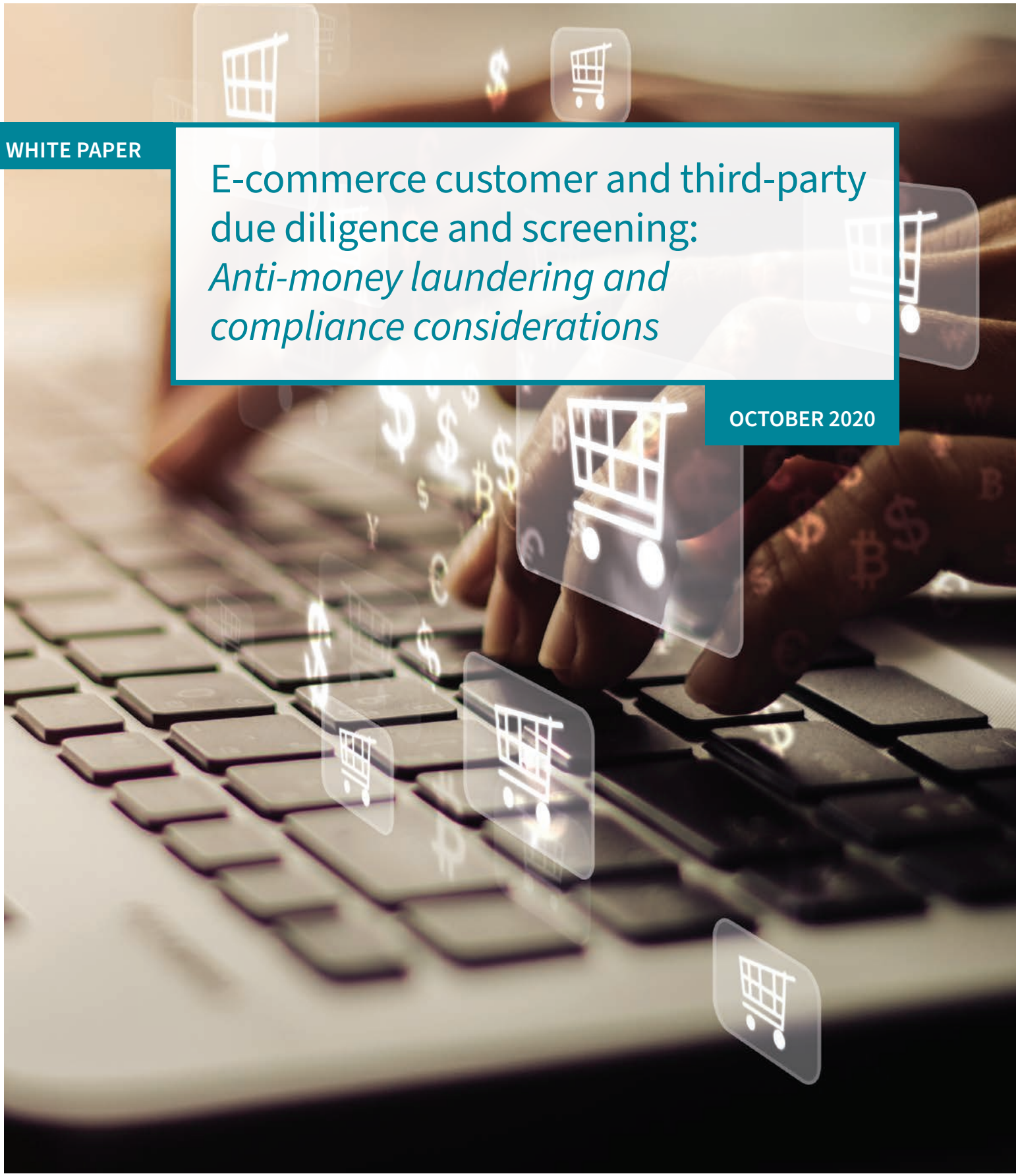
LexisNexis®
RISK SOLUTIONS



WHITE PAPER

E-commerce customer and third-party due diligence and screening: *Anti-money laundering and compliance considerations*

OCTOBER 2020

E-COMMERCE AML AND COMPLIANCE CONSIDERATIONS

Why is anti-money laundering (AML) so important for e-commerce businesses?

Businesses and e-marketplaces develop relationships with a number of entities and third-party suppliers to fulfill their needs and business goals. Maintaining transparency in those relationships as well as ensuring a risk-free customer portfolio is the ultimate goal for these businesses. In order to maintain ethical and compliant business practices, businesses selling goods and products in a more global market need to ensure effective due diligence on not only their customers but also on their trading counterparties. However, many companies tend to disregard that the exposure to risks is not only limited to their customers. The reality is quite different as inherent risks can also arise from business counterparties.

What is the goal of AML customer and third-party screening?

The purpose of customer and third-party screening is to find out whether your customers and/or third-party suppliers are, or could be, involved in any financial crime activity. Protecting your business by taking the right due diligence steps and a subsequent course of action is critical.

AML screening is the critical action that will ensure your business doesn't get involved in or serve as a vehicle for illicit money.

As regulation regimes continue to increase around the world, regulators have significantly tightened their enforcement actions leading to more substantial non-compliance AML laundering fines. Subsequently, the range of businesses that are required to carry out Know Your Customer (KYC) and AML checks is rising. If a business doesn't take the right compliance approach—thinking that they may never come across the wrong customers or third-party suppliers—the business can be exposed to reputational financial risks and severe penalties. Hence, if your business is utilized by criminals as a vehicle to clean their illicit proceeds of crime and becomes part of an investigation, regulators will undertake a rigorous assessment of your existing AML and KYC controls to ensure you are taking the right steps to stay compliant.

AML procedures and controls can be time consuming and, in many instances, costly. In order to stay at the frontline of combating money laundering and the financing of terrorism, ensuring effective policies, controls, human capital and the right AML screening and monitoring technology is key. By taking these steps, your business can be protected—and it will instill complete confidence to stay compliant and waive off any exposure to fines or reputational risks.

Customer and third-party due diligence

Due diligence is the process of assessing the extent to which a customer or business partner exposes a business to risks and breaches of sanctions regulations. This process is usually conducted not only before entering a relationship, but periodically to actively monitor any changes. Like customer due diligence, third-party due diligence should be an ongoing process. Business partners should be thoroughly assessed throughout the entire sales process as well as their relationship with other business parties to ensure that their risk profiles have not changed.

Businesses need to know who their customers and business counterparties are for a number of reasons:

- To comply with the requirements set out by domestic laws and regulations
- To be reasonably certain that customers and business counterparties are who they say they are and that it is safe to do business with them
- To fight against fraud, including impersonation and identity theft
- To help identify and assess, during a continued relationship, what is unusual in order to take the necessary actions when it occurs
- To assist law enforcement bodies by providing available and accurate information on customers and business counterparties being investigated over the course of an enforcement investigation

The most prominent customer due diligence requirements are set out at the European level by the current Fifth European Union Anti-Money Laundering Directive[1] and internationally by the Financial Action Task Force (FATF) Recommendations[2].

Business-to-Business (B2B) and Business-to-Customer (B2C) relationships

B2B and B2C relationships are the most common business relationships. B2B relationships can be sometimes overlooked compared to B2C relationships. Both types of business relationships may involve the same level of risk.

A B2B relationship involves business partnerships, affiliations, mergers, online merchants, third-party vendors, suppliers, transporters and others. These varied relationships can generate a lot of revenue but can also imply certain risks. Wherefore, businesses are required to carry out Know Your Business (KYB) due diligence on their business counterparties as well as an effective verification of customers.

What is KYB and how it is performed?

KYB is the due diligence practice on a business counterparty given in a B2B relationship. KYB entails a regulatory obligation for businesses in conjunction with fraud prevention practices. Carrying out KYB due diligence includes:

- **Verification of business data and registration documents of an enterprise**
- **Background AML screening:**
  - Screening for risks specific to the industry sector in which it operates
  - Global watchlists screening including sanctions, enforcement lists against entities or individuals by government and international enforcement bodies
  - Negative news—adverse media screening against entities and individuals
  - Politically Exposed Person (PEP) screening to assess political and influential connections that may expose your business to a higher risk of money laundering or bribery and corruption
  - Third-party vendors, distributors and suppliers screening. Business counterparties in any of their forms must be continuously assessed and reviewed by any business to ensure they are risk free, still meet the initial criteria and that there are not regulatory concerns around them
- **Verification and screening of Ultimate Beneficial Owners (UBOs)**
- **AML screening across the entire business**

KYB can be undertaken manually or through a specialized KYB screening solution provider. The best way to avoid any potential risks is to conduct KYB screening through a comprehensive automated screening solution that provides best-in-class and reliable global risk data. An AML screening tool can perform real-time and ongoing KYB screening on your business counterparties while providing effective risk and compliance management to stay compliant and minimize financial crime risks. By using an automated screening technology, businesses are likely to stay away from any risk exposure.

AML screening and technology considerations

From a technology point of view:

As sanctions checks are required to stay compliant with due diligence regulatory requirements, businesses must rely on solid technology to screen their entities efficiently and in accordance to the Anti-Money Laundering and Counter Financing of Terrorism (AML-CFT) rules.

From a sanction monitoring perspective:

National and international regulators, including government enforcement bodies, issue and update sanctions and enforcement actions on a regular basis. In order to stay current with the latest sanction's changes, businesses must carefully monitor any changes from the relevant authorities. Monitoring any updates on global watchlists and adjusting the screening processes for sanctions screening and monitoring should be at the forefront of their AML compliance actions in order to ensure compliance adherence. Firms should also ensure an effective and ongoing internal control on any changes that arise from new sanctions updates whenever they are issued.

What are the risks if appropriate due diligence controls are not in place?

In e-commerce, criminals can often use fake or stolen identities to get access to online commerce platforms. This process helps them make purchases with criminal money to later sell goods in order to make diverse layers of transactions. Sometimes criminals may fake their identity to sell goods to a legitimate merchant. At a later stage, they could exploit the business proceeds to incorporate dirty money within.

Relationships with business counterparties are critical for business growth and prosperity. However, these relationships can also expose the business to a number of financial crime risks including money laundering, fraud, bribery and corruption or terrorist financing. Non-compliance with AML and Anti-Bribery and Corruption regulations and inefficient due diligence processes and controls can expose the business to significant enforcement actions, penalties and negative news that can entail substantial reputational damage. Ensuring effective risk assessment procedures, ongoing monitoring and screening of business counterparties can reduce the unnecessary time wasted in dealing with investigations and internal remediation processes and protect your business assets and reputation in the market.

Significance of AML screening for e-commerce businesses

An effective AML screening can help limit exposure to fraud and lead to productive and healthy regulatory compliance. AML regulatory compliance may give credibility and provide a better rating from the authorities in their business community. This can also create business opportunities.

LexisNexis® Risk Solutions can help businesses predict and mitigate financial crime risk and help prevent risky relationships and potential losses.

For more information, please visit risk.lexisnexis.com/EMEA

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 provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, 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 www.risk.lexisnexis.com and www.relx.com.

Our financial services solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843
[2] https://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf