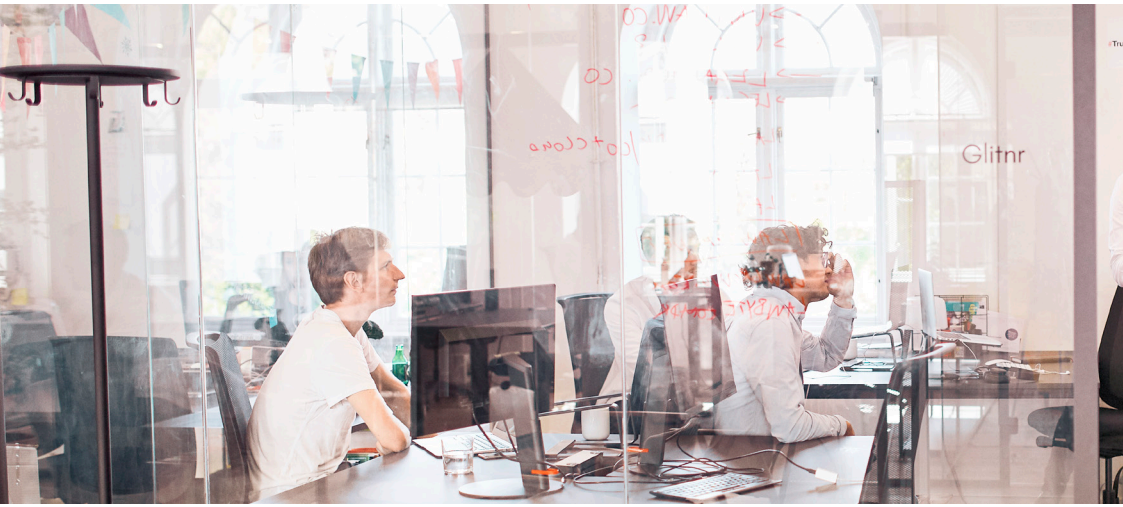
Financial Crime Awareness Guide

Protecting your business

– and realising your growth aspirations

Danske Bank



Financial Crime Risks: Safe, diligent and rewarding international expansion

Globalisation offers potential upside, but comes with additional risks

There are ever more business opportunities available as it becomes easier to engage with international trading partners. However, it is essential, as with any business relationship, that there is mutual trust. Doing thorough research into potential partners can help ensure growth opportunities, foster a good commercial relationship, and establish the foundation for a trustful relationship. This can be challenging when the parties concerned are separated by perhaps thousands of miles, different cultures, business practices, languages and limited face-to-face contact.

Potential buyers and suppliers may offer new sales and supply opportunities, but in return can bring new types of risks to the table - risks that we are not normally as aware of. In this brief guide we will cover some of the things to consider in order to tackle the financial crime risks you may become exposed to.

Importance to tackle Financial Crime risks is ever growing

Financial crime takes many shapes and

has many repercussions from loss of own monetary or informational assets to unintentionally helping others perform their criminal activity. Either way, the result can be extremely harmful for businesses and individuals - with wide monetary and reputational implications – not to mention broader adverse societal impact.

According to the UN, the estimated amount of money laundered globally in one year is in the range of 2 – 5% of global GDP, equivalent to $800 billion – $2 trillion US dollars. We can and must each play a role to counter the crime resulting in this staggering amount. As the fight against financial crime continues, forward-thinking organisations work diligently to ensure that they have the necessary tools, practices and controls in place to help protect them and others against being misused for financial crime purposes.

Financial Crime poses an ever-growing risk for businesses and financial service providers worldwide.

With this brief guide we want to share an overview of some of the Financial Crime risks which may be encountered and to share thoughts on how your organisation may take steps to protect itself.

In doing so we hope to continue to work together to strive for a safer business environment, increase prevention of Financial Crime and raise awareness of these risks.

Protecting your business

Fighting financial crime is an ever-evolving challenge as criminals innovative their approach for their own illicit purposes. Whilst the vast majority of trading counterparties are legitimate, any risky or criminals among them can sometimes be difficult to identify.

It is important to understand your financial crime risks and to have appropriate controls in place to detect and manage these risks. Awareness can come in the form of 'red flags', which may indicate that a counterparty is acting suspiciously or trying to abuse your products or services. 'Red flags' may also help you to apply a 'risk-based' approach towards your controls.

In this brief guide we have gathered some of the potential scenarios to be aware of and, if identified, you may decide to take further steps to understand and mitigate any risks that you may be exposed to.

We have included some examples to help illustrate these risks as well as some general questions to ask yourselves regarding your current processes that may identify areas of control improvement. Moreover, you may also want to consider if training programs and clear documented procedures would help ensure that everyone in your organisation is aware of these risks – and what to do if they encounter them.

Financial Crime risk may be posed by...

Anti Money Laundering

- Descriptive term regarding money coming from criminal activities and being 'cleaned' by putting it into the financial system
- Typically achieved via, multiple and quick transfers of funds over borders, buying and selling assets, making investments etc.
- Goal is to keep origin of the 'laundered money' as opaque as possible
- Cash-based businesses are considered as high risk for money laundering
- *Example: Funds from drug trafficking are used to purchase consumer goods or other products from an unwitting supplier. These goods are subsequently sold and their illegal origins are thereby concealed*

Sanctions & Embargoes

- Sanctions & Embargoes are political instruments put in place against certain countries, persons and entities to maintain or restore international peace and security. They operate and are enforced on a strict-liability basis
- Businesses have a legal obligation to comply with sanctions, and must check whether any business activity they carry out involves - directly or indirectly - counterparties, jurisdictions or activities that are subject to sanctions restrictions
- Failure to comply with restrictions has severe financial, legal and reputational consequences
- *Example: A factory providing parts to your final product is partly owned by a person who is targeted by sanctions. You must understand and carefully assess the sanctions risk and assess whether it is safe to do business with the entity*

Fraud

- Criminals try to take advantage from their victims by getting access to their bank accounts, diverting payment streams, steal their identities etc.
- Fraud is not limited to external criminals, it can happen from within your organization as well
- *Example: Opening phishing e-mail and entering bank data, giving criminals access to the bank accounts of the firms*

Bribery

- Bribery is illegal in many countries and may start at seemingly kind gestures such as being sent a considerate gift
- Breaking bribery laws in one international subsidiary or through a business partner may make your company liable to prosecution in its domestic market
- *Example: Paying a ship inspector for faster processing or clean reports*

Establishing a Business Relationship

Feeling safe with your trading partner
As with domestic activity, there is always the possibility that a potential international partner may not be all that they claim to be. Vigilance and careful scrutiny are advisable in dealing with trading partners to minimise risks.

Your business may not be 'directly' involved in any type of financial crime, but choosing a business partner who is may damage your reputation as well as theirs. Moreover, there can also be legal consequences to unknowingly participating in financial crime.

A standardized approach to vetting trading relationships may be beneficial in assessing the risks you may face – with new as well as well-established relationships. It is helpful to know in advance, how much risk you are willing to take on as a business in regards to types of counterparties, geographies, industries etc. This will help you determine the steps to take when you are faced with new opportunities or changes in existing relationships.

Red Flags to be alert to

- Trading counterparty is reluctant to provide clear answers or documentary evidence to routine questions
- Pressure or aggression is being applied when you ask questions
- There is adverse media available on your counterparty including social media exchanges about their activities and dealings
- counterparty's address cannot easily be found online or multiple companies registered to the same address for no good reason
- counterparty's online presence (website) does not look professional or genuine and seems to be generically 'off the shelf'
- Your trading relationship with this customer does not seem aligned with their stated strategy and business purpose
- Your customer wishes to settle invoices in overly complex ways, such as complex payment routing or using intermediaries

Practices to consider

- Standardise Know your Customer (KYC) due-diligence processes:
  - Understand who owns and controls your counterparty
  - Understand their business model, source of wealth or income
  - Be aware of any adverse media related to them
  - Does their online presence match your understanding of them
- Document a risk appetite and understand your boundaries regarding types of counterparties, countries and industries, etc.
- Apply and use internal risk ratings (high, medium and low) for your customers based on their apparent risk profile
- Always strive for face to face meetings to access your customer
- Be aware of the risks you face in different countries by consulting governmental lists and websites

Questions to ask yourself

- Are your due-diligence processes on international customers more thorough than on domestic customers?
- Do you know anyone who could vouch for this new counterparty?
- Do you understand the country risks associated to where your customer is based and operates?
- Do you have concerns about any of your trading counterparties?
- Do you understand the background of your counterparties, and do you keep detailed records?
- Have you met your existing trading counterparties, and can you vouch for them?

Maintaining a Business Relationship

Staying safe with your trading partner
It is sound business practice to be vigilant and to continue to understand your counterparties' behaviour and practices as well as to notice any changes that may influence the way they operate.

Areas of interest for you can include the industry they operate in, who their customers and suppliers are and the channels they use to sell their goods or services. A trading partner changing behaviour can give rise to reconsider your relationship – and potentially be a sign that your risk exposure is changing. Potentially you should update your assessment.

If, for example, the trading partner suddenly pays you from a sub-contractor from a third country, you may want to re-assess the risk of the customers and learn more about why this is happening. It could be a sign of money laundering, as routing money across national borders is more difficult to trace and therefore could be a means of money laundering.

Red Flags to be alert to

- Transactions are not in keeping with their business strategy
- Discrepancies between invoices issued and payments received
- Purpose of the payment is unrelated to the invoice issued
- Payments from natural persons for corporate counterparties
- Overpayments from counterparties with no good explanation
- Payments from 3rd parties with no apparent relationship to your counterparties
- Unexplained changes to payment instructions
- Use of personal account instead of business account to pay invoices
- Use of cryptocurrencies without a business rationale

Practices to consider

- Have a payment policy related to 3rd party payments, payments from high risk countries and payments in cash.
- Share openly your payment policy with customers and counterparties
- Implement controls to check incoming payments from customers with sign-off protocols in place (e.g. maker and checker)
- Be curious, ask probing questions of your customers transactions if they do not look right
- Have escalation processes in place if your employees are concerned about anything they see
- Implement ongoing refresh processes to maintain information you hold on your customers

Questions to ask yourself

- How many layers of controls do you have around payment processing and do your employees know what is acceptable?
- Do you have a robust procedure for trade documentation?
- Are you confident that your sales activities cannot be considered bribery?
- Are you aware of money laundering risks associated with high risk countries?
- Have you considered how your products or services could be exploited for financial crime or sanction breaches?
- Are you receiving queries from your banks about your transactions with your trading counterparties?

Further Reading

At Danske Bank we are committed to supporting you in achieving your ambitions domestically as well as internationally. We hope this brief guide into the financial crime risks can help you consider some of the things that are important to protect yourself and others.

We encourage you to read more about this important topic. Please have a look at the resources on the next page.

Disclaimer:
The information contained in this brochure is provided for informational purposes only, and should not be construed as legal advice on any subject matter. You should not act or refrain from acting on the basis of any content included in this brochure without seeking legal or other professional advice.

How Danske Bank works with financial crime prevention

https://danskebank.com/about-us/corporate-governance/compliance/fighting-financial-crime

More on Anti Money Laundering, Country Risk and Sanctions

Financial Action Task Force (FATF)
https://www.fatf-gafi.org/

Transparency International
https://www.transparency.org/en/t

OFAC
https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information

Reference guide on AML from Worldbank
https://openknowledge.worldbank.org/bitstream/handle/10986/6977/350520Referenc1Money01OFFICIALOUSE1.pdf?sequence=1&isAllowed=y

Supranational risk assessment of EU commission
https://ec.europa.eu/info/sites/default/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union.pdf

EU 4th and 5th Money Laundering Directives
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32018L0843&from=EN
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN

EU Restrictive measure (sanctions)
https://ec.europa.eu/info/business-economy-euro/banking-and-finance/international-relations/restrictive-measures-sanctions_en

Danske Bank A/S
Holmens Kanal 2-12
DK-1092 København K

CVR No. 61 12 62 28-København
danskebank.com