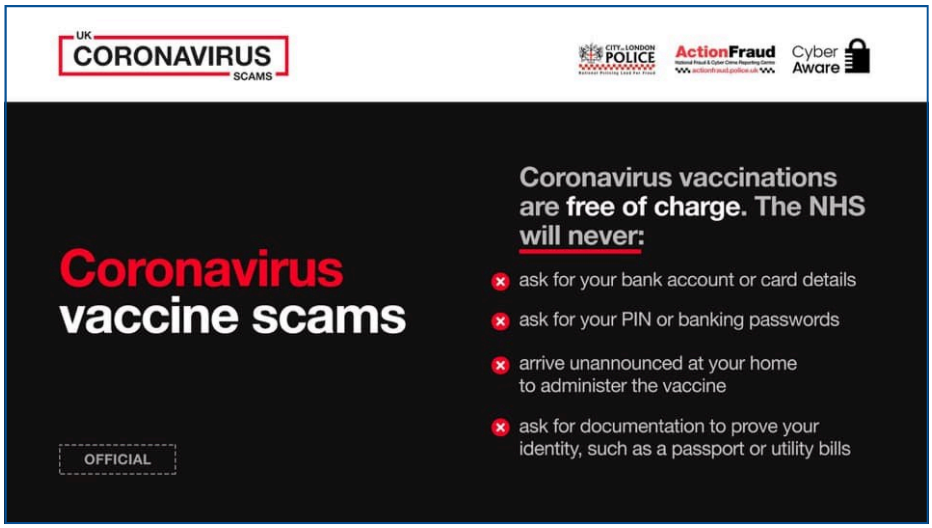
The Government introduced various financial stimulus packages and schemes including, job retention, self-employment income support, statutory sick pay and the famous "Eat Out to Help Out" scheme, which according to government figures attracted £849 million in claims for 160 million meals in August 2020.

While there continues to be a debate over the effectiveness of the UK Government's COVID-19 response, these schemes have provided a valuable lifeline to employers large and small.

The job retention furlough scheme (or CJRS) in particular has granted financial support to nearly 10 million people restricted from their jobs.

Anybody working in fraud prevention and due diligence will tell you that where there is opportunity, there is fraud.

So it was welcome news that HMRC and other enforcement agencies have partnered with CrimeStoppers to open a hotline and online form for members of the public to report so-called "COVID-19 Fraudsters".



Learn more about the types of COVID-19 fraud being investigated on Page 4.

Considerations when investigating fraud in different cultures.

While many aspects of human thought and behaviour are universal, my Psychology degree taught me that cultural differences can lead to often surprising differences in how people think, feel, and act; Senior Associate ***Valeryia Dockrell*** *reports.*

One of the key distinctions between national cultures can be characterised into individualism versus collectivism.

You will find individualistic cultures in Western European countries and North America where there is emphasis on individual goals rather than the group. Whereas Asian countries which have a collectivist culture, such as Japan, India and China, will emphasise group goals and personal relationships.

This is just one of the many ways in which culture can be split and examined, and even within this categorisation there are various nation-specific cultural differences.

It is certainly important to acknowledge that cultural differences exist and where ***an activity might be perceived as normal in one culture, it maybe be considered corrupt when investigated using the cultural values of another***.

Culture also has an influence on the detection of fraud, where individuals in one culture may be less likely to speak out, or simply don't recognise that fraud and corruption is taking place, as the observed practises are not perceived as wrong.

Looking at an example of a collectivist culture such as Japan, we can look at certain cultural traits which are more prevalent in this nation, such as obedience and loyalty.

While these characteristics can have a positive influence in some environments, they can be damaging in the case of fraud and corruption.

In Japanese there is a proverb 'the nail that sticks out gets hammered down'. Whereas in some cultures that nail would probably get a promotion.

In 2015, it was uncovered that Toshiba had inflated their profits numbers by £780m over a period of 7 years from 2008 to 2014. An investigative panel concluded that it was the culture of silence, obedience and loyalty which influenced fraudulent accounting practices.

Additionally, although senior management did not explicitly instruct that fraud be committed, it is believed that they relied on the Japanese corporate culture of obedience. Falsification of the profits occurred as a result of impossible targets, which lead to employees lower in the hierarchy doing whatever it took to meet them.

Some research suggests that loyalty to colleagues and the business that is found in collectivist cultures will mean that employees will be reluctant to disclose improper behaviours of others and in turn discourages whistleblowing.

Data indicates that whistleblowing is the most effective way to detect fraud, therefore cultures which value group goals and harmony, can have a negative impact on fraud detection.

Research found that collectivism is negatively associated with auditor's compliance with fraud risk assessment procedures as they are more motivated to maintain group harmony as part of their national cultural values.

Another cultural theory looked at tight and loose cultures in terms of enforcing social norms, and can be compatible characteristics with individualism.

For example, East Asia is collectivist and tight, and the US is loose and individualistic. But some places that are individualistic can also be tight such Germany and Switzerland.

In a 2018 study it was identified that ***people from tight cultures, like Norway, reported less tolerance for insurance fraud, were less likely to commit the fraud,*** and they perceive higher level of risk of being caught than their counterparts from loose cultures, such as Ukraine.

Other studies looked specifically at different cultures in relation to specific behaviours such as acceptability of bribe payments. Accountants in Asian and Pacific regions were found to not consider bribes as fraudulent behaviour.

A study of Chinese salespeople suggested that their attitudes towards unethical behaviour were more tolerant than those of their US counterparts.

Additionally, in African countries, such as Nigeria, there is a perception that a ***bribe is needed to solve various forms of administrative problems*** in a timely manner and refusal to give a bribe may be met with negative consequences.

As well as other areas of impact, such as culture and susceptibility to becoming a victim of fraud.

However, it should be remembered that despite national cultures, there are many subcultures and individual differences that can also have an effect.

Continued on Page 3

Continued from Page 2

The keynote is that to prevent, discover, and investigate fraud, the impact of culture should be understood. Failure to consider cultural differences may lead to ineffective fraud prevention and detection, in turn leading to major financial loss to the business and reputational damage.

Typical anti-fraud policies may not consider cultural differences, which is especially important for a company which operates across different jurisdictions.

There are many other cultural differences and influences that can be discussed, such as power distance which relates to how society deals with inequality, Masculinity and uncertainty avoidance, etc.

To fight fraud, you should understand the cultures in which you operate, then you can instill a corporate culture within your business that employees can identify with to facilitate an anti-fraud environment.

For further information about how we can help with investigating fraud, contact us on +44 (0) 203 963 1930 or email Val below.

Senior Associate
valeryia.dockrell@tenintel.com

Digital Forensics
Fraud Investigations
Asset Profiling and Recovery
Witness Tracing
Interviewing
Surveillance

www.tenintel.com/investigations

How identifying red flags uncover financial, regulatory and operational risks.

Last year TenIntelligence conducted over 500 due diligence checks on directors and senior executives for our clients, using our traffic light system based on Red Flags (High Risk), Amber Flags (Moderate Risk) and Green Flags (Minimal Risk). Analyst, **Tim Minchin** reports on why identifying red flags is important for your organisation.

Analysis from 2020 identified **16%** of our checks were flagged **Amber** and **3%** were **Red Flags.**

Despite what can be perceived as a low percentage, 3% of red flags can have a big impact on a business. The flags uncovered, helped our clients prevent financial losses from potential reputational impact on the company's public image.

For example, in January 2016, a senior Business Development Manager of an NHS Foundation Trust was dismissed after an internal investigation identified numerous discrepancies in his expenses. The investigation led to the discovery of approximately £350,000 worth of fake expenses and the lie of holding a PhD, a master's degree and five other diplomas being unravelled. Had the right checks been in place, this could have been avoided.

Having the right background information and checking practices in place, allows our clients to work with continued assurance and integrity.

The guidance set out by the London Stock Exchange (LSE) regarding AIM due diligence, should be a substantive tool in assessing appropriateness rather than solely a compliance tick box function.

The flags we identified in 2020 ranged extensively, as do the checks we cover, uncovering numerous severe near misses:

- Undisclosed litigation involving allegations of misrepresentation or **insider trading**
- Undeclared insolvencies from personal **historic bankruptcies** to compulsory company liquidations
- Ties to **sanctioned individuals** and companies or uncovering undisclosed offshore companies in notorious tax havens
- Declared **education qualifications faked** or not passed by the individual.

Our open-source intelligence gathering, includes a detailed examination of subscribed databases, press articles, company registries, court searches, public records and documents, insolvency registers, financial regulator fines and licenses, sanction checks as well social media platforms.

In addition, our in-depth interviews (unbiased industry insights) with former associates also helped reveal undeclared red flag issues such as:

- Misconduct, poor attitude, and misrepresentation
- Mismanagement causing shortfalls, lost contracts, litigation and fines
- Accusations of the misuse of alcohol, drugs and gambling
- The misuse of company funds or shares, short selling and over inflating company shares for gain.

It remains critical at TenIntelligence that our focus is to identify any potential risks to our clients, ensuring the individuals are considered "Fit and Proper" and mitigate any possible loss for our clients.

For further information about how we can help with background checks and enhanced due diligence, contact us on +44 (0) 203 963 1930 or email Tim below.

Analyst
tim.minchin@tenintel.com

COVID-19 Fraud: Continued from Page 1
Don't Let Fraudsters Take Advantage of a Tough Situation

As of 12 January 2021 there have been 21,707 reports of alleged fraudsters targeting COVID-19 stimulus schemes.

Here are three of the most common reported types of COVID-19 fraud, and steps to take to protect yourself and your business:

Furlough Fraud
In September 2020, HMRC's Chief Executive Jim Harra disclosed a working assumption within HMRC that 5-10% of Coronavirus Job Retention Scheme (CJRS) payments were claimed fraudulently. A firm has committed furlough fraud if:

- It furloughs employees but requires them to keep working
- It does not tell the workers that they have been furloughed
- It claims compensation for workers who do not currently work for them
- The firm claims more money than it is entitled to

Authorities are cracking down on furlough fraud with investigations, hefty fines and in extreme cases prison sentences. HMRC recently released recommendations for reforms to the Finance Bill 2020 which if approved by Parliament, would grant the ability to hold directors directly accountable for tax charges if they have knowingly broken CJRS rules.

Many firms are victims of genuine error when claiming furlough reimbursement, but HMRC doesn't discriminate. An investigation for CJRS fraud is a nightmare scenario for any business owner.

To avoid this scenario, firms should regularly audit their COVID compliance.

If you suspect compliance errors have occurred, consider a more forensic investigation, such as reviewing internal communications.

Eat Out to Help Out Fraud
Some eateries abused the "*Eat Out to Help Out*" scheme by submitting claims for takeaway and delivery food and alcoholic beverages that were not eligible for reimbursement. Misuse of the scheme can lead to criminal investigations including fraud by false representation, false accounting and conspiracy to defraud.

The government issued guidance on 2nd November for businesses seeking to repay wrongly claimed funds with a strict notification period of 90 days after receiving the unentitled payment.

There are around 4,000 restaurants facing potential probes by the HMRC and honest errors can and will occur, so eateries and their accountants should be sure to double-check their compliance before the grace period ends.

Scam Calls, Texts and Websites
Phishing scams/frauds have developed over the past year to take advantage of the governments use of texting to deliver official coronavirus alerts.

Fraudsters pretending to be from the government, GPs and the NHS have used calls, texts and fake websites to scam people out of their personal info and bank details.

Some frauds are obvious, while others convincingly mimic official UK Gov messages to direct marks to fake gov.uk and NHS sites which request their personal data.

Most recently, fraudsters have begun sending fake calls to register to get vaccinated. Employers can keep their employees safe and fight scammers by making them aware of phishing scams.

If you or your employee receives a suspicious call or text it should be reported to Action Fraud by calling 0300 123 2040 for investigation.

Official UK_Gov message

Fake NHS message

- The NHS will never ask you for your bank account or card details.
- The NHS will never ask you for your PIN or banking password.
- The NHS will never arrive unannounced at your home to administer the vaccine.

Analyst
jake.durham@tenintel.com

The working environment during COVID-19 in 2020 and into 2021 continues to change and for many, an increase in anxiety.

Our UK team has been working remotely since early March 2020, with a two week window last September, where the team enjoyed a welcome return to the office.

We regularly talk about positivity and communication during our weekly video meetings; and recently members of the team enjoyed a seminar which has prompted one of our new members of the team, **Rae Legg,** to open up about her thoughts on mental health.

Mental health in the workplace – what will really help?
Awareness and understanding of mental health have increased exponentially over the past few decades, with World Mental Health Day being celebrated every year on the 10th of October since 1992.

Despite the growing awareness, clearly there is still a stigma towards mental health in the workplace.

According to a survey conducted on 1,000 people by Aetna International in June 2020, up to a third of employees claim physical illness to take a day off work when in reality, it is stress and mental suffering that is the cause. Yet they feel compelled to conceal the true nature of their illness.

Some may view being open and honest about their mental health as a barrier preventing them from entering the workplace with people being advised by well-meaning family members not to disclose their mental illnesses to potential new employers.

As someone who has suffered with depression and anxiety for several years, I will freely admit to all of the above.

This begs the following question:

What steps can be taken to reduce the stigma towards mental health in the workplace?

Speak openly about mental health:
Often, people with social anxiety disorders (or people who are naturally more introverted) will feel reluctant to talk about themselves and their problems and simply encouraging them to speak out will not suffice.

Speaking candidly and openly about mental health will create a safe environment for people with mental illnesses and will make them feel secure enough to come forward and share their experiences.

This can be done by sharing and discussing articles or TV programmes that deal with mental health, supporting mental health charities, or even discussing past experiences.

Promote a healthy work/life balance:
I was told recently that people should invest more in their hobbies and interests and engage in more physical activity in order to maintain a healthy mental wellbeing.

This is sound advice, but let's look at the reality where people skip lunch breaks and work overtime, where people have long commutes to work, where people go home to their families and resume the full time role of parenting.

The simple fact is that if you don't have more time at home, you won't have time to engage in the things you enjoy.

This can be changed by encouraging people to take mental health days and to take regular holidays in order to build a fulfilling life outside of work.

Provide access to mental health facilities:
Individuals suffering with mental illnesses often talk about feeling lost and not knowing where to turn.

Other people without a history of mental illness may begin to suffer from stress due to smaller difficulties, such as moving to a new house or dealing with divorce proceedings but will downplay their issues.

By providing access to mental health screening tools and counsellors, this will encourage those suffering to take the first step and seek the help they need; whether that be a safe place to discuss their depression, or someone to vent to about the stresses of everyday life.

The above steps are just the beginning to designing a mentally healthy workspace for employees and with time and work, the discussion of mental health will no longer feel like a taboo subject.

Analyst
rachael.legg@tenintel.com

www.tenintel.com
+44 (0) 20 3963 1930
+971 (0) 4321 1210

Data breach incidents and response planning: Our Ten Point Guide for preparing and responding for a breach incident:

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data".

This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. Senior Compliance Executive, **Heba Mostafa** reports.

Examples of personal data breaches provided by the Information Commissioner's Office ("ICO") can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- e-devices containing personal data being lost or stolen
- alteration of personal data without permission; and
- loss of availability of personal data.

In the event of a data breach, GDPR gives regulatory bodies (the ICO in the UK's case) the right to fine organisations four percent of their annual global turnover, or €20m, whichever is the greatest.

A key point is that any organisation should test various scenarios periodically to ensure that the response is rehearsed and roles are known.

1. Responsibilities should be defined to key individuals (the response team) along with contact details.

The response team may include the head of IT, information security, head of corporate communications and senior executives.

2. The internal escalation process for incident responses should be documented and tested periodically. It may be that other bodies need to be notified depending on the industry in which the organisation operates.

3. Robust breach detection, investigation and internal reporting procedures should be in place. This will facilitate decision-making about whether or not the organisation needs to notify the relevant supervisory authority and the affected individuals.

4. You need to run incident risk assessment to decide if the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

For example, if the data is encrypted and there is no way any personal information can be picked up from it, you do not need to let the ICO know. It's worth noting though that the ICO recommends that if it is decided you don't need to report it, you need to be able to justify the decision, and so you should document it.

5. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedom; you need to notify the ICO (or the supervisory authority in your jurisdiction if outside the UK) without what is termed "undue delay".

This means that, from the time that you become aware of the data breach, you have a maximum of 72 hours to report it, and really should do so as soon as you know about it.

6. Working on the basis that the worst happens and reporting to the ICO is necessary. You will need to provide them with as much of the following information as possible:

- The categories and approximate number of individuals and personal data records involved
- The name and contact details of the data protection officer (if you have one) or another contact point where they can get more information
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or you plan to take, to deal with the breach, including any measures taken to alleviate the effects

7. In the case of a severe data breach, you will also need to inform anybody whose data has been caught up in the breach "without undue delay". When communicating with these individuals, you will need to let them know:

- The name and contact details of your data protection officer (as above, if you don't have one, a contact where information can be requested)
- A description of the likely consequences of the breach
- A description of the measures taken, or you plan to take, to deal with the breach, including any measures taken to alleviate the effects.

8. Work to prevent any further breach and stop the current breach (if it's on-going) and mitigate the damage that the breach, and any leaked data, can cause.

9. Giving instructions to isolate the affected systems and devices. These may be needed for any subsequent investigation. Bear in mind that closing down or isolating a system could have a huge impact on the organisation.

10. A record of any personal data breaches must be kept, regardless of whether you are required to notify.

How are personal data breaches discovered?

Data breaches are often discovered through several different channels, such as:

- Automated system monitoring - detecting a potential data breach; this is usually reviewed manually prior to action being taken.
- Whistleblowing facilities for groups such as staff, customers, and suppliers to report concerns anonymously.
- End users may report breaches to the IT helpdesk, however be aware that issues reported in this way may not be logged as breaches. To report incidents, staff need to be aware of the process.
- Data published by hackers, or when members of the public find IT equipment and report it to news outlets.
- When an incident comes to light, the actual report of the breach itself may contain sensitive and/or personal data which should be subject to the organisation's information classification policy and protected appropriately.

Senior Compliance Executive
heba.mostafa@tenintel.com

What are the 6 most commonly discussed data privacy regulations and how do they affect the way the world approaches data governance?

The EU and UK:
General Data Protection Regulation ("GDPR")
EU law on data protection and privacy in the European Union and the European Economic Area.

The USA:
California Consumer Privacy Act ("CCPA")
State statute intended to enhance privacy rights and consumer protection for residents of California, United States.

Health Insurance Portability and Accountability Act ("HIPAA")
Stipulate how personally identifiable information maintained by the healthcare and healthcare insurance industries in United States.

In Brazil:
Lei Geral de Proteção de Dados Pessoais ("LGPD")
Applies to any business or organisation that processes the personal data of people in Brazil.

In Canada:
Personal Information Protection and Electronic Documents Act ("PIPEDA")
Governs how organisations collect, use and disclose personal information in the course of commercial business in Canada.

In Dubai, UAE:
Data Protection Law ("DPL")
Gives individuals control over their personal data and protects against its misuse in both public and private sectors in the Dubai International Financial Centre (DIFC).

TenIntelligence can help support organisations with investigating a data breach:

- Advise on developing procedures to effectively **detect, report and investigate** a personal data breach or incident. Under GDPR, failure to report a breach could result in a fine.
- As an **appointed DPO**, act as the incident responder working with those identified within the Breach & Incident Response Plan.
- Develop a **communication** plan for internal and external messaging to clients and staff.
- Design and develop a **Breach & Incident Response Plan**.
- Support the regular testing regime of breach and incident response including specific development of **bespoke desk-top and play book exercises** to test decision-making procedures.
- Provide support to the appointed nominated DPO or business lead in the **incident response** critical hours.
- Conduct specific **Data Flow assessments** providing Gap Analysis to identify control weakness, strengths and areas for development

Top Ten updates you may have missed:

#1 EU-UK transition period:
The EU-UK trade agreement was reached on 24th December 2020 and data protection provisions have been temporarily extended for a 6 month period. This means organisations need to consider international transfers of personal data and to plan for minimal interruption to their business.

If you have issues or concerns relating to dataflow, data inventory or third party data sharing please contact us if you need help sorting out data transfers.

Last month, the Government announced that the Treaty agreed with the EU will allow personal data to flow freely from the EU (and EEA) to the UK until adequacy decisions have been adopted, for no more than six months. This will enable businesses and public bodies across all sectors to continue to freely receive data from the EU (and EEA), including law enforcement agencies.

As a sensible precaution, we recommend businesses work with the EU and EEA organisations that transfer personal data to them to put in place alternative transfer mechanisms, safeguarding against any interruption to the free flow of EU to UK personal data.

#2 Latest fines by the UK's ICO (Information Commissioner's Office):
The ICO fined Marriott International Inc £18.4million for failing to keep millions of customers' personal data secure. The Marriott group estimates that 339 million guest records worldwide were affected following a cyber-attack in 2014 on Starwood Hotels and Resorts Worldwide Inc.

The attack, from an unknown source, remained undetected until September 2018, by which time the Starwood Hotels had been acquired by Marriott.

On 29 Oct 2020, the ICO has fined Reliance Advisory Limited ("RAL") £250,000 for breaking electronic marketing law. The ICO found that over a six month period from the start of 2019, the Bury based company RAL made 15.1million calls in relation to claims management services such as mis-sold PPI.

All of the calls, of which 1.1 million connected, were made to people who had not consented to receive them.

The ICO fined British Airways ("BA") £20m for failing to protect the personal and financial details of more than 400,000 of its customers. An ICO investigation found the airline was processing a significant amount of personal data without adequate security measures in place. This failure broke data protection law and, subsequently, BA was the subject of a cyber-attack during 2018, which it did not detect for more than two months.

#3 Fraud now accounts for one-in-three crimes in the UK:
A report by ex-Metropolitan Police Deputy Commissioner Sir Craig Mackey, found that fraud now accounts for one-in-three crimes in the UK. It is estimated that 86% of fraud is committed online, permitting fraudsters to operate from anywhere in the world.

London sees the greatest concentration of fraud cases. Throughout 2019, the Metropolitan Police investigated more than 8,000 cases of fraud, compared to the 1,600 by Greater Manchester Police.

#4 Banking Fraud reports:
TSB Bank have reported that in H1 of this year, £582.2m has been lost to bank fraud. Of this figure, £207.8m was a result of "Authorised Push Payment" fraud, where victims are tricked into making large bank transfers to an account posing as a legitimate payee. TSB Bank believes that reporting only stands at 25% and the problem is likely to significantly larger than previously reported. The pandemic has seen an increase in internet banking, which has created more targets for the fraudsters.

#5 Deepfake Fraud:
Additionally, new fraud trends using artificial intelligence have been observed, namely "deepfake" fraud. A deepfake is a video or audio clip where someone's face or voice has been replaced with another person's likeness using Artificial Intelligence.

Last year, the CEO of a UK energy firm followed directions given over the phone by the chief executive of the firm's parent company to transfer €220,000 to one of their suppliers. However, it was not the parent company's CEO speaking, instead it was a convincing example of voice cloning. According to the victim, the voice was indiscernible from the real thing, and he only caught on due to certain inconsistencies including the phone number being Austrian when it should have been German.

Deepfakes can be used for new account opening fraud or account takeover fraud. Security practices to protect from deepfakes:

- Trust but verify, call back on a number you know to be correct
- Consider the source
- Look for inconsistencies, check the phone number, email, or account the audio or video came from
- Limit access to your voice and images, fraudsters need recordings, images or footage of you to create deepfakes.

Top Ten updates you may have missed:

#6 The Office of Financial Sanctions Implementation (OFSI)
Since the EU-UK transition period ended on December 31st 2020, the UK will no longer apply EU sanctions regulations and all sanctions regimes will be implemented through UK regulations.

The Sanctions and Anti-Money Laundering Act 2018 (the Sanctions Act) provides the legal framework for the UK to impose, update and lift sanctions autonomously.

The Foreign, Commonwealth and Development Office (FCDO), which determines international sanctions policy in the UK, has already implemented regulations for over 30 sanctions regimes in preparation for the transition.

Office of Financial Sanctions Implementation
HM Treasury

Organisations should check the new legislation to ensure that their activities are still compliant. A list of the UK regimes, legislation and guidance already made in preparation for the end of the transition period is available on FCDO's website.

#7 H&M handed GDPR fine of 35M Euro
On 1 October 2020, the German State Commissioner for Data Protection and Freedom of Information (Landesbeauftragte für Datenschutz und Informationsfreiheit) of Hamburg (the DPA) imposed a fine of EUR 35.3 million under the GDPR against the German subsidiary of the fashion retailer H&M.

The DPA found that the company had collected extensive records relating to the private lives of several hundred employees, which included health data and sensitive data. The DPA also expressed concerns over personal data collected in relation to so-called "Welcome Back Talks" which followed an employee's leave of absence.

The records of these talks included not only the employees' vacation experiences, but also symptoms of illness and diagnoses. In addition, some supervisors recorded other private information such as family problems and religious beliefs.

#8 Irish Organisations Online Cookie Compliance
Organisations in Ireland had until 5 October to update their online cookie compliance and there are significant penalties for non-compliance under GDPR legislation.

ACOI

This is the advice of the Association of Compliance Officers Ireland ("ACOI") who say that implementation of the Data Protection Commission's (DPC) guidance has significant implications for Irish organisations, particularly those SMEs whose resources may be already fully focused on surviving Covid-19 and preparing for Brexit.

The ACOI advise that all organisations should give high priority to this issue for the remainder of this year.

#9 Egypt introduces new Data Protection Law
After several years of debate, the Egyptian government has introduced the Republic's first standalone data protection law, which aims to regulate and protect citizens' data online.

On 15 July 2020, Resolution No. 151 of 2020 (the Law) was published in the Official Gazette. The provisions under the new Law are modelled on GDPR and the Law adopts similar concepts and definitions.

It is hoped that the new Law will help Egypt attract foreign investment by increasing consumer confidence in electronic data processing and setting clear parameters for companies looking to capitalise on the growth of the digital economy.

The Law will enter into force three months from when it was published in the Official Gazette.

#10 Zimbabwe to amend its cyber security and data protection laws
Debates in the Zimbabwean Nation Assembly last week led to amendments in certain clauses of their Cybersecurity and Data Protection Bill. The clauses in question are 13, 17, 23, and 164.

Clause 164 suggests a criminal lawsuit against any person who sends data messages which have the potential to provoke or incite violence and damage to property.

The reprimand would be a monetary fine, or imprisonment of up to 5 years.

News from our Dubai Team

Dubai Police seize £1.7 billion worth of counterfeit products in 5 years. A success story that our Dubai team has had a big influence

The Department of Anti-Economic Crime at Dubai Police arrested 2,430 accused and recorded 2,145 economic crime cases over the past five years.

The Department has also made confiscations with an estimated value exceeding Dhs8.9 billion.

Brigadier Jamal Salem Al-Jalaf, Director of the of Criminal Investigations Department ("CID") stated; "Dubai Police are keen to arrest those involved in economic crimes through a precise action plan in coordination with trademark partners" adding that; "regular meetings are held between brands' representatives and officers of the Department of Anti-Economic Crime to explore methods and tools to uncover counterfeit goods."

Our team in Dubai continually provides online training to the Dubai Police, and more recently the Ajman Department Economic Development back in November, on how to differentiate between counterfeit and genuine products.

Despite what the COVID-19 pandemic restrictions present, TenIntelligence continues to carry out enforcements along side the UAE Law Enforcement Authorities (CID, DED and Customs) for counterfeit products.

In 2020, our team were able to apply and attend the destruction of approximately 135,313 products.

Furthermore, in collaboration with the Dubai CID and Dubai Customs the team have been able to seize a total of 9,036 counterfeit products (electronics and clothing) since October 2020.

Email: dubai@tenintel.com

Contact TenIntelligence | www.tenintel.com

If you have been affected by any of our insights in this edition, please **contact us** and we can help guide you through any fraud, compliance, investigation, cyber or regulatory due diligence requirements you may have.

- Director Due Diligence
- Virtual Data Protection Officer
- Cyber-Crime Investigations
- Enhanced Due Diligence
- Data Protection Audit & Assessment
- Penetration Testing
- Forensic Intelligence
- Breach & Incident Response
- Brand Protection
- Financial Crime Compliance
- Background Checks
- Regulatory Compliance
- Anti-Corruption
- Intellectual Property Infringements

Email us | info@tenintel.com
UK +44 (0) 203 963 1930 | UAE +971 4321 1210

United Arab Emirates | Brand Protection Services

Our brand protection services help clients identify whether their products are being counterfeited.

Firstly, trade mark infringements are serious Intellectual Property crimes. Secondly, they threaten the health and safety of consumers and violate the rights of trademark, patent, and copyright owners.

Food products, electronic goods, toys, software, luxury items, car and aircraft parts are being manufactured and maintained with substandard or counterfeit parts.

This continues to be a huge risk to consumers and the brand owners' reputation.

Our team helps brand owners gather the evidence required to produce prosecution packages for civil and criminal proceedings.

Our services cover on the ground enforcements in the UAE and investigations across the Middle East, including; Bahrain, Iraq, Kuwait, Oman and Saudi Arabia.

https://www.tenintel.com/brand-protection/

Our Services

Due Diligence	Investigations	Protection
Assurance	Corporate Fraud	Brand Protection
Financial Crime Compliance	Litigation Support	Cyber Security
Strategic Intelligence	Digital Forensics	Data & Privacy Advisory

@tenintelligence

London | Moorgate	Kent | Kings Hill	Dubai | Sheik Zayed Road
+44 203 963 1930	+44 173 252 5810	+971 (0) 4321 1210
info@tenintel.com	info@tenintel.com	dubai@tenintel.com