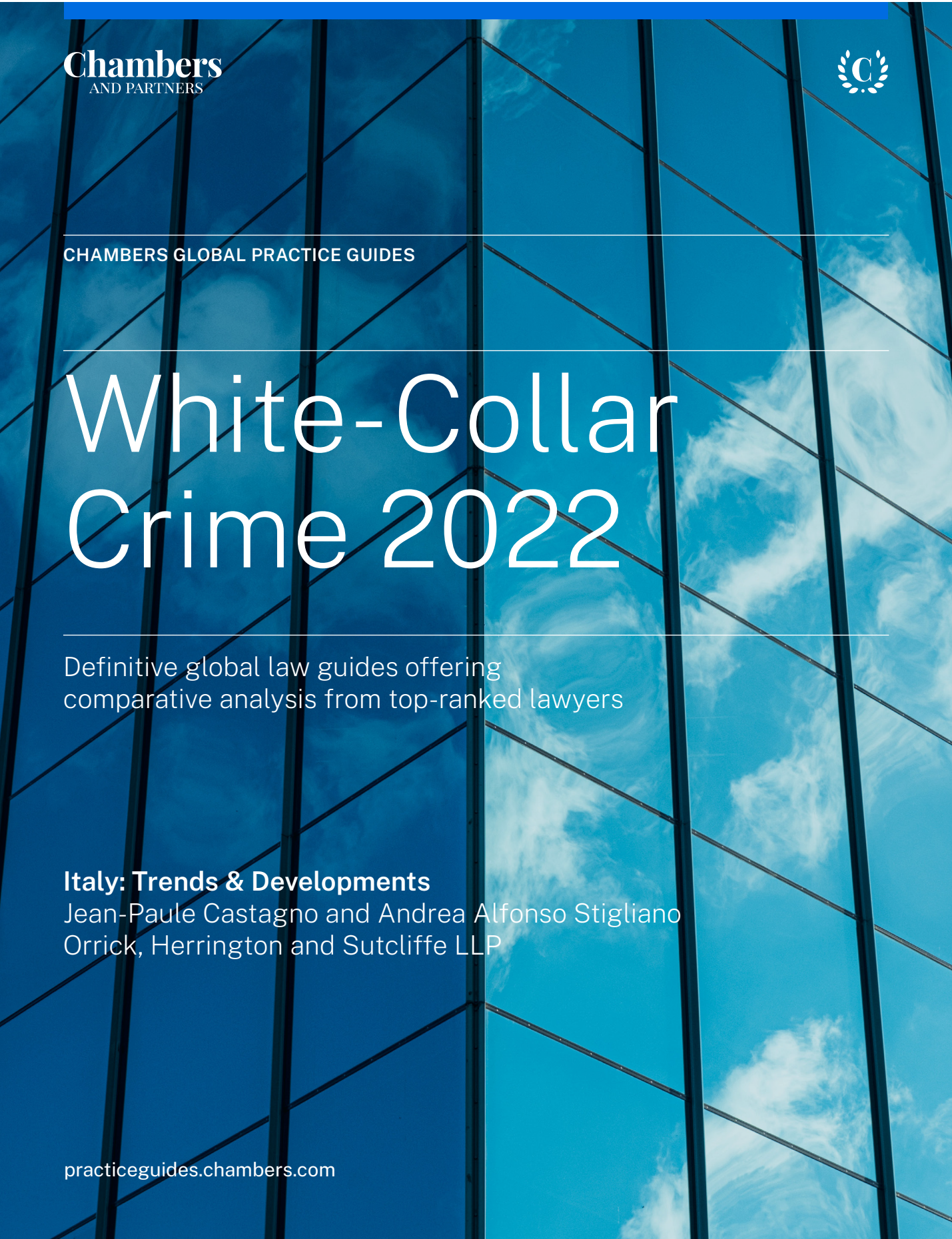


Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

White-Collar Crime 2022

Definitive global law guides offering comparative analysis from top-ranked lawyers

Italy: Trends & Developments

Jean-Paule Castagno and Andrea Alfonso Stigliano
Orrick, Herrington and Sutcliffe LLP

practiceguides.chambers.com

Trends and Developments

Contributed by:
Jean-Paule Castagno and Andrea Alfonso Stigliano
Orrick, Herrington and Sutcliffe LLP **see p.10**

Introduction

Following the end of the critical phase of the COVID-19 pandemic, notwithstanding that there are other emergencies such as the energy crisis and the war in Ukraine, life is slowly starting to get back to normal.

Even in the world of white-collar crime, after years of state of emergency and remote hearings, in recent months things seem to have returned to the pre-pandemic status quo.

There is therefore a need to understand whether these unusual years have introduced any changes, even long-lasting ones, both in terms of crime trends and of tools used within the criminal justice system to deal with potentially unlawful situations.

Especially after the summer recess of 2022, some conclusions can be drawn to try to understand how this "new normal" will develop and what changes, both social and legal, that emerged during the pandemic will characterise future trends.

In an attempt to give an overview of the issues that have undergone the most significant changes, as well as to identify the common features and specific trajectories that the Italian and European judicial systems will follow in the coming years, this article will cover the current "hottest trends", including:

- cybercrimes and cyber-laundering, with an increase in digitalisation and the related risk of exploitation of new technologies for criminal purposes, which has led to a rise in control functions delegated by the authorities to financial operators and companies in order to fight money laundering;
- fraud related to European and national funding, with an increase of the latter as a means to overcome the COVID-19 crisis, which has resulted in more stringent conditions being put on financial operators and companies with regards to compliance and due diligence so as to avoid any potential illegal use thereof; and
- the new trend set by the Milan Prosecutor's Office of appointing "monitors" under the anti-Mafia legislation to companies that, though outside the Mafia environment, have shown a lack of compliance, especially in the selection of third parties, with the aim of encouraging compliance culture.

Analysis of the above trends will reveal:

- an increasing focus on the involvement of entities in the financial and industrial sectors in preventing, together with the authorities, the commission of crimes by means of thorough checks of the relevant operations;
- the pressure put on companies to structure their internal compliance systems in effective and integrated terms; and
- the need for internal investigations to allow for the testing of compliance systems and active co-operation with the authorities.

Digitalisation, Cybercrimes and Money Laundering

As a result of the lockdown period, which in Italy lasted from 2020 to 2021, and the rise of remote work, which still characterises employment relationships in 2022 with the majority of the population being confined to their homes, and the subsequent increase in the use of the internet, of online transactions and the digitalisation of many economic fields, criminals have (successfully) tried to take advantage of the situation. The direct consequence is that financial cybercrimes have increased exponentially.

Financial cybercrimes constitute a variety of offences, including phishing, spoofing, IBAN swapping etc, which concern both individuals and companies and can cause multi-million dollar damage, as a result of which companies and individuals are increasingly investing in cybersecurity in order to protect themselves from hacker attacks.

In these kinds of attacks, follow-on action lacks effectiveness, given the difficulties in tracking down criminal proceeds and the frequent use of sophisticated technologies to conceal one's digital identity.

Therefore, prevention becomes a fundamental asset for companies and, in particular, cybersecurity has become one of the main tasks in companies' compliance agendas, with the relevant budget constantly growing year after year.

However, avoiding falling victim to cybercrimes is not sufficient. As once said by a manager of a cybersecurity company: "the whole idea is why invest hundreds of thousands of dollars to build your own malware when you can just convince someone to do something stupid?". Companies are now focusing more on internal compliance rules regarding both the use of IT devices and the checklist before approving bank transactions, together with continuous and tailored training for employees.

Anti-money laundering (AML) has a pivotal role in combating cybercrimes: while money laundering is a long-standing problem, with the increase in cyber flows this phenomenon is progressively evolving into cyber laundering – obviously strictly connected to cybercrimes, in order to secure the relevant proceeds – particularly targeting the financial sector and causing damage of up to USD6 trillion globally over the last year.

With the rise of new technologies, this phenomenon has become more and more sophisticated, making cash flows more difficult to trace and allowing for funds for illicit asset purchases and other illegal activities to be created.

Recent trends include a surge in virtual asset management, a proliferation of cryptocurrencies and an increased use of schemes and filters, including virtual ones, to conceal the beneficiary of a given transaction. In fact, more and more relationships with financial institutions are no longer initiated through face-to-face encounters, but rather online, thus making it easier for them to be exploited for criminal purposes through anonymity and the difficulty in tracking down transactions.

In order to prevent this type of criminal activity, regulators, both at a national and European level, have provided for decentralised control mechanisms, to be performed by individual national authorities and agencies, which are part of a network of transnational horizontal collaboration – between, for example, National Prosecutor's Offices, Financial Intelligence Units and the European Public Prosecutor's Office (EPPO) –

and continuous exchange of data and information.

In this respect, European provisions on AML, set out mainly in EU Directives No 2015/849, No 2018/843 and No 2018/1673, aim to harmonise member states' legislation and avoid "forum shopping", which could be an issue given differences in the way offences are worded as well as the provision of different penalty levels in each state.

Furthermore, AML regulations provide for the increased involvement of financial operators in the fight against money laundering by delegating control functions to the latter. For example, Legislative Decree No 90/2017, amending Legislative Decree No 231/2007 (the "AML Decree") provides for an AML officer who is charge of all AML-related compliance within each entity, whereas the European Banking Authority's Guidelines of June 2022 require entities to identify at least one board member responsible for implementing the provisions necessary to comply with EU Directive No 2015/849. Legislative Decree No 90/2017 also imposes a duty of active co-operation with the authorities through the reporting of suspicious transactions and the disclosure of information concerning clients, with a view to preventing and punishing unlawful behaviours.

In this regard, one of the newest pieces of AML legislation in Italy, which follows the path laid down by European AML Directives and the AML Decree, is a Decree issued by the Ministry of Economy and Finance in January 2022, which sets out certain operational requirements for crypto-asset service providers, including enrolling in a register (as already provided for money changers) and reporting obligations in relation to transactions involving cryptocurrencies.

As a result of the above, therefore, financial operators are being pressured into taking risk-based approaches and adopting effective AML programmes, by making use of artificial intelligence (eg, blockchain technology, which allows firms to keep track of transactions by using cryptography), to ensure ongoing compliance with the evolving regulatory landscape, anticipate emerging risks appropriately and avoid the negative consequences of failing to do so, such as reputational harm and adverse financial repercussions.

In fact, while new technologies may be the cause of the emergence of new AML risks, they can nonetheless help in mitigating said risks, as they allow information to be analysed in a swift manner and any suspicious transaction pattern to be detected automatically, hence they can make a valid contribution to know your customer (KYC) processes and also reduce costs for operators.

Against this backdrop, prosecutors are now focusing on verifying financial institutions' compliance with AML regulations, especially those in the fintech sector, such as electronic money institutions and payment institutions. In fact, considering that – according to prosecutors – many online financial providers have often been used for criminal purposes, owing to a lack of compliance within the financial system, another new trend consists in the increase of criminal proceedings against financial institutions for money laundering. In more detail, prosecutors consider entities which do not comply with the AML framework as having acted recklessly by knowingly not adopting an AML programme and by accepting the risk of having fraudsters as clients, and consequently are considered to be accomplices in the crimes committed by the latter.

This latter trend requires financial institutions, especially new players with lighter corporate and compliance histories, to include compliance, mainly but not only in the area of AML, at the top of their agenda and to implement constant and smooth co-operation with the authorities, demonstrating their commitment to combating financial crimes and money laundering.

The Green Transition and Fraud Related to EU and National Funding

Over the past two years, there has been a sharp increase in funding, both at national and European level, as a way to overcome the COVID-19 crisis and as part of the EU's plan to secure a number of goals, such as digitalisation and the "green transition". This phenomenon, however, in addition to playing an important role in terms of relief and stimulus, is appealing to criminals and has proved vulnerable to Mafia meddling.

In this context, with the National Recovery and Resilience Plan (NRRP), adopted in 2021 as part of the Next Generation EU Plan (NGEU) to revive the economy following the COVID-19 pandemic, and allocating EUR191.5 billion to be used in six policy areas, including digitalisation, innovation, sustainable mobility and the green transition, two different phenomena have emerged (or, at least in the first case, became more evident): fraud aimed at obtaining public funds and tax credits.

Obtaining public funds

Obtaining public funds is linked to, for example, obtaining incentives related to renewable energy sources or to specific types of digitalisation, creating an area in which, as stated by the Milan Prosecutor's Office, there is a high risk of Mafia infiltration and which will see an increase in controls by the newly established EPPO and, consequently, in internal investigations and litigation.

In order to counter these types of fraud, the law provides for both preventive checks at the time of application, in which importance is given to self-declarations submitted by the individuals or entities making an application and claiming to be eligible for funding, and ex-post controls, carried out by certain authorities such as the Italian Anticorruption Authority (ANAC), at a national level, and by the EPPO and European Anti-Fraud Office (OLAF) at a European level, since supervising the granting of incentives has always been one of the goals, from the point of view of enforcement agencies, which has had a focus on phenomena such as fraud against the State and dissipation of public funds.

The very idea of the EPPO, which is the first example of a central prosecution authority in the EU, stems from the need to protect EU interests, and, in fact, its focus is on VAT and other EU-related fraud.

Though it only started operating in June 2021, the EPPO has carried out almost 1,000 investigations so far, with more to come in the following years. Concerning Italy, EPPO investigations have recently led to:

- the seizure of EUR1.1 million from two Italian companies operating in the medical supply sector, following the allegation that they provided hospitals in Northern Italy with face masks and protective suits without suitable certification;
- the seizure of EUR2 million and the arrest of twelve individuals in relation to alleged fraud concerning EU agricultural funds in the Italian region of Sardinia; and
- the arrest of two public officials working in the field of social housing in Palermo and an accountant in relation to alleged unlawful inducement to give or promise money

concerning the renovation project of a social housing building.

In addition to the control carried out by the authorities, in the current system we can see that there is greater accountability for all those involved in the process of granting funding, who are called upon to conduct a thorough check as to the suitability of applicants to obtain funding, ranging from financial liability to criminal liability for complicity in the fraud committed by the applicant, in relation to behaviour that appears more of an oversight in compliance than actual co-participation in the crime.

One example of this type of accountability concerns the State, which, if it does not recover European funds obtained unlawfully by fraudsters, must partially reimburse the funding.

Further examples where liability extends beyond the main fraudster involve mergers and acquisitions of companies that have unlawfully benefited from public funds.

Given the fact that, in the case of a merger or transfer of a business unit, the acquiring company would become, in the former case, criminally liable pursuant to Legislative Decree No 231/2001 ("Law 231"), which establishes corporate criminal liability, or jointly and severally liable for the payment of a fine in the latter case, it becomes crucial, in the acquisition phase, to understand whether there are any risks of criminal corporate liability, to assess whether it is possible to proceed with the transaction and, if so, to create mitigants.

Tax credits

EU-level interventions, such as the NGEU, have been complemented by various national interventions, among which are a series of bonuses aimed at developing the construction sector, such as the "Renovation Bonus" and the "110% Superbonus scheme", which consists of a deduction of expenses incurred for the implementation of specific interventions aimed at energy efficiency and increasing building safety.

These incentives usually consist in tax credits, in which the subject carrying out renovation works advances the payment and later, by proving that he or she falls within the parameters to qualify for the bonus, will receive a tax credit equal to a share of the amount spent for the work carried out.

Tax credits are a type of public funding which may be transferred to financial institutions in exchange for cash, thus creating a secondary market, mainly managed by financial institutions, concerning the possibility of the beneficiary obtaining immediate liquidity from the relevant bonus through the transfer of the tax credit, for example, to whomever actually carries out the work or to a bank, against a reduction of what the beneficiary would have received if he or she had waited until the deadline set for obtaining the tax credit.

However, the main menace in this area is that the underlying credit may not be real, ie, not due (such as tax credit for fictitious construction work, R&D costs or other activities related to the NRRP). Therefore, there is also an investigative focus on the transfer of tax credits lacking those requirements under which the credit could have been granted in the first place.

The risk is that criminal liability could also extend from the transferor of the tax credit to those financial institutions which, in order to obtain the credit, did not make a proper assessment and thus accepted the risk of the wrongdoing.

Hence, once again, financial institutions should focus on credit due diligence, in order to double-check the legality of the credit which is being acquired.

In particular, if the underlying credit turns out to be undue, financial institutions would be held criminally liable together with the original beneficiary. If, on the other hand, the underlying credit was transferred after all the required functional checks were put in place to verify the beneficiary's claim, financial institutions would not be held liable if they were able to prove that they had effectively and thoroughly performed due diligence in this regard.

As is also the case for AML, in the area of public (national and European) funds too, Italy is witnessing increased pressure by the authorities on the private sector, especially the financial sector, as it is increasingly being called upon to play a role in monitoring the fairness of economic transactions.

Preventive Measures as a Means to Encourage Compliance Culture

The last trend that has been emerging recently is the increasing use, especially by the Milan Prosecutor's Office, of what is known as monitorship (*amministrazione giudiziaria*) under anti-Mafia legislation, which is being used as a means to encourage compliance culture in companies, though it was originally created as a sanctioning tool to permanently strip the Mafia of any ties with the economic world through the confiscation of assets, such as businesses used to launder the proceeds of illegal activities.

Monitorship is characterised by a streamlined enforcement procedure: in fact, for it to apply there is no need for a criminal trial to take place nor for criminal liability to be established, as it is a preventive action based on presumptive evidence which implies a burden of proof shared between the prosecution (who only have to prove the existence of evidence) and the affected party (who, when confronted with said evidence, has to prove its lack of involvement in the Mafia system).

Once a monitor is appointed by the court, they will try to bring the company back to its ordinary, lawful business activity, and make sure that such problems do not recur. If, however, following the period during which a company is monitored strong relations with the Mafia emerge, the company shall be permanently confiscated.

In recent years, the Milan Prosecutor's Office has used monitorship in a different way, not so much for the purpose of fighting the Mafia through confiscation, but rather as a temporary measure aimed at incentivising all those companies that have shown a poor compliance culture, which thus led them to have Mafia-related companies among their suppliers, to implement their own internal procedures so as to avoid further possible meddling in the future.

In this view, in fact, monitorship does not so much affect the Mafia-related company as those companies, part of the lawful production circuit, that have entered into contracts with suppliers or customers from the Mafia world and that, through the relationships established with these individuals, risk indirectly benefitting organised crime.

It has been noted that, in this case, monitorship acts as a response to the violation of normal rules of prudence, good business administrationand transparency, and is intended to last for a limited period of time, at the end of which the company would not be confiscated (as provided

for in the anti-Mafia regulations) but would be returned to the owners with a new, enhanced compliance capacity.

In practice, therefore, the use of this tool is often almost as an alternative to criminal trials under Law 231, as it achieves, in a quicker manner, the goal of strengthening compliance which might instead take longer within the context of a criminal trial.

Once again, as for AML and public funding, companies are required to implement strict internal control systems to detect not only the risks of "direct" Mafia infiltration, but also of indirect Mafia infiltration, through their suppliers and customers.

Therefore, similarly to how financial institutions are held liable for money laundering if their account holders commit this crime, as well as for the unlawful transfer or use of sham tax credits, companies may also be held criminally negligent for failing to provide an adequate internal control system.

Conclusion: A Shift from Punishment to Prevention

What emerges from this analysis is how, over recent years, there has been a shift from a punitive perspective to a preventive one in the area of white-collar crime, connected with a widening of the scope of corporate criminal liability with regards to companies and financial operators, resulting from the pressure put upon the latter by the authorities in order to carry out control functions over their business counterparts (eg, clients, suppliers, tax credit transferors) so as to discourage the commission of crimes and foster a culture of compliance.

Hence, it is fundamental that companies and financial operators properly assess risks and that there is continuous monitoring, so as to avoid any potential negative consequences which could have devastating impacts on their business activities.

In this regard, besides ensuring that compliance exists not only on paper but also in practice, entities should opt for an integrated approach to corporate compliance by adopting organisation, management and control models, such as the one provided for by Law 231, which are tailored to the specificities of each entity and which concretely interact with other compliance tools relating to the areas of, for example, privacy, supplier quality management (eg, ISO certifications) and sustainability (eg, sustainability reports).

A further push in this direction is given by the so-called "Crisis Code" (Legislative Decree No 14/2019), which requires companies to introduce "appropriate arrangements to prevent business crises", therefore, a coherent system that looks at both the financial soundness and the overall resilience of corporate compliance, which is no longer seen as an obstacle to business activity but rather as a guarantee for its continuation and as an additional stimulus.

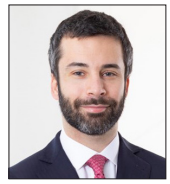
Therefore, with a view to ensuring effective and continuous monitoring and in addition to setting up a compliance system, it is essential that, should any compliance risks arise, entities proceed to carrying out internal investigations which, in order to achieve a balance between the need to conduct investigations and the risk of self-incrimination, should take the form of preventive defensive investigations, carried out by outside counsel, which provide a series of guarantees, such as secrecy of communications between client and counsel, a prohibition

against seizing the investigation reports and the probative value of the evidence collected, which could therefore be used if criminal proceedings are instituted.

Orrick, Herrington and Sutcliffe LLP is a leading international law firm with offices in over ten countries. The Milan team works with leading multinationals, financial institutions and investors, many of them listed on the Milan Stock Exchange, as well as SMEs, that play a key role in driving the Italian economy. It provides support on cross-practice, cross-border, corporate, M&A, private equity, compliance, and financial transactions as well as defending clients in their disputes, both in and out of court, particularly in the technology, energy and infrastructure, and financial sectors.

Authors

Jean-Paule Castagno is a partner in Orrick's Milan office and Head of the Italian white-collar criminal defence team. With more than 15 years of proven experience in criminal litigation, crisis management, internal investigations, and representation of individuals and entities before courts and supervisory authorities, Jean-Paule advises clients in high-profile criminal proceedings with specific reference to anti-money laundering, financial crimes, bankruptcy offences, tax crimes, corruption and bribery in both the public and private sectors, environmental crimes, occupational health and safety offences, intellectual property crimes, cybercrimes and vicarious liability of corporate entities. She is a member and chairwoman of the surveillance committees of many Italian and foreign companies.



Andrea Alfonso Stigliano is a senior associate in Orrick's Milan office and a member of the firm's white-collar criminal defence team. His activity focuses on criminal defence, internal investigations and regulatory enforcement. For over ten years, Andrea has represented entities and individuals in connection with criminal and regulatory investigations and proceedings. Andrea has extensive experience in cases involving anti-money laundering and trade sanctions, financial crimes, bankruptcy offences, tax crimes, corruption and bribery in both the public and private sectors, environmental crimes, occupational health and safety offences, intellectual property crimes, data protection issues and cybercrime. Andrea is a member of the International Commission of the Milan Bar Association.

Orrick, Herrington and Sutcliffe LLP

Corso Giacomo Matteotti 10
20121, Milan
Italy

Tel: +39 02 4541 3800
Fax: +39 02 4541 3801
Email: gtesta@orrick.com
Web: www.orrick.com

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com