TenInsight

TenIntelligence

www.tenintel.com | October 2017 | Issue 1

Insight from the top

The regulatory and political landscape is changing. Political uncertainty, Brexit and terrorism are at the top of business agendas. These are important and companies should be implementing contingency measures, yet still be aware of the hidden risks, such as fraud, financial crime and cyber security.

These are often thought of as "victimless" crimes; but all are on the increase. The Institute of Directors (IoD) recently produced a policy report around cyber security stating 95% of directors considered this "very" or "quite" important to their business, and yet 45% do not have a formal cyber security strategy.

Recent research by ISP company Beaming showed a staggering 52% of British businesses fell victim to some form of cyber crime in 2016. That's 2.9 million companies across the UK at a cost of £29.1 billion. It's time to place cyber security on your immediate agenda.

It is impossible to predict or calculate the true cost of fraud or its financial impact as much goes undetected and unreported. Fraud is a significant threat to businesses, not just the cost, but understanding the impact it might have.

The Association of Certified Fraud Examiners (ACFE), the globally recognised authority on fraud, publishes its annual survey, Report to the Nations. In their 2016 report, the median estimate of what fraud could cost an organisation was five per cent of yearly turnover. This is based upon known frauds reported by its members.

What would this loss of revenue do for your business? What could you achieve with an additional five per cent on your turnover? Report to the Nations estimated the most common detection method (39.1%) was a tip off.

My advice is: do what you can to protect your company from internal and external perpetrators. Review your financial controls, educate employees and consider due diligence on vendors.

Neil Miller
CEO, Ten Intelligence Limited

The new Money Laundering Regulations are here

Businesses need to be aware of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("MLR 2017"), which came into force on 26 June 2017.

Broadly speaking, this introduces a greater emphasis on risk assessments and an enhanced risk-based approach in respect of anti-money laundering/counter-terrorism financing (AML/CTF) compliance programmes. **Sonel Martin** highlights some of the changes:

• MLR 2017 does away with "automatic" simplified due diligence (SDD) categories. Instead, each business area or function – as well as individual relationships and transactions – requires a risk assessment to decide whether a lower degree of risk exists and SDD can be applied. This should take into account a list of specific risk factors referred to in the MLR 2017.

• Enhanced due diligence (EDD) is required in respect of PEPs, correspondents, larger or complex transactions, as well as transactions with unusual patterns. More generally, EDD has to be applied in any case where there exists a higher risk of money laundering. Again, MLR 2017 refers to a list of high risk factors that should be considered.

• The definition of politically exposed persons (PEPs) for AML requirements is extended to include domestic PEPs, "members of the governing bodies of political parties" as well as "directors, deputy directors and members of the board or equivalent function of an international organisation".

This substantially broadens EDD's scope. Where a person ceases to be a PEP, entities should continue to monitor the risk they pose for at least another 12-months.

• The threshold for customer due diligence (CDD) in respect of cash transactions has been reduced to €10,000.

• Under MLR 2017, estate agents are required to conduct CDD on the purchaser and the seller.

• A new blacklist of high-risk jurisdictions is to be published from time to time. Any transactions or business relationships in such jurisdictions will require EDD.

Application of AML/CTF requirements will clearly demand more than a tick box approach; focused risk assessments and comprehensive due diligence, supported by documented evidence, in respect of individual business relationships, customers and third parties will be essential to avoid potential personal liability.

More changes to the UK financial crime regime

The Criminal Finances Act 2017 (CFA) came into force on 30 September 2017. It introduces further changes to the UK financial crime regime that may necessitate a review of businesses' existing compliance programmes and financial crime controls. Proper and comprehensive risk assessments will be key.

One of the main measures is the introduction of criminal corporate offences, where a company (or partnership) fails to prevent the facilitation of tax evasion by "associated persons" (including employees and global contractors). Currently, where an employee of a company facilitates the evasion of tax by a customer, both the employee and customer will be committing an offence, but not necessarily the company.

The company or partnership will, however, have a defence if it can show that it had "reasonable procedures" in place to prevent the facilitation of tax evasion. The Government is to issue final guidance in this regard. Companies need to consider their current processes and procedures in light of these changes, as well as the guidance, to ensure compliance and avoidance of strict liability under the proposed new offences. Contravention of the CFA will be punishable by unlimited fines.

The CFA will also make it possible for the suspicious activity reports (SARs) moratorium period under the Proceeds of Crime Act to be extended by further periods of 31 days, up to a maximum of 186 days. This may prove challenging to firms managing customer relationships during such extension periods without falling foul of the tipping off provisions.

Other changes proposed by the CFA include:

- Unexplained Wealth Orders will enable law enforcement agencies to obtain court orders to require individuals who are suspected of being linked to serious crime and whose assets are disproportionate to their known income, to explain the source of their wealth. Failure to do so could result in such assets being treated as "recoverable property" under the Proceeds of Crime Act.
- Enforcement agencies' existing rights to obtain Disclosure Orders in fraud and corruption investigations will be extended to AML investigations and will be afforded to a wider range of agencies.
- Regulated firms will be able to share information about specific suspicious activities and lodge joint SARs.
- Law enforcement agencies will be given enhanced powers to seize and forfeit property and assets in the UK and obtain freezing orders over bank accounts where there is a reasonable suspicion they represent or hold proceeds of crime.

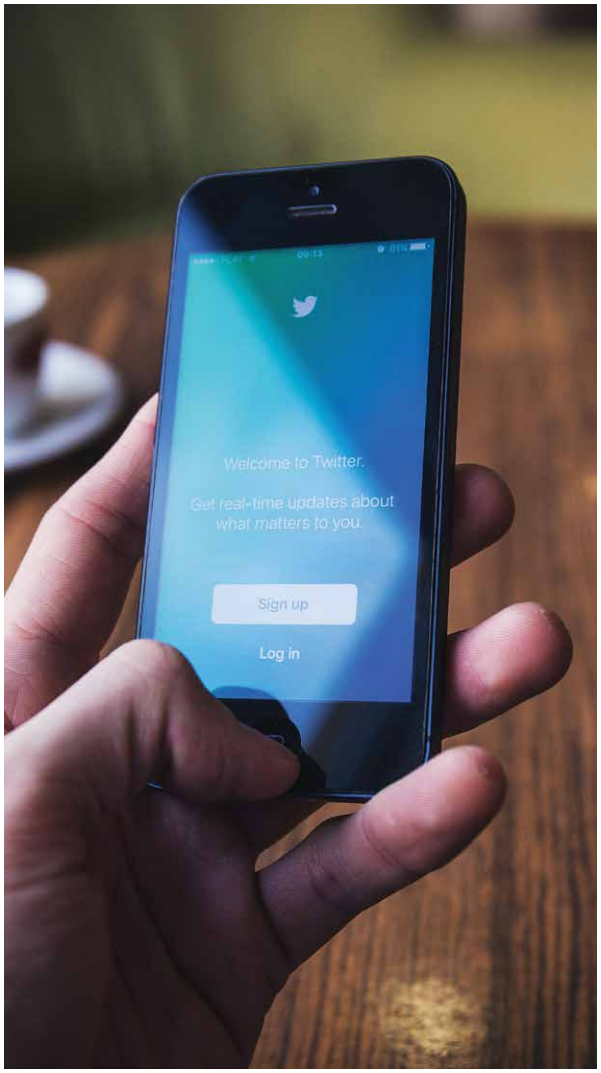
Through these changes the Government is trying to send a clear message "we will not stand for money laundering or the funding of terrorism through the UK". At what cost and burden this will come to businesses in practical terms, remains to be seen.

The cost of organised crime

- **£24bn – estimated cost of serious and organised crime in the UK per year**
- **£36-90bn – estimated range of money laundered in the UK per year**
- **€110bn – estimated income generated by illicit markets in the EU**
- **404,735 – number of SARs received by the NCA as per its 2015/2016 annual report and accounts**
- **£5bn – estimated cost members of the British Bankers' Association spend annually on their financial crime compliance programmes.**
- **£255m – the amount recovered from criminals by the UK government in 2015/2016**

Social media and pre-employment screening

Social media searches often highlight potential issues and suitability risks not evident from a candidate's CV.



Social media due diligence could assist companies to identify adverse or negative content in respect of prospective employees. This could not only spare potential embarrassment and reputational risk, but also save costs, time and effort of appointing someone who may need replacing shortly after.

Social media searches involve the scanning of an individual's online profiles *(Facebook, Twitter, Instagram, LinkedIn etc)* as well as media and web blogs to identify any potentially adverse content or references.

Sometimes these searches may be limited due to the individual's privacy settings; however, even comments made on blogs and websites leave a footprint and can potentially be identified.

We were recently instructed by an international client to conduct due diligence on an individual, Mr J, who was proposed to be appointed to the Board of a public listed company. On his disclosure form Mr J stated he was a director of a construction company. However, searches of his Facebook and Twitter account identified links to a support group for a prominent controversial political figure, Mr. P.

Further investigation identified an alias for Mr J that led our investigators to the discovery he was in actual fact the head of security of Mr P, his so-called association with the construction company merely being a smoke screen.

No PEP list contained any reference to Mr J's political connection to Mr P. If it wasn't for the enhanced due diligence into Mr J's social media profile, this would not have been discovered.

Social media searches need to be conducted with care and with regard to an individual's privacy. However, information obtained from these searches could be instrumental in deciding whether a candidate poses any risk to your company's internal operation or external reputation.

In other news…

- According to Cifas, the leading UK fraud prevention service, 172,919 identity frauds were recorded in 2016 – the highest number on record. Eighty-eight per cent of these frauds were perpetrated online.
- Spanish prosecutors recently secured their first bribery convictions, regarded by many as a watershed moment. The case involved two executives of a Spanish publishing company who bribed a minister from Equatorial Guinea to secure contracts with the government. The company was not a party to these proceedings as the conduct of the executives occurred prior to 2010, when corporate criminal liability was introduced in Spain. However, it is believed prosecutors will next set their sights on the prosecution of a company. It is vital that businesses with a presence in Spain ensure they have suitable compliance programmes.
- This February, the Trump administration repealed the "Cardin-Lugar regulations", previously regarded as a crucial anti-corruption rule for oil, gas and mining companies. These regulations were due to come into force in 2018 and would have required US listed companies in the mining sector to disclose certain expenditure, costs and payments made in respect of or to foreign governments relating to extractive projects. The main aim of this was to curb corruption, bribery and illicit payments, specifically in developing countries. Going forward, US companies will still need to adhere to the US FCPA, but they will not be required to make any expenditure or payment information public. There is concern this u-turn could put US companies in the natural resources sector at an advantage compared to companies subject to more strict transparency and reporting rules in the UK, EU and Canada.

Bitcoin and the regulation of digital currency

Despite strong debate over the regulation of digital currency, Bitcoin users and governments agree consumer protection is important. In the UK, the FCA is yet to produce a full regulatory framework for Bitcoin, but profits and losses are taxable.

The FCA is working with Bitcoin start-ups in the UK to develop a 'regulatory sandbox'. This would act as a voluntary framework of best practice standards to protect consumers, and stabilise prices, writes **Thomas Hughes**.

Calls for further regulation are generally focussed around three main issues: volatility; anonymity and exploitation; and inclusion.

Bitcoin is a volatile currency. Most major currencies average between 0.5 and one per cent. According to the Bitcoin Volatility Index, Bitcoin was almost five per cent in March 2017. While proponents believe regulation would help steady the price, critics claim the volatility will be comparable to major currencies by 2019. They argue that while prices may have gone up, volatility is decreasing.

As disclosing your identity to use Bitcoin is not necessary, fears of criminal exploitation and money laundering have led to strong calls for increased regulation. Indeed, the EU published draft legislation on 9 March, that would allow financial intelligence units to collect and store identifying data on digital currency users.

Privacy rights activists oppose this action, arguing money laundering and criminal activity are discouraged by the open, transparent nature of the blockchain.

Proponents of regulation argue the reason banks and other major financial institutions have thus far rejected the inclusion of Bitcoin is due to a lack of regulation.

Critics claim the banks will never accept cryptocurrency, as the peer-to-peer nature of the network only makes banks more obsolete.

The future of Bitcoin will certainly include some form of loose regulation. However, if financial authorities push too hard, they could see Bitcoin trading fall further into the dark web and into the hands of criminal enterprise, simultaneously losing the incredible potential this technology holds.

Bitcoin – the Basics:

- **Bitcoin** is a form of digital currency. It is exclusively electronic.
- Unlike traditional currency, the value of Bitcoin is not based on a tangible commodity, like **gold or silver**. Rather, Bitcoin derives its value from the **consensus** of its users.
- When Bitcoins are traded, records of the transaction, including the **sender, recipient, date and time** are saved into part of a **block**.
- A block is a file which holds the records of recent transactions, and a link to the previous block. The entire history of trades of Bitcoin is **open** to all users of the Bitcoin network. This history is called the **blockchain**. This stops a user trading the same Bitcoin multiple times. Every user is aware who controls which Bitcoins.
- Bitcoins are created digitally, in a process known as **mining**. Solving complex mathematical problems allows miners to **complete** a block by adding it to the blockchain and linking it to the **next** block. Miners receive their own Bitcoin as a **reward** for adding to the blockchain. In this way, a **continuous history** of all Bitcoin transactions is available to all users on the network, which allows for the **verification** and **trust** which is behind the value of Bitcoin.
- Bitcoin is **anonymous**. Anyone can have as many accounts as they wish, and accounts are not linked to real identities or addresses.
- Bitcoin is **decentralised**. There is no 'Bank of Bitcoin' to control production or monetary policy.
- There is a **limited supply** of Bitcoins. The difficulty of the problems miners must solve to complete blocks automatically changes to maintain the **steady production** of bitcoins. The ideal average mining time is **10 minutes per block**.

Contact Us

UK
+44 (0)20 3102 7720
info@tenintel.com

MIDDLE EAST
+971 (0) 4333 4669
dubai@tenintel.com

@tenintelligence