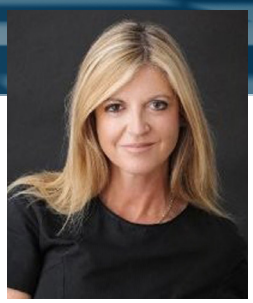
Client Alert:

Post-Brexit Fraud Considerations in the UK and EU

FEBRUARY 2021

By Sarah Keeling and Alexander Moss



Sarah Keeling
Partner, StoneTurn
skeeling@stoneturn.com
+44 (0)20 7427 0417

Alexander Moss
Senior Manager, StoneTurn
amoss@stoneturn.com
+44 (0)20 7427 0410

The last-minute scramble in the Brexit story has created unique and significant fraud risks.

Fraudsters and fraud schemes flourish whenever there is change or uncertainty. The massive regulatory changes that have been announced, and the many that are still emerging, mandate new processes and controls be put in place, in a condensed time frame. Required responses to these risks include re-examining risk assessments, considering whether existing controls and processes are adequate, and implementing steps for one-off consideration and approvals on emergency or urgent needs that (perhaps driven with fraudulent intent) will arise. This article outlines some specific possible risks and steps to address them.

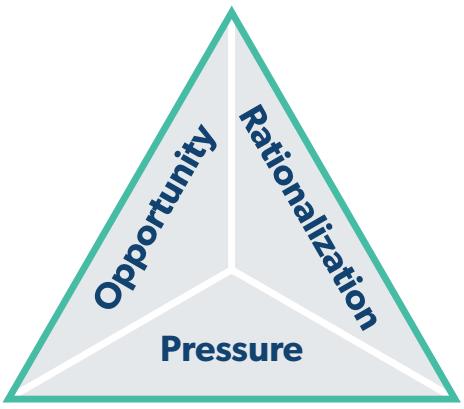
Supply chain risk is enhanced. Businesses may have to engage with new suppliers, either in the short-term to address customs and import issues, or on a longer-term basis as part of resetting within the new trading world. If a business needs to engage a new supplier, which may often be at short notice, it may enter a new relationship without performing appropriate due diligence, inadvertently exposing the business to corruption and money laundering risks. As is the case in more routine times, having a sufficient understanding of who you are dealing with—the corporate entities as well as the principals behind them—is a necessary protection. Rushed decisions, without sufficient knowledge, create unknown risks that may not surface for some time.

As businesses seek to retain access to markets in the EU and UK, they may be tempted to exaggerate future revenue streams, profits, or assets to raise

StoneTurn

capital or obtain loans. Financial misstatement or manipulation may start with a small adjustment to make results appear healthier. However, as the perpetrator feels under pressure to maintain the deception, one misstatement often leads to another. Although the risk of financial misstatement or manipulation cannot be eliminated, it can be reduced by leadership demonstrating a strong, ethical "tone at the top" and encouraging a questioning mindset at all levels of the organisation.

The fear of job losses may damage employee morale and loyalty, increasing the risk of misconduct. In addition, as businesses restructure and reallocate resources, there is a risk of funds being fraudulently diverted. Anyone has the potential to engage in fraudulent activity. According to Cressey's Fraud Triangle (named after the criminologist Donald Cressey), three conditions exist whenever misconduct occurs: (1) pressure or incentive; (2) a perceived opportunity: and (3) rationalisation of the misconduct. The uncertainty and disruption to business operations, due to Brexit, creates a higher likelihood of even the most trusted employees going rogue.



Suppliers are updating their processes as well, which may include changes to ordering, shipment or payment instructions. One of the most prevalent scams is for fraudsters to impersonate suppliers and falsely claim they are relocating overseas, and request that all future payments be made to a different bank account, controlled by the fraudster. Any changes to suppliers' details or the vendor master file should be examined closely and directly confirmed with the counterparty.

Another common scam is "CEO fraud"—also known as "Business Email Compromise"—whereby fraudsters, purporting to be from management, send a fake email to finance staff requesting an urgent payment. The fraudster may stress that the payment is confidential or time sensitive, to discourage the member of staff from verifying the payment. It is critical that employees are alert to possible scams, particularly while Brexit and the pandemic are causing unprecedented disruption. Staff should not be pressured into making urgent payments, even if the request appears to come from senior management. Furthermore, all requests containing new or updated bank details, should be independently checked before processing the payment.

As cybercrime becomes more sophisticated and widespread, it is increasingly dealt with by cross-border teams working collaboratively. An integrated strategy, spanning government departments and law enforcement agencies, is necessary to target cybercriminals, who operate across the globe. Following Brexit, enforcement professionals in the UK and EU face significant challenges in the detection and prevention of cross-border fraud. Brexit could restrict information-sharing among law enforcement agencies and place strain on these critical relationships. Therefore, companies need to examine their risks and controls in this critical area, understanding there may be gaps in the level of law enforcement capabilities.

Complicating matters further, as of 1 January 2021, the UK can no longer rely on:

- Fast track extradition under the European Arrest Warrant.[1]
- Participation in the management of Europol and Eurojust, including direct access to databases, such as the Secure Information Exchange Network Application (SIENA).

In addition, the UK can no longer access the European Criminal Records Information System (ECRIS), which allows authorities in one EU Member State to check whether an individual has any convictions in other EU Member States. The **EU–UK Trade and Cooperation Agreement** provides for an enhancement of the 1959 **European Convention on Mutual Assistance in Criminal Matters**—records will be exchanged within 20 working days of a request, whereas ECRIS operates under EU legislation which requires each country to respond within 10 days.

It is not all bad news, though. A possible benefit of Brexit to the UK Exchequer could be in the form of a reduction in the amount of "carousel" fraud. Also known as "missing trader" fraud, or "intra-community VAT fraud", carousel fraud is where fraudsters import goods from overseas, then sell them to domestic buyers, charging VAT. Once the goods have been sold, the importer does not remit the VAT, collected as part of the sale, to the government.

How can businesses protect themselves?

1. **Supply chain due diligence:** Certain industries are more likely to be impacted by Brexit than others, especially UK entities whose business models rely on supply chains located within the EU and vice versa. Businesses may need to look outside their normal supply chain to meet demand. However, they should not be tempted to cut corners when performing due diligence, thereby allowing transactions prior to the successful completion of formal vetting. Without access to previously available databases to vet politically exposed persons (PEPs) and high-risk individuals, companies may need to engage different resources to maintain acceptable levels of third-party risk. Furthermore, supply chain risk is likely to evolve over time—businesses should, therefore, continually monitor existing supplier relationships to identify risks as they arise.
2. **Be alert for possible scams:** Businesses must be alert to the threat of scams, such as the impersonation of genuine individuals or organisations to obtain personal or banking data. It is critical that businesses know who they are dealing with when entering a new relationship.
3. **Brexit health check:** Businesses need to proactively monitor the threat of fraud and ensure they have adequate controls in place, which are operating effectively. Businesses should assess the efficacy of their fraud controls, as a general "Brexit health check," and perform regular reviews, as a matter of course. In doing so, businesses must consider the impact of Brexit on the control environment, for example, diversification of operations and increased pressure on sales staff to meet targets. Other factors, such as increased remote working, may provide individuals with greater opportunity to commit fraud.
4. **Post-event assurance:** Fraud and corruption violations committed since the start of 2021 may not be immediately apparent, while businesses

are navigating the operational implications of the EU-UK Trade and Cooperation Agreement. The risk of misconduct going unnoticed is exacerbated by the ongoing disruption due to the COVID-19 pandemic. Businesses should, therefore, perform targeted post-event assurance to assess how their policies performed, identify potential instances of fraud, and determine what remediation may be needed.

5. **Anti-fraud training:** Businesses should make sure that employees receive adequate anti-fraud training, to enable them to recognise potential misconduct and respond appropriately. After all, previously acceptable protocols and behaviours may now pose significant risks to the organisation in light of Brexit. Employee anti-fraud training should be updated regularly to ensure that the content reflects the evolving relationship between the EU and UK.

Extreme change—such as the UK's departure from the EU—presents unique challenges and creates conditions in which misconduct can thrive. Fortunately, strong internal controls such as fraud risk assessments, vendor due diligence, and sound training and communication can help ensure businesses are best positioned to thrive in a post-Brexit world.

About the Authors

Sarah Keeling, a Partner with StoneTurn, is a former senior British government official with more than 20 years of experience in national security and intelligence matters in the U.K. and overseas. She assists companies, family offices and their counsel on operational, reputational and investment risk matters worldwide.

Alexander Moss, a Senior Manager with StoneTurn, has more than 12 years of experience in investigations, government advisory, internal audit and tax engagements. He has managed teams on several high-profile projects, both in the U.K. and overseas. Alex has worked on projects across various industries, including financial services, oil & gas, construction and the public sector, among others.

[1] The **EU–UK Trade and Cooperation Agreement** provides for an extradition system, known as 'surrender', to replace the European Arrest Warrant, although states can refuse to surrender their own nationals.