FINANCIAL CRIME QUARTERLY – ISSUE 1 - SEPTEMBER 2020

Tracking threats and opportunities

EXPERTS WITH IMPACT™

Foreword

Tracking threats and opportunities

Does financial crime get enough attention? Stories of fraud and misconduct – from Enron to the Russian Laundromat – drive headlines and can change organisational behaviour (sometimes for the better, but also for the worse). Yet much of financial crime takes place in the background and only emerges when light shines on the magnitude of the problem.

In this spirit, we are excited to welcome you to our newest publication: the Financial Crime Quarterly. Within these pages, FTI Consulting's Financial Services team will showcase the threats and opportunities facing the financial system (or financial systems, the term we prefer to use). Each issue is dedicated to providing space for industry-leading thought on the most pressing financial crime issues — the latest regulatory insights, case study analyses and stakeholder viewpoints.

The content is designed for our clients and industry leaders in the public and private sectors. We are focused on quality and brevity, and hope that each issue leaves you with a better understanding of the financial crime typologies, control frameworks and regulatory infrastructure with which we all interact on a daily basis.

In this issue, our spotlight is on financial institutions that are criminally owned or controlled by criminals – be it organised crime or smaller groups of corrupt individuals. Ironically, perhaps, we have seen first-hand how regulators, financial intelligence units and enforcement agencies struggle with taking action against these types of firms more so than against firms that simply have poor systems and controls.

Join us for a journey into the mechanics of the many threats and opportunities that exist in the world of financial crime investigations.

Happy reading,

NIGEL WEBB
Senior Managing Director (Partner)

FEDERICA TACCOGNA
Senior Managing Director (Partner)

Bringing criminals under control:

Insights into the complexities of financial crime investigations

In recent years, I have had the pleasure – and the honour – of working closely with regulators and enforcement agencies in Europe and around the globe. I have even led a financial crime unit for one of them. The experience could not have been more varied and diverse. Yet, there is a common feature that I was not expecting: the challenges of prosecuting, or even just fining, firms that are owned, controlled or infiltrated by criminals.

It is counter-intuitive. It should be easy to take down, or just fine heavily, a firm that is so evidently corrupt (thought the innocent me)! Yet, I realise that our collective regulatory and legislative frameworks are too politically correct, bureaucratically sound and naïve to do this.

Years of having to deal with poorly controlled financial services firms, through which criminals could push vast amounts of ill-gotten wealth, have led to regimes that, by and large, do a decent job of telling firms what standards they need to implement and detecting failures early on.

But it is the firms that are owned or controlled by criminals that are often amongst those with the best controls. They have the latest transaction monitoring systems and even tell you that they make full use of artificial intelligence.

And whilst they do that, they will have a Director, who is 'friends' with organised crime or a group of heavily corrupt individuals. He helps his friends obtain accounts and pass their riches (made through corrupt business deals, drug dealing and other unvirtuous endeavours) into the mainstream financial system.

When the regulator knocks on their door, the firm and its employees put forward their best stance. Some – often most of the staff – are completely unaware of what 'really' goes on, or succumb to the dominance of its owner(s) and/or director(s). On occasion, some of them are in on it, too. They showcase pretty solid controls – reasonable due diligence, a decent transaction monitoring system – and they say all the right things.

At times, the regulator has a strong suspicion that something is wrong (the questionable associations are starting to become known, or they have seen a group of questionable clients migrate from a 'bad' bank).

But they cannot find evidence. That is because regulation is designed to penalise, for example, a firm with poor due diligence, but all these clients have been onboarded impeccably (with all the concerning information nicely hidden or 'risk accepted'). Regulation accounts for ways to fine firms that do not detect and report anomalous transactions. But all anomalous transactions belonging to these clients are hidden in separate systems, not audited or shown to the regulator.

"It is the firms that are owned or controlled by criminals that are often amongst those with the best controls".

I have sat in meetings in which I have heard regulators say that their powers were to audit controls, not to extract transactions. To ask for evidence of robust due diligence processes, not to re-perform due diligence on the firm's clients. And I could not disagree. It is true. Regulation is often designed in that way. And so is the legal framework. The lack of education of judges, for example, relating to the problem of financial crime means that, even if a regulator were to take on a different role, the firm would have all the chances of winning a legal challenge on a point of technicality.

So perhaps it is the wider regulatory and legal framework that needs re-thinking. Not because it was not once adequate, but because it is rather evident that it no longer is.

Meanwhile, I work with my teams and clients to work around it. We focus on governance (some of the less than transparent, overly controlling behaviours are major governance failures), on interview techniques (probe, doubt, assume guilt, if you have to) and on obtaining data preservation orders (and then analysing that data independently). It does not always work. It is not ideal. But I have learnt that being on the side of the regulator and enforcement agencies means having to make do with a far less than perfect world.

- Federica Taccogna

New tech, old tricks?

Exposing risks in non-bank financial institutions

Geographically, socially, commercially – the fintech sector is revolutionising how the world consumes financial services by making financial products easier and quicker to access. Thanks to economies of scale, many firms are expanding rapidly within and across jurisdictions, led by a global customer base and a growing web of user data.

Cultures of innovation, growth… and financial crime

Over the years, we have had the privilege of inspecting and designing controls for numerous non-bank fintech institutions across Europe. Privilege, because these firms are some of the continent's most dynamic and innovative enterprises. We were less surprised, though, to find that many fintech firms simply lacked the appropriate understanding and measures to minimise the substantial risk exposure to financial crime.

Putting aside the honest, legitimate firms that sought to rapidly improve their financial crime controls to the required regulatory standard, a cluster of non-bank fintechs that we came across (particularly those offering electronic money, payment cards, payment gateways, remittances and digital payment tokens) appeared to exist solely for the purpose of facilitating financial crime.

> *"In a sector driven primarily by new business models and technologies, regulators are catching up either by surprise (look no further than Wirecard) or by force."*

The more unscrupulous Payment Service Providers (PSPs) varied in several respects, including the sophistication of their operations. Some lacked any form of due diligence and ongoing monitoring entirely. Others appeared to have many of the required controls in place, complete with an MLRO, a transaction monitoring system and a process for running identification and verification checks. Yet when probed further, it became clear that these PSP operators had overcontrolling owners and compromised governance structures — making the typical financial crime controls all but window dressing for illicit activity.

It came as no shock, then, to find that illegitimate firms (and the more reputable ones as well) claimed to be 'adjusting' to recent updates of EU-wide and domestic regulation. And, in an ever-evolving regulatory landscape, this may be true.

But more misconceptions emerged as we delved further into PSPs and other non-bank financial institutions. In particular, several PSPs mistakenly placed the burden of risk on banks. We heard one PSP absolve their obligation to perform customer due diligence by claiming that they only 'rely on banked customers so the customer due diligence has already been done'. Their assumption was clearly flawed, as placing any degree of reliance disintegrates without robust agreements in place and frequent oversight/monitoring of the relationship to ensure compliance.

Mistaken assumptions proved to be just one of the more straight-forward problems. Perhaps the more concerning revelation was the frequent use of intermediaries and chains of PSPs to process customer transactions to obfuscate the payment originator and beneficiary. Much like the manual equivalent of mixers/tumblers in the cryptocurrency space, criminal groups exploited networks of PSPs to separate the transaction details from the actual users. Then consider the combination of PSP chains with the mixing of illicit and licit funds from customers linked to shell companies and high- risk industries (such as gaming), and the financial crime exposure increases exponentially.

It is not a secret that shell companies and shelf companies are often the common denominator for financial crime. But even after major money laundering scandals across Europe, certain now-notorious structures, such as Scottish Limited Partnerships, are re-emerging as convenient vehicles for anonymous buyers to gain access to existing bank accounts with PSPs. They do business with PSPs that are controlled by organised crime through shell companies, offering an end- to-end channel through which to launder illicit gains.

We could go on and on. The bottom line is, though, that the sector's widespread growth and nascent controls leave it highly exposed to financial crime. A renewed effort to collaborate between regulators, investigators and firms across jurisdictions is needed to help prevent these heightened risks from becoming a permanent reality.

Taming TCSPs:

Improving incentives, transparency and accountability

The economic growth of recent decades has, in part, been facilitated by the crucial role that Trust and Company Service Providers (TCSPs) play in facilitating cross-border investment around the world.

Yet the sector faces substantial exposure to financial crime and money launderers are quick to exploit the privacy and economic interconnectedness that TCSPs offer.

Are TCSPs doing enough to be better gatekeepers?

In an effort to boost standards in the sector, recent improvements to financial crime regulation in the UK and EU have introduced more stringent requirements for TCSPs, with an emphasis on transparency – such as performing due diligence and disclosure of corporate directors and ultimate beneficial owners (UBOs).

Keeping up the momentum, however, has been a challenge for regulators and firms alike. Regulators often find that TCSPs are widely underprepared to implement their regulatory obligations. For their part, TCSPs have not been accustomed to closer supervisory scrutiny and are often playing catch-up.

But improving the sector's due diligence and financial crime controls only scratches the surface. How can it, when at the crux of the problem is the inherent conflict of interest at the very heart of the current role of TCSPs?

We have seen this story before. Through 'business- friendly' policies to attract investment, governments put pressure on lowering the time it takes to open a business. Corporate registries lack the resources and expertise to verify the legitimacy of incorporated entities, so they rely on TCSPs to complete the customer due diligence.

Meanwhile, TCSPs enjoy a vested interest in the incorporation of a given company, and fail to adequately vet their customer to the correct standard. When jurisdictions place trust in the due diligence procedures of TCSPs without probing to ensure that the TCSP's controls are adequate, a lack of accountability emerges. This combination of factors has allowed all types of suspect players to compete.

The problem typically manifests in two ways, albeit with the same outcome. When both legitimate and illegitimate firms blindly incorporate and service entities (often shelf companies and entities that end up behaving like shell companies), the sector is abused for illicit purposes — all stamped with a jurisdiction's seal of authorisation and approval.

Making matters worse, some TCSPs deny the extent to which their clients exploit their business. Excuses in lieu of due diligence and ongoing monitoring, such as 'my HNWI client is within their rights to want banking secrecy' or 'my client is the son of the King of XYZ country and so I didn't bother to ask' are common refrains from TCSP directors (both which should have never passed regulatory scrutiny in the first place). There is, of course, a time and place for practices like legal privilege — but using it to obscure compliance failures is not one of them.

Identifying essential improvements

Because the sector has a mixed track record, a paradigm shift is sorely needed. Corporate registries are calling out for resources to help to incorporate entities and associated parties with the correct considerations. At the same time, regulators require reorienting resources to challenge the sector's low-cost, easy route model to obtaining a company; association; bank account; director; trustee; nominee shareholder, and so on.

But perhaps the largest improvements have to come from the industry itself. Core components of compliance, such as independently identifying source of wealth and source of funds, are not merely tick-boxes to address (or ignore). The onus is on TCSPs to ask: does this structure make sense? Is it being used for a legitimate purpose? Why are shell companies involved?

Should TCSPs improve their due diligence, staff training, remuneration, recordkeeping and governance measures, the sector is extremely well placed to monitor financial crime. Yet to truly move in this direction, TCSPs need to align their operations with the ethical and regulatory standards required of them — rather than just collecting fees whilst failing to monitor the firms they serve.

Lagging or leading?

Deconstructing Eastern Europe's efforts to combat financial crime and accountability

It is no secret that Eastern Europe is often singled out as a key corridor for the proceeds of crime. Massive volumes of illicit funds, from the Baltic money laundering schemes ($500 billion) to the Russian Laundromat ($20 billion), have come to light in recent years and exposed the region to the extent of the problem.

Centrally problematic to the region's challenges is a lack of a harmonised approach to regulatory investigation, supervision and enforcement, which is exacerbated by limited resources and shifting political priorities.

Numerous international bodies, including the European Central Bank and Moneyval, have identified shortcomings in the implementation of regulatory controls across the region, including but not limited to key EU member jurisdictions.

Catching up with the EU's legal architecture

Although EU-wide regulation continues to develop at a fast pace, certain jurisdictions have been slow to catch up to the EU's AML/CTF legal architecture and adopting the core components of the regulatory framework.

In one of the more concerning cases, the European Court of Justice ordered Romania earlier this year to pay the European Commission €3 million after failing to transpose the Fourth Money Laundering Directive (4MLD) into national law within the prescribed timeframe.

Yet vulnerabilities due to the slow implementation of the 4MLD are not the only concern for the region.

In January 2020, the EU's Fifth Money Laundering Directive (5MLD) came into force, amending its predecessor by strengthening the AML/CTF regime for cryptocurrency firms, fintech firms and designated non- financial businesses and professions (DNFBPs). Adding to existing regional shortcomings, several member states, including Hungary, Poland and Slovenia also missed the implementation deadline for the EU's Fifth Money Laundering Directive (5MLD).

The lag time that it takes certain jurisdictions to transpose Europe's legal architecture opens up the pan-European economy to criminals who exploit these weakness to their advantage. Think of the networks that try forming a dubious fintech institution in the Baltics, locating data servers in the Mediterranean region and processing payments through an obscure bank supervised by one of the regulators in a Visegrad Group country.

Adopting a risk-based approach to AML/CTF

In the absence of a robust legal framework, regulating and supervising firms from a financial crime perspective becomes much more difficult. International bodies, such as Moneyval, often highlight that regulators in Eastern Europe fail to adequately adopt a risk-based approach to financial crime supervision. After all, in the same way that regulators assess licensed institutions, regulators are also assessed in their ability to embed a risk-based approach in their governance and supervision of ML/TF concerns.

A notable example of this situation is seen in Hungary. Ranking 31st out of 32 European countries assessed by the Basel Institute on Governance's annual AML index, Hungary has one of the weakest AML/CTF regimes in Europe. In particular, Moneyval's most recent evaluation identified its regulation of financial crime to be systemically weak on major issues such as failing to adopt a risk-sensitive approach with respect to correspondent banking and respondent institutions within the EU. In this case, though, it is not just a problem of writing legislation: although Hungarian law already requires firms to apply additional due diligence on a risk-sensitive basis, we have seen firms operating in the jurisdiction with substandard knowledge and inadequate resources.

We also see that a lack of pressure by regulators can have a detrimental impact on firms, exposing them to potential remediation exercises across multiple jurisdictions to ensure adherence to EU-wide requirements.

Improving due diligence and transaction monitoring

One issue at the core of the region's challenges is the institutional weaknesses within regulatory and control frameworks with respect to due diligence and transaction monitoring. In recent cases we have investigated, networks of firms controlled by the Italian and Russian mafia have easily set up bank accounts using rogue trust and company service providers (TCSPs) in various Eastern European jurisdictions to avoid the right level of scrutiny that would expose and prosecute their illicit operations.

It should be no surprise, then, that recent EU Directives, FATF guidance and Moneyval assessments focus squarely on strengthening existing due diligence requirements. Nonetheless, small and large jurisdictions alike in Eastern Europe have found it difficult to supervise customer due diligence requirements in practice.

For example, Moneyval's assessments have highlighted that Poland (amongst other jurisdictions) lacked regulatory requirements for firms to conduct periodic due diligence reviews on existing business relationships. Such a gap in regulatory guidance makes it difficult for firms to determine best practices with respect to implementing a risk-based approach to their business relationships.

Though these weaknesses expose firms and investors to greater risk, Polish prosecutors have increasingly shed light on the legal ramifications of non-compliance by launching investigations into suspected money laundering at multiple financial institutions. With an upcoming Moneyval assessment scheduled for 2021, Poland will likely find its approach to preventing financial crime under greater scrutiny over the coming months.

Ultimately, the absence of strong due diligence practices in the region means that even the most obvious money laundering typologies will be able to wash their illicit funds with relative ease. Without probing regulatory visits and a culture of compliance within the private sector, jurisdictions across Europe will continue to remain exposed to some of the more obvious financial crime schemes.

Thoughts on possible solutions

Weaknesses in Eastern Europe mirror the challenges that we see in other European jurisdictions: a stricter—and often smarter—regulatory approach is required to deter and prevent financial crime from exploiting bona fide efforts to grow the economy and attract investment.

The point is not that every regulator should look or act the same, but that public institutions fulfil the mandates endowed to them by taxpayers and firms by preventing financial crime within the context of the unique economic factors and risks that prevail within each jurisdiction.

Again and again we find that the status quo in relations between regulators and firms is one of animosity or mistrust, rather than the collaborative and cooperative approach that the enormous task of fighting financial crime demands.

Across the region, there is an urgent need for regulators to make broad and deep improvements to financial crime supervision and encourage firms to build the knowledge, resources and technologies needed to prevent ever- changing criminal networks from exploiting the status quo. The future of the region's economic growth, reputation, and ability to generate clean economic growth and investment very much depends on these combined efforts.

Our Team

NIGEL WEBB

+44 (0) 7786 656 278

nigel.webb@fticonsulting.com

Nigel is a Senior Managing Director at FTI and leads the Financial Services practice for EMEA. Originally an econometrician by training, his 30-year career has encompassed both consulting and business roles across a broad range of the banking world. Nigel regularly provides support to a wide range of financial services clients in preparation for regulatory visits and during or in response to Skilled Person's reviews on the topic of AML and financial crime, coaching and advising senior managers and board members.

PIERS RAKE

+44 (0) 7866 144 063

piers.rake@fticonsulting.com

Piers is a Managing Director in the Financial Services practice, based in London. He has led a wide range of complex cross-border investigations across the EMEA region, on behalf of private and public sector clients, including in relation to organised crime networks, high-end money laundering, fraud and corruption. In his role as former Global Head of Financial Crime Investigations and Nominated Officer at a large transatlantic bank, Piers planned and led proactive and reactive investigations into the full range of complex money laundering typologies, and worked with law enforcement on criminal disruption operations.

HENRY DUGGAN

+44 (0) 7790 984 735

henry.duggan@fticonsulting.com

Henry is a Managing Director in the Financial Services practice, based in London. Henry has led specialist assignments covering sanctions investigations, terrorist financing, fraud & misconduct investigations, accounting irregularities, fraud risk management and AML. He works closely with Data Analytics, Forensic Technology and Intelligence experts to develop methodologies to investigate terrorist financing and sanctions breaches for submission to regulatory authorities and law enforcement agencies.

FEDERICA TACCOGNA

+44 (0) 7590 112 559

federica.taccogna@fticonsulting.com

Federica is a Senior Managing Director in the Financial Services practice, based in London. Previously holding senior risk and compliance positions in industry, she now supports a broad range of financial services institutions and regulators globally advising on, investigating and remediating regulatory and financial crime matters, governance and control concerns including conflicts of interest, pricing and sales practices, governance structures, control frameworks, product and client governance and remuneration.

ANDREW HADLEY

+44 (0) 7967 776 656

andrew.hadley@fticonsulting.com

Andrew is a Managing Director in the Financial Services practice, based in London. Andrew has worked on transaction reviews, financial crime reviews and remediation exercises, delivered training to first and second line functions, assisted in reviewing governance structures (including those overseeing financial crime), delivered a review of a firm's transaction monitoring governance arrangements, drafted policies and procedures for financial services clients. He has also advised clients on business strategy.

FTI Consulting:
Experts with Impact ™

FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes. Through our breadth of expertise, culture, services and industry experience, we have a tangible impact in helping our clients solve their most complex opportunities and challenges.

Our expertise

- Forensic & Litigation Consulting
- Corporate Finance & Restructuring
- Economic & Financial Consulting
- Strategic Communications
- Technology

Financial services

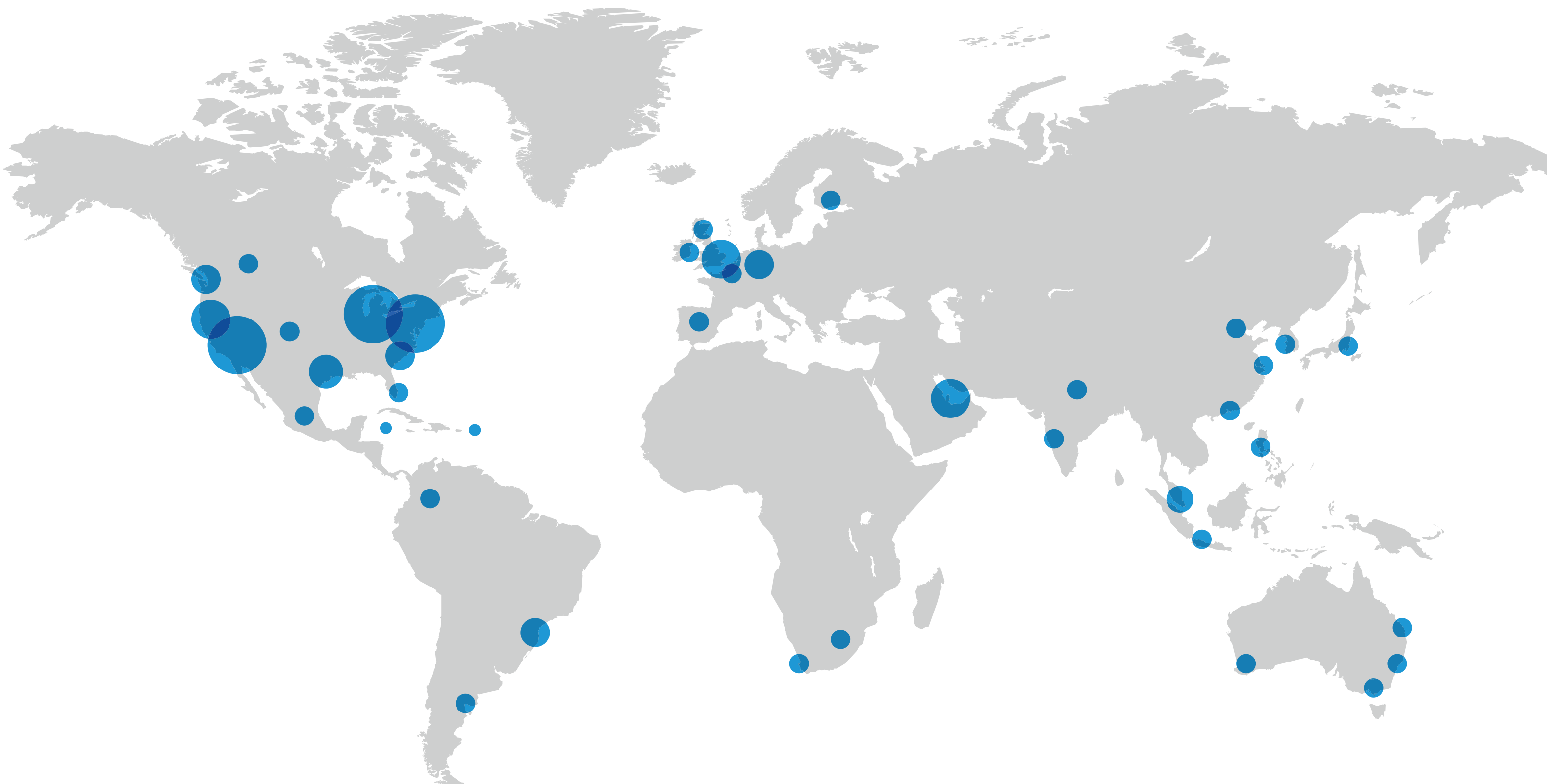
Our Financial Services practice is comprised of a team of regulatory experts who specialise in investigating financial crime concerns on behalf of regulators and enforcement agencies, building and strengthening regulatory resilience and assisting regulated firms in designing and implementing risk control frameworks.

We have led many of the recent large-scale investigations on behalf of our clients in the public and private sectors (such as ABLV Bank in Latvia and the Malta Financial Services Authority).

Industries

- Aerospace & Defense
- Agriculture
- Automotive & Industrial
- Construction & Engineering
- Energy, Power & Products
- Environmental
- Financial Services
- Global Insurance Services
- Government & Public Sector
- Healthcare & Life Sciences
- Hospitality, Gaming & Leisure
- Insurance
- Metals & Mining
- Real Estate & Infrastructure
- Retail & Consumer Products
- Telecom, Media & Technology
- Transportation & Logistics

Our Global Offices



Asia Pacific

Australia	Indonesia	Malaysia
China	Japan	Philippines
India	Korea	Singapore

Americas

Argentina	Colombia	Canada
Brazil	Mexico	United States
Caribbean		

Europe, Middle East & Africa

Belgium	Ireland	Spain
Denmark	Netherlands	United Arab Emirates
France	Qatar	United Kingdom
Germany	South Africa	

5,800+

Employees

590+

SMDs

$4.4B

Equity Market Capitalisation*

1982

Year founded

53

53 of Fortune Global 100 corporations are clients

8/10

Advisor to 8 of the world's top 10 bank holding companies

96/100

Advisor to 96 of world's top 100 law firms

84

Cities in 27 countries

*Number of total shares outstanding as of July 23, 2020, times the closing share price as of July 30, 2020.

Our Awards

2018 - 2020

UK's Leading Management Consultants

Financial Times & Statista

2017 - 2019

Consulting Firm of the Year

Who's Who Legal

2020

#1 Forensic Accounting, eDiscovery & Economic Analysis

Chambers & Partners

2020

Public Affairs Consultancy of the Year

PRovoke Media

2020

Best Thought Leadership: Resilience Barometer

Managing Partners' Forum Awards

2020

25 Investigations Experts Recognised

Who's Who Legal

Join our mailing list: **financial.crime@fticonsulting.com**

Learn more about us: **fticonsulting.com**

Our insights: **ftiinsights.com**

1156 - 09/20