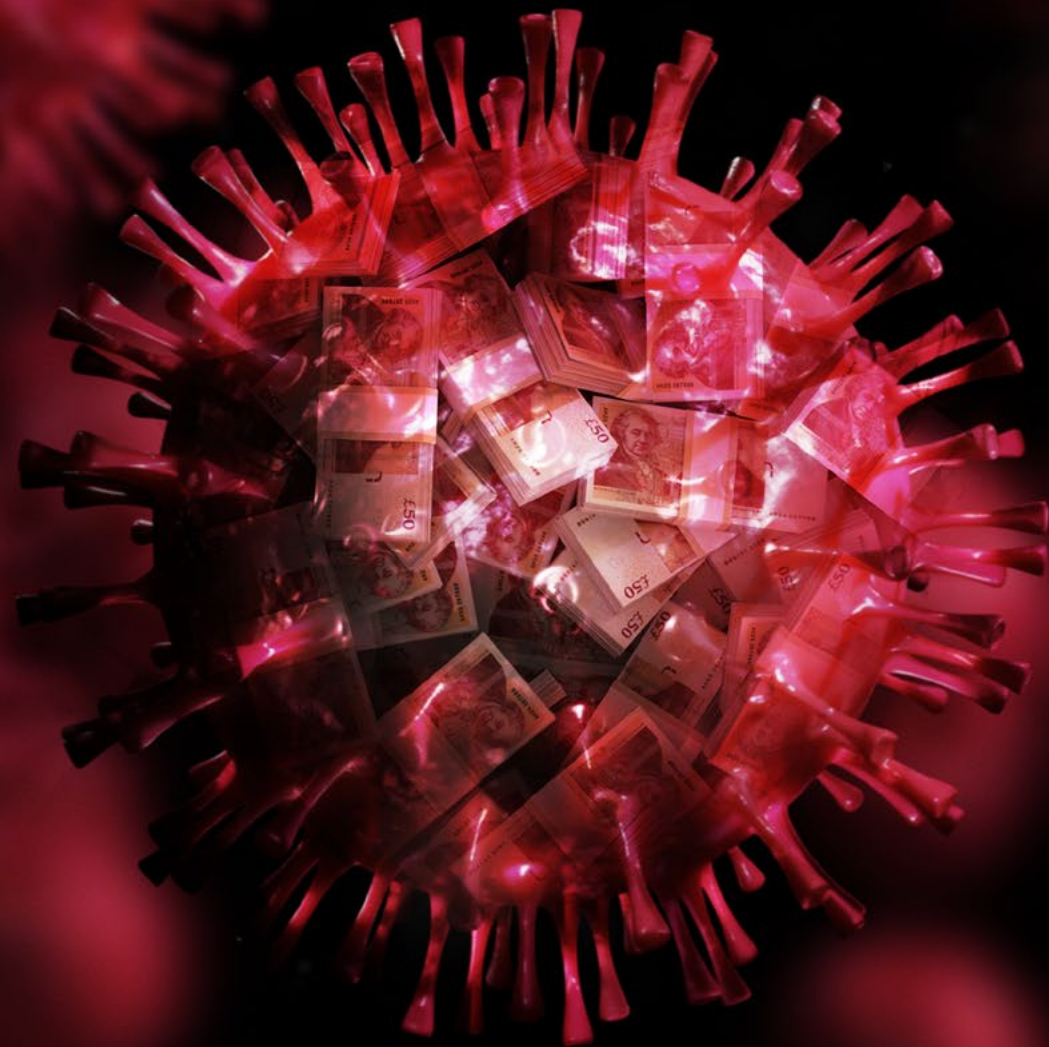


FACING!► CHANGE

How is COVID-19 altering the financial crime risk landscape and what can we do about it?







The global pandemic has caused a crisis of epic proportion and has led to unprecedented global challenges: deaths, suffering, economic disruption and an increase in COVID-19-related crimes.



But for criminals, crisis and chaos creates the perfect conditions to target weaknesses and exploit the most vulnerable. In May, the Financial Action Task Force (FATF) warned that “*measures to contain COVID-19 are impacting on the criminal economy and...profit-driven criminals may move to other forms of illegal conduct.*”

It's the perfect storm for criminals. Not only are opportunities rife, but security is compromised:

 Law enforcement... ...may be distracted from supporting humanitarian aid and maintaining social order.	 Financial intelligence units... ...face limited capacity due to people being furloughed or reassigned, and are even closed down in some countries.	 Supervisory authorities... ...no longer able to conduct on-site investigations, are reduced to desktop investigations.	 Compliance teams... ...trained to detect unusual and suspicious activity are having to re-evaluate what exactly is unusual and suspicious in the face of such change, while at the same time being forced to work remotely at home, in often challenging circumstances and employing online verification and authentication tools that they're not familiar with.
---	---	---	--

There is a real risk that we allow criminals to syphon money out of our economy that could otherwise be put towards healthcare or government support schemes. By allowing financial crime and fraud to take place, we're also permitting criminals to take advantage of vulnerable individuals and gain control of important institutions within our community: the buildings we live in, the shops we buy from, the restaurants we eat in, the professional services firms we rely on and trust.

In this guide, we explore the emerging financial crime and fraud threats we're seeing and consider how organisations can best support their teams to recognise the patterns and signs of criminal activity, to protect their customers and their own business reputation, as well as safeguarding wider society.

The pandemic increases existing vulnerabilities and creates new ones.



The coronavirus outbreak is making society's vulnerable more vulnerable: those who are abused, exploited or in need of support suffer behind closed doors.

For example:



Child and domestic abuse cases are reportedly rising, at the same time as becoming even harder to detect, as abusers are locked down with their victims and people's movements remain restricted.



Victims of human trafficking are at a higher risk than ever – a disrupted supply chain means labour populations are more valuable and more vulnerable to exploitation through overwork, underpay and a lack of appropriate safeguarding.

The virus outbreak also creates newly vulnerable people:



Many who would have considered themselves financially secure at the start of 2020 may now have recently lost their jobs and therefore incomes, plunging them into poverty.



Those who are 'new to digital' are finding they need to use devices to manage their finances and shop online for food for the first time ever, exposing them to systems processes they're unfamiliar with.



Those who are shielding, suddenly find themselves relying on others to provide them with care and provisions.

Members of the Financial Action Task Force (FATF) and FATF-Style Regional Bodies (FSRBs) note that, in a prolonged economic recession, those with financing needs may seek out non-traditional or unlicensed lenders, which may include criminal groups, further exacerbating people's predicaments.

Criminals use the crisis to exploit vulnerabilities in people and systems.



Preying on vulnerable groups, such as the young and the over 70s

Lockdown has spurred a massive surge in domestic online activity and transactions. A significant number of users are 'new to digital', including the elderly, minors and digital 'sceptics'. These users, often characterised by a lack of experience and 'online savviness', are particularly vulnerable to scams and online harm.



Preying on people's need for information and provisions during isolation

FATF warns of criminals attempting to profit from COVID-19 through activities such as impersonating officials, counterfeiting, including essential goods, and fundraising for fake charities and fraudulent investment scams.



Preying on people's need for vital services

Interpol's Cybercrime Threat Response Team has detected a significant increase in attempted ransomware attacks against key organisations and infrastructure engaged in the virus response.¹



Preying on government stimulus measures and support packages

FATF and FSRB members report that economic support directed to businesses and individuals may present potential fraud risks, and consequent money laundering. In particular, criminals can falsely claim to provide access to stimulus funds to obtain personal financial information. Criminals may also use professional enablers to make fraudulent claims on government stimulus funds by posing as legitimate businesses seeking assistance.



Preying on individuals and companies desperate for financial support

Criminals are preying on people's desperation and vulnerability as a result of losing their income, recruiting them as money mules to move illicit money. Individuals and businesses on reduced incomes are also being targeted by loan sharks. In addition, organised crime gangs will use the opportunity to recruit support and increase their power.



Exploiting migrants and other vulnerable workers

FATF warns that the shutdown of workplaces, slowdown in the economy, rising unemployment, and financial insecurity are all factors that could result in an increase in human exploitation. The suspension or reduced activity of government agencies regularly engaged in detecting human trafficking cases and identifying victims, means that cases may go undetected.



Exploiting drug addicts, desperate for supplies

Dealers are circumventing lockdown restrictions. Gangs are finding new routes to market. County lines gangs are recruiting online, using social media to groom their targets, and spiralling drug costs force end users to commit more petty crime to raise the funds and keep their supply flowing.



Taking advantage of the chaos in financial and compliance systems

Criminal groups and even some legitimate but fraught businesses may attempt to take advantage of the crisis to circumvent controls and introduce illicit proceeds into the financial system. FATF members highlight tax evasion and related crimes, as well as illicit corporate and financial market activities, such as market abuse and insider trading.

Online shopping fraud has risen by **46%** since the start of the lockdown, "making it one of the biggest crime growth areas" in the UK.¹

By early May, over 500 coronavirus-related scams and over 2,000 criminal phishing attempts had been reported to UK fraud authorities, with total losses estimated at **£1.6 million**.¹

How to spot the unusual when everything is unusual.

In the current environment, there will be many legitimate businesses who are desperate – suffering from a lack of business and lack of cash flow; facing closure – who will be approached to help launder the proceeds of crime. Their vulnerability puts them at higher risk of being coerced into activity they may know doesn't feel right, but they might turn a blind eye to save their business. The same goes for individuals facing unemployment and economic hardship.

Likely targets

The type of businesses likely to be targeted can vary but they're often cash-intensive and at present, will be those whose revenue is most impacted by lockdown. It might be a restaurant that is surviving on takeaway business only and is struggling to make ends meet. It could be a nail, beauty or hair salon, a tanning studio, a chip shop or a small manufacturing business whose production has been interrupted. It could be a small family law firm, whose partners have put their life's work into their business and face losing it all.

Commercial property is at risk too. With millions of people out of work and struggling to make ends meet, landlords may well be struggling to collect rent from their tenants. Meanwhile their utility bills, council tax, and business rates stack up. Criminals may see this as an opportunity to acquire property at a bargain price, whilst also acquiring a legitimate business interest through which they can launder cash under the guise of 'rent payments in cash,' 'maintenance costs,' 'staff wages' and so on.



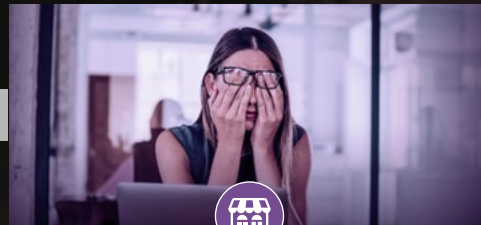
“Be alert, look at the risk and make sure you know who you’re dealing with.”

Michiel van Dyk – UNODC

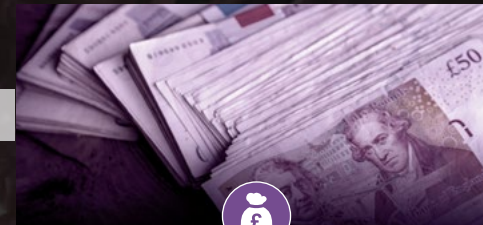
How a gang might approach a business to launder money:



Criminals give cash to runners to buy up large volumes of low-value prepaid cards.



They target businesses in dire straits, asking them to help them place large amounts of cash, as a 'favour'.



They offer to give the business (for example) £10,000 in cash and prepaid cards, which they can use to buy goods and supplies, pay wages and rent.

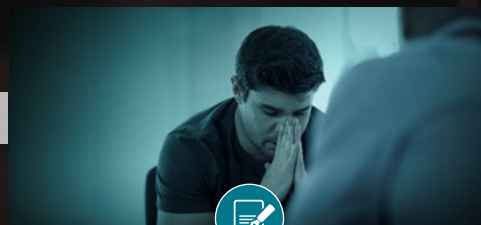


In return, the business writes £9,000 worth of cheques to the criminals, disguised as 'delivery services', 'repairs', 'logistics' and so on.

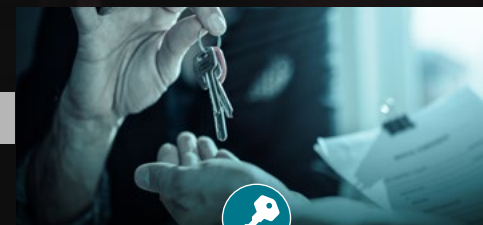
How an organised crime group might approach commercial property owners to launder money:



The criminal approaches a landlord they believe may be struggling to collect rent or is struggling financially.



They make an appealing offer such as: 'I know your property would have been worth £1m a year ago but you probably couldn't sell it at all now, so I'll give you £700,000 for it.'



They sweeten the deal by offering to declare the sale as £400k to avoid higher taxes and give the rest to the property owner as cash.



They 'raise' rents, increase maintenance costs and give 'wage increases' to employees, giving them 'legitimate' routes to launder large sums of cash through the business.

What are the warning signs that companies should be looking out for in this environment?



The good news is that, despite an ever-changing landscape due to COVID-19, nevertheless, standard methods of due diligence are still effective. Public records, adverse information checks and research into individuals and business ownership are all still valid ways to determine who you're dealing with, but companies do need to be extra vigilant at this time.

Apply a COVID filter, be extra critical and look twice for the unusual. For example:



Has the company been set up recently?

Do they have a website and has it been created recently? Has a business address been provided and if so, is it a genuine physical address, not a PO Box or mail servicing facility? Be particularly vigilant for third sector fraud: charities and trusts.



Would you expect the business to be taking revenue at this time?

Use your knowledge of current industry conditions and government restrictions to ask who is falling outside of the expected parameters: would you expect this business to be generating income or spending money and carrying out transactions at this time? And at the levels you're seeing?



Is the company operating in an industry segment that's experiencing surges in activity?

Entertainment businesses, online casinos and gambling platforms, dealers in precious metals and stones, and crypto exchanges are all seeing a surge in activity in the current environment, so might represent good targets for criminals looking to disguise their activity and launder their funds.



Has the company recently been acquired?

Look carefully at the corporate ownership structure. Who's buying the business? What else do they own? Who else are they involved with and do they have adverse media against them? Are they claiming government support/funding for businesses that they don't actually own, or affiliations with businesses that don't exist?



Are customers making frequent changes to their account information, or displaying unusual behaviour?

Particular attention needs to be paid to customers or entities making multiple transfers to third parties who have not previously been seen, or to jurisdictions where the customer has no known ties.



Is the customer moving funds around using alternative payment providers?

Criminals are particularly fond of alternative payment providers, such as digital wallets, money service bureaus or prepaid cards, which provide banks with a narrower view of transactions and make it harder for their controls to detect illicit activity.

What should companies do if irregularities are found?



If you find irregularities, follow the trail; follow the money. It's the route to detecting organised crime networks. Rarely do illicit organisations operate in isolation. Once you find one illicit business or activity, the money trail, the digital trail and corporate or ownership structures will typically lead you to additional illicit businesses and criminal organisations. Check whether a pattern of potential illicit activity stretches out to their networks beyond the initial company or operation.

To summarise, today more than ever businesses need to know who they're dealing with – effective customer due diligence has never been more important:



Throughout the customer journey, not just at onboarding

It's more important than ever to conduct thorough due diligence on customers and entities, both at onboarding and also on an ongoing basis as they continue to transact with the business. Circumstances can change quickly in this environment and it's important to recognise that customers may be the victims of identity theft, as a result of the many scams and cybercrime attacks in operation. There is also a risk that they are compromised – acting as mules or otherwise providing a conduit for money laundering.



Look beyond the individual or entity to their ecosystem and close associations

Who are their associates? Who's in their network? What other businesses do they own? Which other businesses and business owners are they linked with as part of corporate ownership structures and supply chains?



Look below the surface

Basic internet search engines only trawl the surface web and are not sufficient. Criminals will have covered their tracks. They will have exercised their right to be forgotten. An in-depth adverse information search is required, to uncover adverse news, CCJs and other blemishes on their record.

Protect your customers, protect your business, protect society.

LexisNexis® Risk Solutions is here to support you in protecting your customers and your business from the threat of financial crime and fraud. Our combination of trusted data, advanced analytics and intelligent technologies can form a keystone in your financial crime and fraud defences; enabling you to identify potential fraud, verify and authenticate customer identities, screen for politically exposed persons (PEPs), sanctions and adverse information, monitor customers on an ongoing basis and support your enhanced due diligence for clients who present a higher risk.

Through a single trusted relationship you can help protect your organisation and customers from financial crime and fraud:



Fraud Prevention

Keep fraudsters out of your business

In many cases, businesses use traditional identity data and documents to verify an individual. However, with our unique digital identity capabilities, we can add a new and increasingly important dimension to identity assurance and fraud prevention processes.

Incorporating digital evidence (such as users' device attributes, account activity and behavioural biometrics), to substantially increase levels of confidence that the person presenting actually exists (i.e. is not a synthetic identity) and that they are who they say they are, as well as being able to raise alerts for risk factors (e.g. previous frauds linked with the digital devices used by the individual, or changes in the way the person interacts with their device, which would suggest they might not be the same person), our combination of physical and digital identity attributes, will help you stop criminals getting access to services they shouldn't.

Digital Footprint:

Identify any potential fraud risk by evaluating online behaviour associated with the presented identity. Our global digital identity network aggregates more than 30b global transactions annually including logins, payments and new account opening.

Email Risk:

Assess the level of fraud risk associated with a provided email address. Our global contributory fraud database contains more than 40 million email addresses connected to fraud.



Identity Verification & Authentication

Ensure you're dealing with the right person

Identity checks usually verify individuals against a combination of electoral roll and credit reference data. However, these data sources won't capture all of the population and in the UK, somewhere between 10-15% of individuals cannot be verified using traditional data suppliers.

LexisNexis Risk Solutions reduces the shortfall by providing market leading data coverage of the UK population, simultaneously searching the data of 2 of the UK's 3 leading credit bureaus, alongside our proprietary database of UK consumer records.

Over and above this, we offer a variety of supplementary checks such as identity document authentication, facial biometrics and two-factor authentication to provide an additional level of confidence in an individual's identity; crucial when there is insufficient information to complete a data-driven identity check.

Quick:

Online identity verification, which checks multiple trusted information sources (including physical and digital data attributes) via a single platform, minimising customer friction.

In-Depth:

Confirm the claimed identity belongs to the presenting client through electronic document authentication and supplementary checks, such as facial biometrics.

Easy-To-Use:

Results clearly highlight whether the customer has passed or failed, or if more information is required.



Financial Crime Risk Screening

Identify the potential risk associated with the customer

As the pandemic has reinforced, risk evolves rapidly. Yesterday's low risk, model customer can suddenly become today's high risk entity. We can notify you of emerging risks at the earliest opportunity via our financial crime screening capabilities. Drawing on a market leading, globally curated, financial crime risk database, our screening and monitoring engine is relied on by some of the world's largest banks to flag business relationships which present a risk at the earliest possible opportunity and allow for the risk to be investigated. A transparent audit trail, helps you to evidence your robust procedures and controls to relevant regulators.

Ongoing Monitoring:

Stay alert to your customers' evolving risk profiles by monitoring them on a regular basis. Our solutions will automatically notify you when there is any change in the risk associated with your customers.

Global Risk Data:

PEPs, sanctions, adverse media and enforcements. Our proprietary risk dataset is updated 24/7 by our global team of 400+ researchers who are fluent in 57 languages.

Bespoke Screening:

Configure the data matching tolerance to align with your level of risk exposure, to reduce unnecessary 'false positive' matches.



Enhanced Due Diligence

Investigate higher risk entities

Through enhanced due diligence you can attain a clear understanding of a high-risk customer's individual circumstances, and unpick the inherent risk in their eco-system of associations. Our desktop-based research tools will help you to scrutinise higher risk entities against a wealth of UK consumer records, international business and corporate registry information and global financial crime risk data.

When the level of risk requires an even deeper dive into the entities background, you can call upon our team of professional researchers to create bespoke, in-depth enhanced due diligence reports.

Ownership Data:

Identify ultimate beneficial owners and persons of significant control, and understand the risk associated with them.

Corporate Structures:

Explore corporate structures, understand ownership, investigate relationships and evaluate the level of risk posed by a business and its stakeholders.

Unique Combination of Data:

Access extensive business, consumer and financial crime risk data, and conduct adverse information searches of the deep web, via a single platform.

Find out how you can combat financial crime more effectively – call our team today on **029 2067 8555** or email **ukenquiry@lexisnexis.com**

Protect your customers, protect your business, protect society.
For more information, please call 029 2067 8555
or email ukenquiry@lexisnexis.com

risk.lexisnexis.co.uk



About LexisNexis® Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers across industries. For more information, please visit risk.lexisnexis.co.uk and www.relx.com.

LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. Other products and services may be trademarks or registered trademarks of their respective companies. No part of this document may be reproduced without the express permission of LexisNexis. LexisNexis Risk Solutions UK Ltd is a company registered in England & Wales at Global Reach, Dunleavy Drive, Cardiff CF11 0SN. Registration number 07416642. Tracesmart Limited is a LexisNexis company, operating under the trading name of LexisNexis, with an England & Wales Registration Number 3827062. Registered Office is Global Reach, Dunleavy Drive, Cardiff CF11 0SN. Authorised and regulated by the Financial Conduct Authority (Firm Reference number 742551).