McDermott Will & Emery

NORTON ROSE FULBRIGHT

WSBA | WALL STREET BLOCKCHAIN ALLIANCE

CRYPTOCURRENCY GLOBAL TAX ENFORCEMENT: WHAT INVESTORS AND COMPANIES IN THE INDUSTRY NEED TO KNOW NOW

June 28, 2021

mwe.com

SPEAKERS

Gary Alford
Supervisory Special Agent
IRS-CI

Mayling Blanco
Partner
Norton Rose Fulbright

Perry Carbone
Chief of the White Plains Office
US Attorney's Office for the SDNY

Andy Cole CBE
Former Director of Specialist Investigations
HM Revenue & Customs

Simon Airey
Partner
McDermott Will & Emery
sairey@mwe.com

Andrea Kramer
Partner
McDermott Will & Emery
akramer@mwe.com

Carlos Ortiz
Partner
McDermott Will & Emery
cortiz@mwe.com

Kevin Spencer
Partner
McDermott Will & Emery
kspencer@mwe.com

AGENDA

- Global Enforcement
- Tax Guidance
- DOJ Update: Corporate Compliance
- The UK Criminal Finances Act 2017
- Summary & Conclusions

GLOBAL ENFORCEMENT

IRS ENFORCEMENT - 2021

- **Operation Hidden Treasure**
  - In early March, the Director of the Office of Fraud Enforcement for the IRS announced certain fraud enforcement priorities, including a dedicated team of IRS Criminal Investigation professionals working on “Operation Hidden Treasure”
  - Focused on cryptocurrency and taxpayers who omit cryptocurrency income from their tax returns
  - Compromised of agents specially trained in cryptocurrency and virtual currency tracking
  - Joint partnership between the civil office of fraud enforcement and the criminal investigation unit to “root out” tax evasion from cryptocurrency owners

IRS ENFORCEMENT - 2021

- **Finding John Doe**
  - Issued two John Doe summonses in order to obtain information on cryptocurrency holders. IRS successfully defended court challenges
    - In the Northern District of California, the IRS won an order authorizing a John Doe summons on popular cryptocurrency exchange, Kraken
    - In the District of Massachusetts, the IRS secured another order against Poloniex
  - IRS also defeats court challenge to use information obtained by summons
  - These victories, coupled with the IRS' increased knowledge of virtual currency transactions, are big steps in its efforts to, as stated in the IRS' court filing, "root out tax noncompliance"

IRS ENFORCEMENT - 2021

- **Finding John Doe – The *Kraken* Response**
  - Government required to file a response explaining its need for the information requested in the summons. The response provided numerous examples of how the data received in the Coinbase summons required additional requests in order to locate actual taxpayers
  - Detailed how information, such as accountholder telephone numbers and email addresses, will facilitate the IRS's ability to utilize relevant cryptocurrency platform data already in its possession including data from foreign-based cryptocurrency exchanges
  - Noted the potential for abuse by an accountholder by providing an example of an individual falsifying their identity as the basis for its need for complete account history in order to catch these issues
  - In addition, stated, "[m]atching the IP addresses for Kraken users to IP addresses and other data points in the IRS's information will allow the IRS to link substantive account information from multiple sources for a single individual taxpayer and make a more accurate initial determination of whether that individual is in compliance with the internal revenue laws"

IRS ENFORCEMENT – 2021 AND BEYOND…

- **Biden Administration Proposals Enhance IRS' Ability**
  - Department of the Treasury released its American Families Plan Tax Compliance Agenda, laying out tax compliance measures. The report sets forth a number of initiatives designed to "close the tax gap," identify the underreporting of tax liabilities and detect tax evasion. These measures, which are part of an $80 billion proposal for the IRS, would significantly enhance the agencies' ability to address the challenges involved with finding taxes that result from virtual currency transactions
  - The Treasury's report notes that "[c]ryptocurrency already poses a significant detection problem by facilitating illegal activity broadly including tax evasion." To address this issue, the Biden Administration is proposing "additional resources for the IRS to address the growth of cryptoassets"

IRS ENFORCEMENT – 2021 AND BEYOND…

- **Biden Administration Proposals Enhance IRS' Ability**
  - Most notably, the Biden Administration is proposing enhanced reporting requirements for domestic and foreign financial accounts that specifically address cryptocurrency. Financial institutions, including "cryptoasset exchange accounts and payment service accounts that accept cryptocurrencies" would be required to submit third-party annual reports of all "gross inflows and outflows" from business and personal accounts to the IRS using a form similar to the IRS 1099-INT
  - Additionally, "businesses that receive cryptoassets with a fair market value of more than $10,000 would be reported on" in a manner similar to how cash transactions are reported on Currency Transaction Reports. These new reporting requirements would dramatically increase the IRS' ability to identify and detect unreported cryptocurrency transactions

OFF SHORE ENFORCEMENT – J5

- June 2019, the Joint Chiefs of Global Tax Enforcement (known as the “J5”) met in Washington to commemorate its one-year anniversary and announce its first year results
- The J5 consists of the leaders of the tax enforcement agencies in Australia, Canada, the Netherlands, England, and the United States
- The J5 was formed to collaborate on the investigating and combating of cross-border tax and money laundering threats, including cybercrime, cryptocurrency, and enablers of global tax crimes
- The J5 is currently investigating more than 50 entities for international tax evasion. These entities were previously thought to be beyond the reach of the J5. Besides exchanging unparalleled amounts of information, the J5 is also actively cooperating on investigating potential crimes ranging from money laundering to the smuggling of illicit commodities to personal tax frauds and evasion

OFF SHORE ENFORCEMENT – J5

- In its relatively short history, the J5 has worked on a number of high profile actions in connection with money laundering using cryptocurrencies
- Most recently, J5's investigative efforts resulted in the high profile arrest of a CEO in New York for securities fraud, money laundering, tax evasion and a number of other offenses. With respect to this case, IRS-CI Special Agent-in-Charge Larsen specifically thanked the J5 for contributing to the IRS's ability to "unravel the web of lies"
- March 25, 2021, the J5 announced its third "Challenge" – explicitly stating its regulatory enforcement focus on FinTech and cryptocurrency. This publicly reported "Challenge" is another significant step in efforts by tax authorities to bring criminal charges against those seeking to use the perceived anonymity of cryptocurrency to evade taxes

GLOBAL DEVELOPMENTS - TAX

- **2009**: compulsory disclosure notices issued to 308 UK financial institutions collected data about UK residents with offshore accounts. Followed by the *Liechtenstein Disclosure Facility* in the UK and numerous disclosure programmes around the world
- **2010**: U.S. *Foreign Account Tax Compliance Act* ("FATCA")
- **2012**: UK / Swiss Agreement - further significant voluntary disclosures of unpaid tax – significant data gathered by HMRC
- **2012**: whistle-blower Bradley Birkenfeld (UBS)
- **2013**: under new regulations in **Singapore**:
  - tax evasion designated as a money-laundering predicate offences for the purposes of suspicious activity reporting. Any bank based in Singapore that is suspected of facilitating tax evasion or having inadequate controls liable to civil fines, criminal prosecution or even loss of its licence

GLOBAL DEVELOPMENTS - TAX

- **2013** - **Switzerland** signs *Convention on Mutual Administrative Assistance in Tax Matters*
- **2014 - global** Common Reporting Standard ("**CRS**") announced - will identify the underlying "controlling person" of investment vehicles'. As well as funds, assets, income and gains, CRS will also identify the UBOs of offshore structured products, trusts, pension and insurance products
- **2015** - campaign announced in **China** to use CRS data to track down nationals with funds held offshore
- **2016** - conclusion of **US** “Swiss Bank Program”: 80 Swiss banks enter into DPAs and pay $1.4 b to IRS
- **2016**: "**Panama Papers**": 11 million records over 40 years from just one law firm - data implicates many well known people, institutions + advisers
- **2017**: “**Paradise Papers**”: are a huge leak of financial documents that throw light on the top end of the world of offshore finance. More than 1,400GB of data, containing about 13.4 million documents. Some 6 million come from an offshore law firm and a corporate services provider. A smaller amount comes from a trust company in Singapore. The leaked data covers seven decades, from 1950 to 2016
- **2017** “**FinCEN Files**”: leak of 2,500 Suspicious Activity Reports sent by banks to FinCEN in the US between 2000 and 2017

GLOBAL COMMON REPORTING STANDARD ("CRS")

- CRS is based upon **reciprocal exchange of information**, designed to prevent tax evasion relating to funds and assets concealed in other countries
- **102 countries** joined the Agreement by the end of 2018 and are committed to ensuring effective automatic exchange of information
- **First information exchange** (49 'early adopter' countries, of which the UK is one): commenced **September 2017**
- **Full exchange** (53 countries): commenced **September 2018**
- Countries that have not yet joined CRS can still supply or exchange information spontaneously or upon request

49 Countries Committed to Exchange in 2017 (“early adopters”)
Anguilla, Argentina, Belgium, Bermuda, British Virgin Islands, Bulgaria, Cayman Islands, Colombia, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Faroe Islands, Finland, France, Germany, Gibraltar, Greece, Guernsey, Hungary, Iceland, India, Ireland, Isle of Man, Italy, Jersey, Korea, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Mexico, Montserrat, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Seychelles, Slovak Republic, Slovenia, South Africa, Spain, Sweden, Turks and Caicos Islands, United Kingdom
53 Countries Committed to Exchange in 2018
Andorra, Antigua and Barbuda, Aruba, Australia, Austria, Azerbaijan, Bahrain, Barbados, The Bahamas, Belize, Brazil, Brunei Darussalam, Canada, Chile, China, Cook Islands, Costa Rica, Curaçao, Dominica, Ghana, Greenland, Grenada, Hong Kong (China), Indonesia, Israel, Japan, Kuwait, Lebanon, Marshall Islands, Macao (China), Malaysia, Mauritius, Monaco, Nauru, New Zealand, Niue, Pakistan, Panama, Qatar, Russia, Saint Kitts and Nevis, Samoa, Saint Lucia, Saint Vincent and the Grenadines, Saudi Arabia, Singapore, Saint Maarten, Switzerland, Trinidad and Tobago, Turkey, United Arab Emirates, Uruguay, Vanuatu

TAX GUIDANCE

IRS GUIDANCE

- Notice 2014-21 (March 25, 2014)
- Rev. Rul. 2019-24 addressed the tax treatment of cryptocurrency forks (October 9, 2019)
- On October 9, 2019, the IRS posted 43 questions and answers (FAQs) on cryptocurrency on its website, updated on December 31, 2019 to 45 FAQs and March 2, 2021 to 46 FAQs

TAX REPORTING CONSIDERATIONS

- 2020 Form 1040 and revised instructions (April 13, 2021)
- Form 14457, Voluntary Disclosure Practice Preclearance Request and Application
- Virtual Currency Industry Reporting
  - Brokers and barter exchanges
  - Form 1099 reporting

BIDEN ADMINISTRATION PROPOSALS

- Significantly expand information reporting for crypto exchanges
  - Gross flow of $600 (or balance of $600)
  - Report single transactions of $10,000 or more
  - Report certain beneficial owners as identified in future Treasury regulations
- Codify US participation in Common Reporting Standard (CRS) to aid enforcement and reciprocity

IRS TAX AUDITS OF CRYPTO CURRENCIES

- First question on Form 1040 after your name is:
  - "At any time during 2020, did you receive, sell, send, exchange, or otherwise acquire any financial interest in any virtual currency?"
  - IRS believes there is significant under reporting
- Numerous civil tax issues for cryptocurrency investments
  - Information reporting (i.e., did you receive a Form 1099?)
    - If not, do you still need to report?
  - Very few audits, but we expect a sharp increase in exams
  - IRS is training (and adding new) agents to identify transactions
  - Hiring third-party contractors to assist in audits and calculations
- Biden administration recently proposed new reporting regime for financial institutions, settlement entities, and digital asset exchanges to track inflow and outflows
- Expect a voluntary disclosure program for the previous tax years and compliance program for the industry to track transactions

CIVIL TAX ISSUES TO CONSIDER

- Potential civil penalties
  - Between 20-40% of the tax owed (fraud penalties are higher), plus interest
- Penalties (but not interest) can be abated based upon reasonable cause
  - Reasonable reliance in good faith of a tax professional's advice
  - But you will waive attorney-client/tax-practioner privilege
- Failure to report keeps the statute of limitations on the entire return year until reported
  - So if never report, the SOL is open forever on the return!

CRIMINAL TAX ISSUES TO CONSIDER

- Potential Criminal Charges
  - Title 26 Section 7201 – Tax evasion
  - Title 26 Sections 7206 (1) & (2) – Filing a false return & aiding and assisting the filing of a false tax returns
  - Title 26 Section 7212 (a) – Obstructing function of IRS
  - Title 18 Section 371 – Conspiracy
- Penalties
  - Individuals - 5 to 3 years prison (per count) & fines
  - Corporations – Fines, reporting requirements & monitor

PREPARATION IS YOUR BEST AUDIT DEFENSE

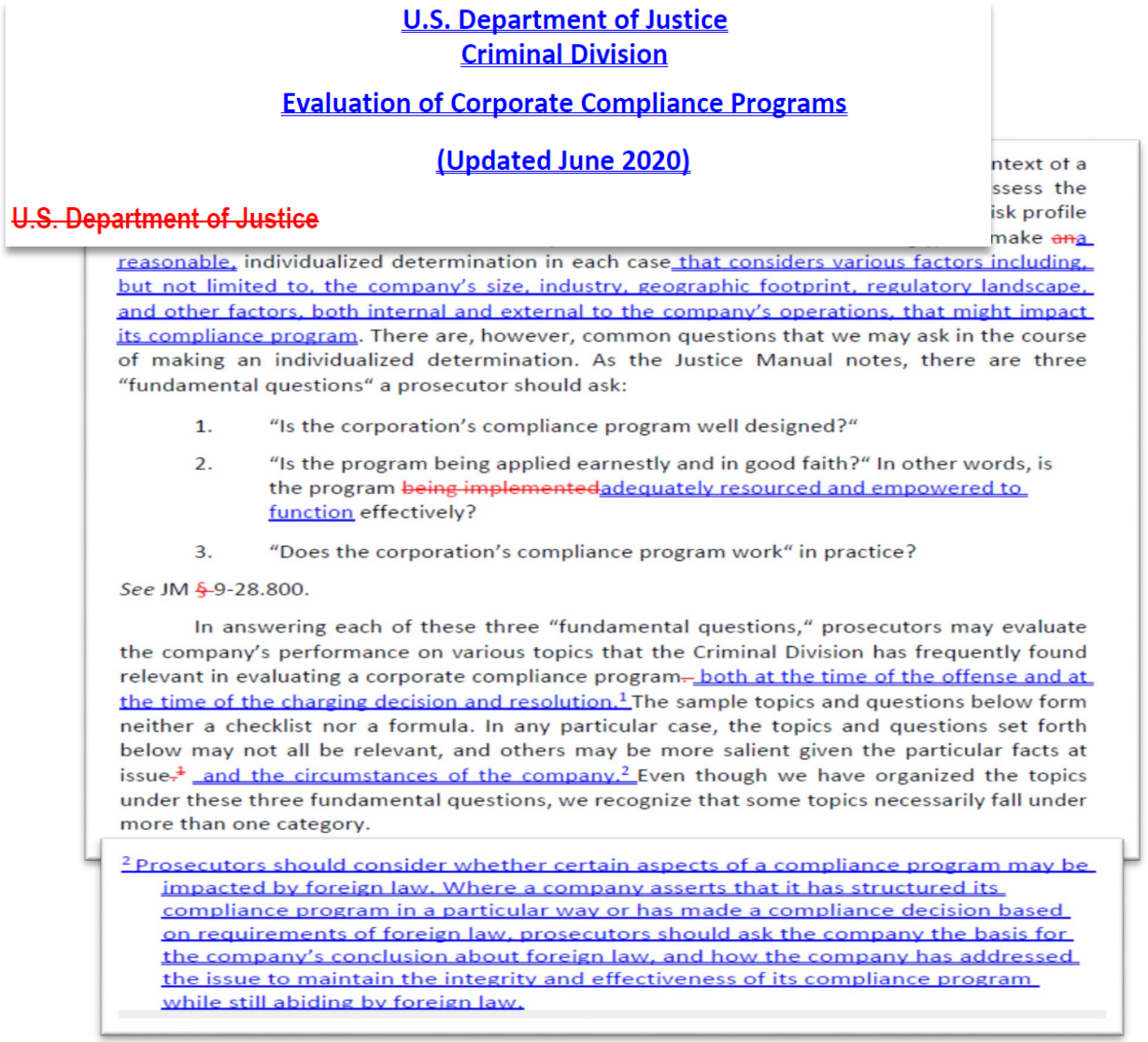
- Get good advice before you report (or not)
  - Abate any penalties that the IRS could assert
- Do you have all of your records?
  - Date and time of purchase and sale
  - Cost at purchase, plus any fees
  - FMV at sale, plus any fees
  - Any adjustments to basis
  - Hard or soft forks? Airdrops?
- Do you need to file an FBAR?
  - New rule coming

DOJ UPDATE: CORPORATE COMPLIANCE

EVALUATION OF CORPORATE COMPLIANCE PROGRAMS

Key takeaways from the updates:

- Assessing the right fit
- Resourcing and empowerment
- Continuous assessment, review, and development
- Data-driven program
- Third-party risk management



U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated June 2020)

~~U.S. Department of Justice~~

ntext of a
ssess the
isk profile
make ~~an~~a
reasonable, individualized determination in each case that considers various factors including, but not limited to, the company's size, industry, geographic footprint, regulatory landscape, and other factors, both internal and external to the company's operations, that might impact its compliance program. There are, however, common questions that we may ask in the course of making an individualized determination. As the Justice Manual notes, there are three "fundamental questions" a prosecutor should ask:

1. "Is the corporation's compliance program well designed?"
2. "Is the program being applied earnestly and in good faith?" In other words, is the program ~~being implemented~~adequately resourced and empowered to function effectively?
3. "Does the corporation's compliance program work" in practice?

See JM ~~§~~ 9-28.800.

In answering each of these three "fundamental questions," prosecutors may evaluate the company's performance on various topics that the Criminal Division has frequently found relevant in evaluating a corporate compliance program~~.~~ both at the time of the offense and at the time of the charging decision and resolution.[1] The sample topics and questions below form neither a checklist nor a formula. In any particular case, the topics and questions set forth below may not all be relevant, and others may be more salient given the particular facts at issue.~~[1]~~ and the circumstances of the company.[2] Even though we have organized the topics under these three fundamental questions, we recognize that some topics necessarily fall under more than one category.

[2] Prosecutors should consider whether certain aspects of a compliance program may be impacted by foreign law. Where a company asserts that it has structured its compliance program in a particular way or has made a compliance decision based on requirements of foreign law, prosecutors should ask the company the basis for the company's conclusion about foreign law, and how the company has addressed the issue to maintain the integrity and effectiveness of its compliance program while still abiding by foreign law.

KEY TAKEAWAYS

Continuous Assessment, Review, and Development

- Is the compliance team conducting on-going assessments of the risks posed?
- Is the compliance team monitoring the company's own conduct and that of other companies facing similar risks?
- Is the company updating policies based on data and lessons learned?
- If misconduct is uncovered, what is done to address the lapse?
- Is the company continuously managing third-parties throughout the "lifespan of the relationship," including being able to explain the necessity for the relationship?
- With M&As, can the company explain the pre-acquisition process? If the pre-acquisition process was not completed, can the company explain why not?
- With M&As, has the company completed post-acquisition due diligence, including audits?

KEY TAKEAWAYS

Data-Driven Program

- Is the compliance team given “continuous access to operational data and information across functions”? And does the compliance team apply lessons learned?
- Is the company regularly monitoring employee and third-party behavior, including access to policies/procedures, spending habits, and use of hotlines?
- Is the company analyzing the effects of its trainings, if any?

Assessing the Right Fit

- Can the company justify the structure of its compliance program including decisions pertaining to budgeting, staffing, on-going training and development, access to company data, reporting structure, and independence?
- If the company makes compliance decisions based on the demands of foreign law, can it justify its analysis and explain “how the company has addressed the issue to maintain the integrity and effectiveness of its compliance program while still abiding by foreign law”?

KEY TAKEAWAYS

Third-Party Risk Management

Emphasis on continued management of third-party risks throughout the life of the third-party relationship

- Can the company justify why the third party was hired?
- Can the company identify the risks posed by third party partners?
- Can the company identify other relationships that third party partners maintain?
- Does a contract exist to govern the relationship?
- Is the company monitoring the relationship? If so, how frequently?
- How does the company address concerns that result from monitoring?
- Are third party partners required to complete training and sign annual compliance certifications?
- Are third party partners familiar with and have access to resources, including the company's policies and hotline?
- With M&As, has the company completed post-acquisition due diligence, including audits?

THE UK CRIMINAL FINANCES ACT 2017

UK CRIMINAL FINANCES ACT 2017 - OVERVIEW

- The UK *Criminal Finances Act* 2017 introduces new **criminal** offences where a company fails to prevent its 'associated persons' from facilitating tax evasion by a third party
- The Act applies to the evasion of both **UK** and **non-UK** **tax** and **duties**
- The legislation has extensive extra-territorial application
- The **only defence** is for a company to show that it had "reasonable prevention procedures" in place to prevent the facilitation of tax evasion
- The legislation came into force on **September 30, 2017** – this coincided with the first data exchanges under CRS

THE ‘UK’ OFFENCE

- A failure (1) by a company or partnership (a "relevant body") incorporated anywhere in the world (2) to prevent the criminal facilitation (3) by one of its associated persons (4) of the criminal evasion of a **UK** **tax** or **duty**, payable by another person or entity

- There is no need for the company to have any presence in, or relationship with, the UK for it to be caught by the legislation

- The UK offence will be prosecuted by HM Revenue & Customs (“HMRC”)

THE ‘FOREIGN’ OFFENCE

A failure (1) by a relevant body; (2) to prevent the criminal facilitation; (3) by one of its associated persons; (4) of the criminal evasion of a **non-UK** **tax** or **duty** payable by another person or entity

- This offence applies to (a) any company incorporated in the UK or (b) located anywhere in the world but carrying on a business - or part of a business - in the UK (e.g. via a subsidiary or sales operations in the UK, or even via a listing on the London Stock Exchange)

- A company will also be caught where it does not have a UK presence but where any part of the facilitation takes place by an associated person in the UK

- “Dual Criminality” must exist – i.e. there must be criminal evasion according to both UK law and the law of the foreign country

- The foreign offence will be prosecuted by the UK Serious Fraud Office (“SFO”)

NOTE:

- There is no need for there to have been a prosecution or conviction for tax evasion
- There is no need for the person facilitating the tax evasion to have intended or delivered any benefit to the company
- It is irrelevant that the company was not involved in the facilitation
- It is irrelevant that the company did not know that their associated persons were facilitating tax evasion

► the focus of the offence is the failure to prevent the facilitation

Liability is easy to incur

But relatively straightforward to avoid…

DEFENCE OF ‘REASONABLE PROCEDURES’

- There is a complete defence in law if the company can prove that it had “reasonable prevention procedures” in place at the time of the offence. The official Guidance issued by HMRC (dated September 1, 2017) does not seek to define reasonable procedures. Instead, it suggests that reasonable procedures ought to take account of the following six key principles:

1. a risk assessment
2. procedures that are proportionate to risk
3. top (board) level commitment
4. communication and training
5. due diligence
6. monitoring and review

SUMMARY & CONCLUSIONS

THE DATA EXPLOSION

In addition to the huge amount of data obtained by regulators around the world in recent years, information continues to be gathered from many other sources:

- **paid informants**
- **'whistle-blowers'**
- **data thefts and leaks**
- **investigative journalism**
- **law enforcement 'hotlines'**
- **on-going investigations and inquiries**
- **reviewing electronic payments and transfers**
- **voluntary disclosures implicating third parties**
- **formal requests for information between tax authorities**
- **data exchanges between other law enforcement agencies**

THE FALLOUT

- Huge amounts of sensitive data is about to be exchanged with tax authorities around the world as a result of **FATCA** and **CRS** - including from many of the so-called 'tax havens' and secrecy jurisdictions - leaks, thefts and abuse of such data are inevitable

- **Registers of beneficial owners** and the implementation of recent European **Money Laundering Directives** will result in further data becoming available to the authorities and in the public domain

- Historical data will inevitably implicate certain clients in unlawful behaviour. It is also likely to implicate certain financial institutions, financial advisers, trustees, lawyers, accountants, etc, in legal and regulatory breaches

  - key risks relate to advisers and intermediaries who have assisted (or 'turned a blind eye' to) financial crime committed by customers (e.g. tax evasion, bribery and corruption, sanctions breaches, money laundering, organised crime…)

SUMMARY

- Many recent developments and global initiatives regarding tax evasion, exchange of information, money laundering, bribery and financial regulation
- Further significant changes are imminent in the UK and globally, e.g:
  - **in the UK**: new law - failing to prevent the facilitation of tax evasion
  - **globally**: CRS, ABC & AML strategies, registers of beneficial owners
- The legal, regulatory and enforcement landscape has changed hugely and the risks of non-compliance are increasing
- The focus has shifted towards corporate responsibility and ‘enablers’ but individuals are also at risk

CONCLUSION: A FEW THOUGHTS (AND SOME OPPORTUNITIES)

- Crypto-currencies represent a dynamic new product that has huge potential and will inevitably become mainstream. However, its reputation and associated compliance standards must be strengthened and protected
- Those seeking to abuse such products to launder money, conceal the proceeds of crime or evade tax have very few places left to go
- As a result of recent transparency initiatives, many tax havens and secrecy jurisdictions will effectively go out of business; others will need to reinvent themselves as respectable 'financial centres' and develop new products
- £billions of 'white', 'grey' and 'black' money is already on the move. However, capital flight from compliant financial institutions and financial centres must be avoided
- Data flows, transparency initiatives and an aggressive regulatory environment will give rise to significant challenges, an increased compliance burden and new operational risks. However -
- **For companies that are forward-looking and well-advised, there are significant opportunities to preserve existing capital, attract new business, create new offerings and enter new markets: there is no reason why crypto-currencies cannot be a part of this**

THANK YOU / QUESTIONS?

mwe.com