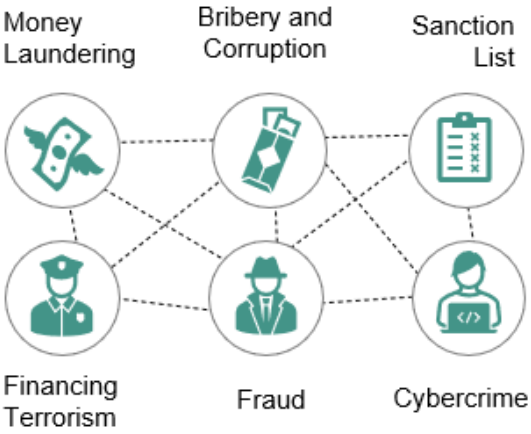
TORI

Experience. The difference.

Combatting Financial Crime with the use of Artificial Intelligence (AI)

Executive Summary

The rise of Financial Crime is an ever-increasing threat to global economies, the financial sector, and individuals. Criminals are becoming more sophisticated at breaking through gaps in Cyber Security, and the traditional methods to combat Financial Crime cannot keep up with the pace that criminals can operate.



According to the Financial Conduct Authority (FCA), in the UK alone, the financial services industry is spending **£650 million** annually to combat fraud, money laundering, and other financial crimes. The financial services industry dedicates copious amounts of money and resources to try to recoup and get transparency of the nearly **£1.2 billion**[1] that was stolen by criminals in 2022, while in the same year, costs associated with financial crime compliance soared at **£220 billion**. With the severity of this risk, it is important to find new ways to detect and reduce financial crime.

As individuals and markets continue to be exposed to all kinds of threats, financial crime teams must become increasingly alert, responsive, and agile to counter emerging threats and navigate unforeseen disturbances. Failure to detect and predict financial crime activities can result in significant financial losses for businesses, and individuals alike.

Given the dynamic threat landscape, traditional semi-automated approaches in combating Financial Crime can be argued not to be as effective. Financial Institutions possess vast amounts of data, which can be seen as a challenge in enabling the identification of Financial Crime activities and therefore the prediction of outcomes, which can have huge financial implications.

Artificial Intelligence (AI): A friend or a foe?

At the forefront of technological advancement, AI stands to revolutionise the battle against financial crime. It is inevitable that AI as a tool can offer massive efficiencies, enhance customer data, and identify new risks. Yet, a growing area of concern and focus is the concept of reliability, how an AI model generates information and stories and how it has come that we trust it so impulsively. However clever we think these systems are, the process of AI in detecting financial crime is iterative. A human being who is an expert to prompt and iterate the response that we need to arrive at the right answer, is essential.

[1] https://www.fdmgroup.com/news-insights/ai-in-financial-crime/

The Regulatory Landscape: A 2024 outlook

Regulatory compliance remains a top focus for financial institutions, requiring ongoing investment in compliance programs, technology solutions, and workforce training to effectively mitigate financial crime risks.

In 2023, the banking industry globally faced more than **£670 million** in fines for inadequate AML Governance processes.[2] Indicatively, it is imperative organisations to bolster their detection capabilities and stay ahead of evolving risks.

In early 2024, the Financial Conduct Authority (FCA) announced its increased focus on financial crime and the efficacy of firms' control systems, through *Dear CEO* and letters. This shift was evident in the review of critical areas such as money mules, sanctions systems, and how firms are adapting to the escalating Russian sanctions. Firms are expected to evaluate their financial crime approaches against the FCA standards, promptly enhancing them if needed.

As Fin Crime professionals continue to find new ways to leverage AI, it's the responsibility of policymakers to ensure they are aware of the threats of these technologies.

At the most recent G7 summit in Hiroshima, world leaders indicated their firm commitment to collaborative efforts in establishing an inclusive framework for AI governance.

In October, the G7 issued a Statement on the Hiroshima AI Process, announcing the Hiroshima Process International Guiding Principles for Organisations Developing Advanced AI Systems. This reflects a shared recognition by the international community in fostering innovation while safeguarding against potential threats.

Also, the Hiroshima Process International Code of Conduct for Organisations Developing Advanced AI Systems, ensures that AI advancements are guided by principles of transparency, accountability and fairness.

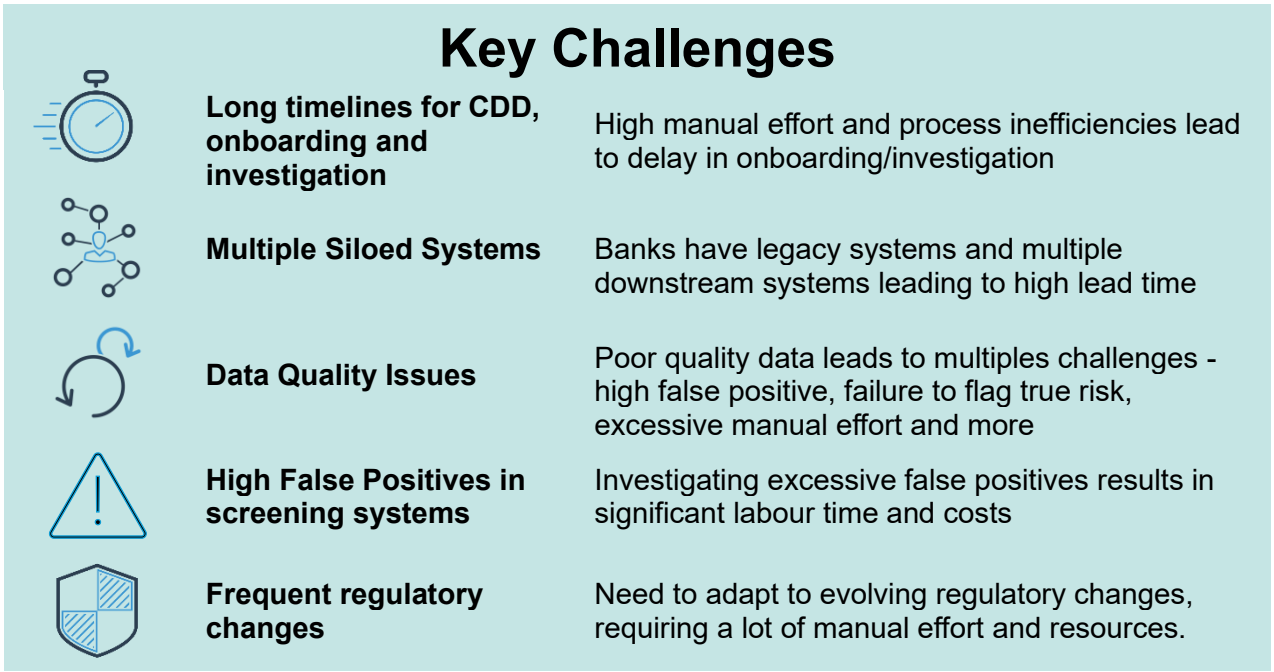
The Inadequacies of Traditional Approaches

Traditional approaches to combatting financial crime have relied heavily on manual processes, rules-based systems, and legacy technologies. As part of Financial Crime compliance, risk management activities such as transaction monitoring comprise KYC, AML measures and screening, based on predefined rules and thresholds to flag suspicious activities. However, these rules often fail to capture the latest trends of money-laundering behaviour. There are traditional ways of doing things, but how can AI make detection techniques more sophisticated?

This can be a challenge for organisations who have large amounts of data at their disposal but can't get the insights they require, or they can't get them quickly enough to ensure greater resilience against evolving threats.

Outdated, manual systems lack the predictive power needed to identify emerging patterns, trends, and anomalies indicative of financial crime. The most common encounter is a **high rate of false positives** in screening systems. False positives in AML compliance refer to when a transaction or customer record is flagged to be suspicious, i.e. matching a name on a sanction, watchlist or a politically exposed person (PEP) list, when in fact that flag is incorrect.

Figure 1: *Key Challenges of traditional approaches*

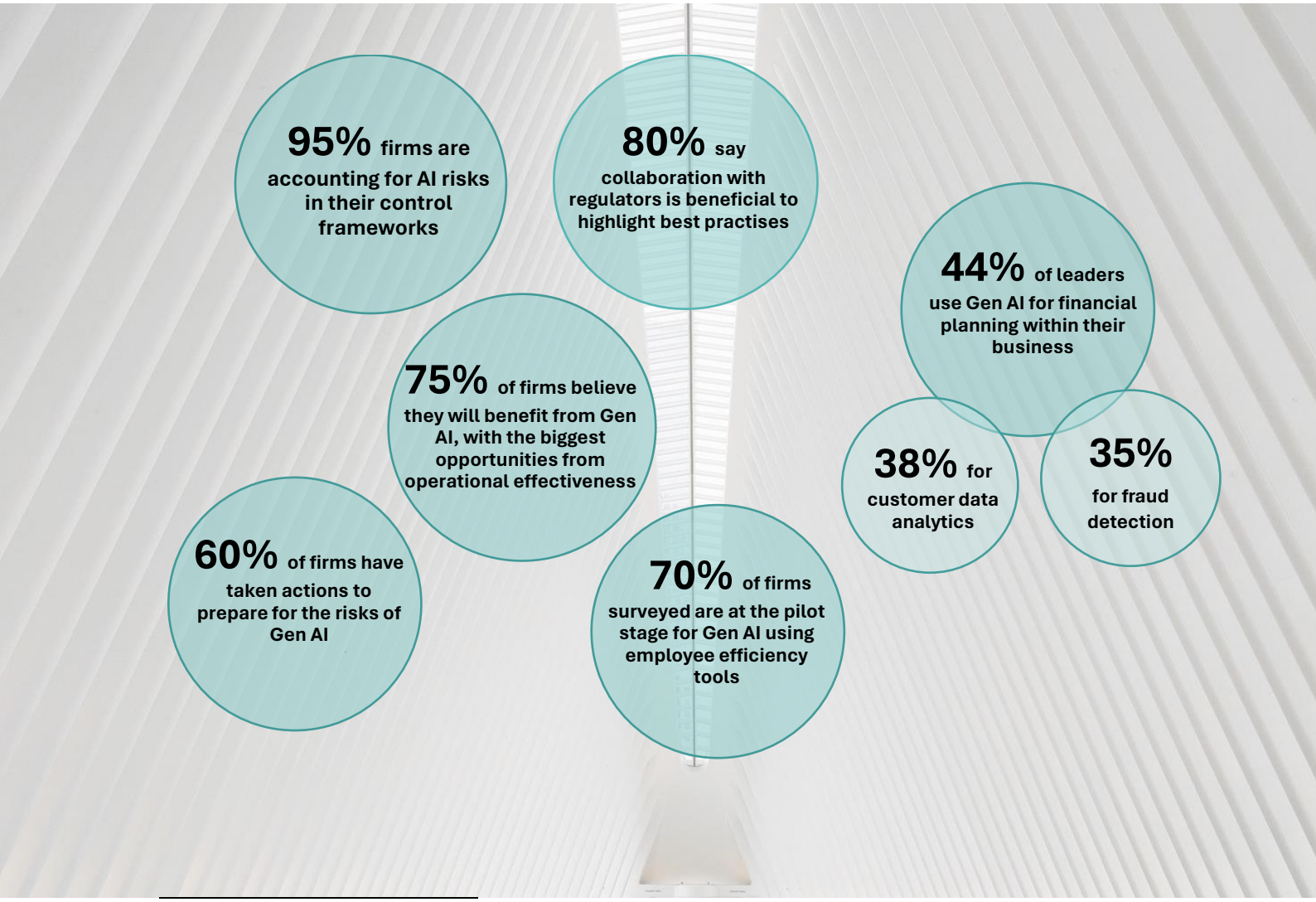


The Rise of Artificial Intelligence tools

While financial institutions are increasingly adopting AI, it's evident that criminals are also adept at leveraging these technologies. Therefore, we shouldn't view AI merely as a passing trend, but rather as a necessity. Financial institutions and importantly financial crime prevention teams must continue innovating and employing multi-layered approaches to fighting financial crime and stay one step ahead of the criminals.

Introducing AI in Financial Services: What do firms in the banking sector think about Gen AI?

Figure 2: *Data from 23 companies ranging from international to mid-size banks and non-banking FS firms.* [3] [4]



[3] https://www.ukfinance.org.uk/news-and-insight/press-release/majority-banks-are-piloting-opportunities-generative-ai-and#:~:text=Three%2Dquarters%20(75%20per%20cent,revenue%2Drelated%2C%20use%20cases.

[4] https://www.cityam.com/city-leaders-turn-to-ai-bots-for-financial-advice/

Embracing Generative AI tools:

Within financial services, Generative AI (Gen AI) can become a catalyst for financial institutions' risk management, from modelling analytics, to automating manual tasks, and synthesising unstructured content.

How should companies prepare to capture the benefits of Gen AI to manage risk better?

Delve into the potential of AI to strengthen Anti-Money Laundering (AML), fraud detection and risk management efforts and foster a more secure and trustworthy financial landscape.

- **Machine Learning for Transaction Monitoring**

Emulating human-like decision-making, **Machine Learning (ML**) can help identify complex patterns and anomalies within large datasets and report suspicious activities.
In theory, financial institutions can apply ML across the entire AML value chain, but particularly they can reap immediate benefits within transaction monitoring.

- **Natural Language Processing (NLP) or Credit Risk**

NLP is an AI-driven tool that leverages advanced language analysis to identify patterns and risks from unstructured data, eliminating manual processes and providing an effective approach to detect and mitigate financial threats.

Put simply... ML is like teaching the computer to predict the stock market. Instead of relying on human intuition or rules, you feed the computer tons of data – like stock prices, company metrics, economic indicators, and news headlines. Using this data computer learns patterns that humans might not articulate or even notice. Over time, as it sees more data, it learns from its mistakes, and it gets better at making predictions for the things you want, i.e. which stocks will go up.

In the same way, ML algorithms can be trained on historical transactions to learn normal behaviour patterns across various dimensions; frequency, location, parties involved. It adapts and learns continuously.

ML-based AML solutions can significantly enhance the detection of suspicious activities. Research has delved into the efficacy of AML tools, with one study evidencing how ML algorithms outperform traditional rule-based systems; A **28% increase** in identifying intricate patterns and anomalies in transaction data, compared to non-ML-Based solutions.

Put simply... Imagine you're interested in understanding how certain individuals have become billionaires. You want to analyse news articles, social media posts, and financial reports to uncover common patterns or strategies used by successful individuals. Using various techniques, NLP comes in and can enable the extraction of valuable insights into the

strategies and patterns behind this topic; wealth accumulation.

Within banks, NLP can be used for customer due diligence; Customer information can be summarised i.e. transactions with other banks, to inform credit decisions.

Financial institutions leverage this technology to automate the generation of credit risk reports and extract valuable insights from credit memos, expediting the entire credit process. In turn, it can help generate estimates for default and loss probabilities, empowering banks to make informed lending decisions swiftly and accurately, while bolstering Anti-Money laundering efforts. [5]

- **User Behaviour Analytics (UBA) for Anomaly Detections**

Behaviour analytics focuses on analysing patterns on behaviour and activities within an organisation's networks to detect and mitigate security threats. **Machine Learning (ML)** plays an important role in supporting behaviour analytics, indicating best results when large data sets are involved. With anomaly detection algorithms, financial institutions can flag transactions or activities that deviate significantly from their expected behaviour.

Companies can better monitor model performance and generate alerts if metrics fall outside tolerance levels, through the migration of some legacy programming languages to rule-based model that incorporate ML.

Real life scenario within fin crime compliance is the implementation by investment bank JPMorgan Chase for machine learning approaches for fraud detection. Through transaction patterns analysis, user behaviour, and historical data, the bank achieved a significant reduction in false positives and reported an improved accuracy of their fraud detection systems.

[5] https://amazinum.com/insights/what-is-nlp-and-how-it-is-implemented-in-our-lives/

Need for attention: Fraud in Authorised Push Payment

Authorised Push Payment (APP) Fraud Liability is when individuals fall victim to fraudsters posing as legitimate payees, resulting in financial losses. According to UK Finance, the year 2023 witnessed a staggering **£239.5 million** lost to APP fraud alone. [6]

Within the financial services industry, banks emerge as prime targets in the fraud landscape, underscoring the imperative for continuous investment in enhanced systems capable of detecting criminal activities, including account takeover attempts.

Therefore, the integration of automated systems leveraging machine learning (ML) models, will not only reducing overall costs but also enhance the accuracy of fraud detection by minimising false positive rates.

Risk-Driven KYC: What financial institutions can do to improve their due diligence remediation.

To gain a deeper understanding of the positive impacts that ML-based AML (Anti Money Laundering) tools can have, TORI researched how financial institutions can enhance their risk-driven KYC procedures and customer due diligence remediation.

- **Segment customers more finely:** By using AI for customer segmentation, banks can identify and focus on high-risk customers, while dedicating more attention to those who pose significant risk and allocate fewer resources to low-risk customers. By choosing between proactive and reactive contact with customers, companies can determine various monitoring procedures and controls that the 'risky' customers might need.
- **Third-party data, external providers, and AI:** Regulatory technology companies and other providers have data available of beneficial owners, politically exposed persons or those who feature negatively in media coverage. This is particularly relevant with the great deal of political activity and geopolitical disturbances happening in 2024.
- **Optical character recognition (OCR):** OCR technology enables the extraction of data from historical customer records, facilitating validation or pre-population processes. The data can then be processed using AI and NLP technology to identify high risk individuals or entities involved in a trade transaction.

[6] https://www.form3.tech/_prismic-media/899da9a9bef0b078080c1b0ecb1063f80798f402fb5f3a1ec2403350b549c8b7.pdf

AI's Positive Impact on Reducing Financial Crime

Enhanced Detection and Accuracy

ML and AI algorithms are adept at sifting through massive volumes of financial data, identifying intricate patterns, and flagging potentially suspicious activities. (Note: the accuracy and validity of data and all corresponding attributes e, g. lineage, ownership, source etc. are challenges which need to be fully addressed before any AI based output is trusted)

Efficiency and Productivity

Leveraging Gen AI helps generate material that would otherwise have to be produced manually, consuming valuable time and resources. Automation tasks have brought significant boost in efficiency, with manual tasks now be streamlined, allowing AML professionals to focus on higher value tasks. Survey conducted on Fin Crime specialists reported **67% reduction** in manual work by AI & Machine Learning [7].

False Positive Reduction in screening

Compliance teams have been overwhelmed with this pain point, diverting attention away from genuine risks. Using fine-tuning algorithms and incorporating advanced data analytics, the number of false positives can be substantially reduced.

Adaptability and Regulatory Compliance

Technology-driven AML tools can substantially help in keeping up with evolving requirements. They can be instantly updated to align with new rules and regulations that are constantly being enforced, i.e. by the FCA or PRA.

Empowering AML Professionals

Rather than replacing human expertise, these tools assist and empower AML professionals, providing valuable insights, streamline processes, and help improve the precision that is vital within capabilities of compliance teams.

[7] https://sanctionscanner.com/Content/Report/2023-2024-Financial-Crime-and-Compliance-Report.pdf

The complexities of Implementing AI in AML and KYC

AI will not only speed up the due diligence process but will also help to improve it continuously.

Skills and Training: Undoubtedly, there are still knowledge gaps within AI, impacting confidence and trust in technology. For the potential of Gen AI to be fully realised, organisations need to ensure proper training for the skills required in creating value, achieving long-term productivity and competitiveness.

Planning and Strategy: Integrating KYC data from multiple sources and systems can be complex, particularly when dealing with legacy systems or proprietary formats. It requires careful planning, data mapping, and interoperability solutions to ensure seamless integration and compatibility with AI-driven analytics.

Integrated Systems: As the volume and complexity of KYC data grow, the scalability and accuracy of AI systems become critical considerations. Designing scalable architectures, optimising algorithms for efficiency, and leveraging cloud computing resources can help address scalability challenges and ensure optimal performance that aligns with an organisation's objectives.

Automation of Supporting tools: Security measures must be implemented at various levels, including data encryption, access controls, network security, and threat detection mechanisms. Automating supporting tools, including Machine Learning Operations, data and processing pipelines to accelerate the development and maintenance of Gen AI solutions.

Multifaceted Solutions: Integrating expertise for comprehensive resilience.

Addressing these challenges requires a holistic approach, involving many different areas of expertise in cyber security, cloud computing, data management, machine learning, software engineering, and regulatory compliance.

It is important not to understate human intervention with these tools and their input in maintaining the complexities of Artificial Intelligence. It is necessary to strike the ideal balance between human and technological inputs.

Building an effective Financial Crime Risk Management approach.

- Experts can bring the necessary knowledge to understand the nuances of evolving and sophisticated criminal tactics, understand complex regulations, and identify potential vulnerabilities within the institution's operations.

- Financial Crime advisors must remain well-informed and equipped to navigate the evolving landscape, and Gen AI can assist it regularly review latest regulatory requirements and industry standards, i.e. **APP fraud, PEPs, AI Regulations (G7), Economic Crime Plan 2 (UK).**
- Skilled professionals, and especially Financial Crime experts are integral to supporting AI systems. To name a few; Machine Learning Engineers, Data Scientists, Business Intelligence Developers, play a pivotal role in updating AI models, fine-tuning algorithms, and interpreting results; prompting them to get the outcomes they need.

- Necessary ongoing refining of AI tools. Whether organisations use external suppliers for AI tools, or their own developed products, they must ensure that the tools are consistently being updated and maintained. Criminals will find ways to update their strategies to penetrate the security measures embedded within the AI tools. It is imperative that the tools are kept up to date in terms of OS and firmware versions and are underpinned by the latest cyber security enabling capabilities. At the current of AI development is vital that humans compliment AI and verify and regulate the data that it produces.

Inevitably, AI exists on both sides of the equation. It is a remarkable tool that can defend against crime, but also perpetuate crime. As the world quickly becomes more prone to the automation era, it is important to note that automation must be used where appropriate and consider the scale of companies – it is not for everyone. AI should not be seen as a replacement for skilled resources, instead augment them, to work more efficiently and reliably.

How TORI Can Help

TORI Global specialise in helping companies with the implementation of emerging technologies and the corresponding governance and organisational transformation that may be required. Some of the ways that TORI Global can help, include:

- **Strategy Development**: TORI Global can help companies develop a clear strategy for incorporating AI into their business operations. This may include identifying the key areas where AI can add value and developing a roadmap for implementation.
- **Project Management**: TORI Global can provide project management support to help organisations successfully implement AI projects on time and on budget. This may include project planning, resource allocation, and risk management.
- **Technical Expertise:** TORI Global have a team of experienced subject matter experts who can provide technical expertise to help organisations design and implement AI solutions. This may include the selection of appropriate technologies and the development of custom AI models.
- **Change Management**: The implementation of AI often requires organisational change; we can assist organisations to manage this process effectively. This may include training and communication support to ensure that employees are able to work with AI technologies, to ensure the realisation of value to the firm.

Our technical expertise is complimented by the TORI Subject Matter Expertise in Compliance & Risk advisory, through well-defined propositions and delivery of related engagements with numerous clients.

Costas Liassides

Co-CEO

t: +44(0) 2038394454 **m:** +44(0) 7768022753
costas.liassides@toriglobal.com

Chloe Larkou

Junior Consultant

t: +44(0) 7398493859
chloe.larkou@toriglobal.com

Ellie Hills

Junior Consultant

t: +44(0) 7754427100

ellie.hills@toriglobal.com