

The logo for FINEKSUS, featuring the company name in a bold, white, sans-serif font followed by a small white square icon.

Tackle financial crimes and risks
with AI-powered solutions

Global Financial Crime Report

May 2024

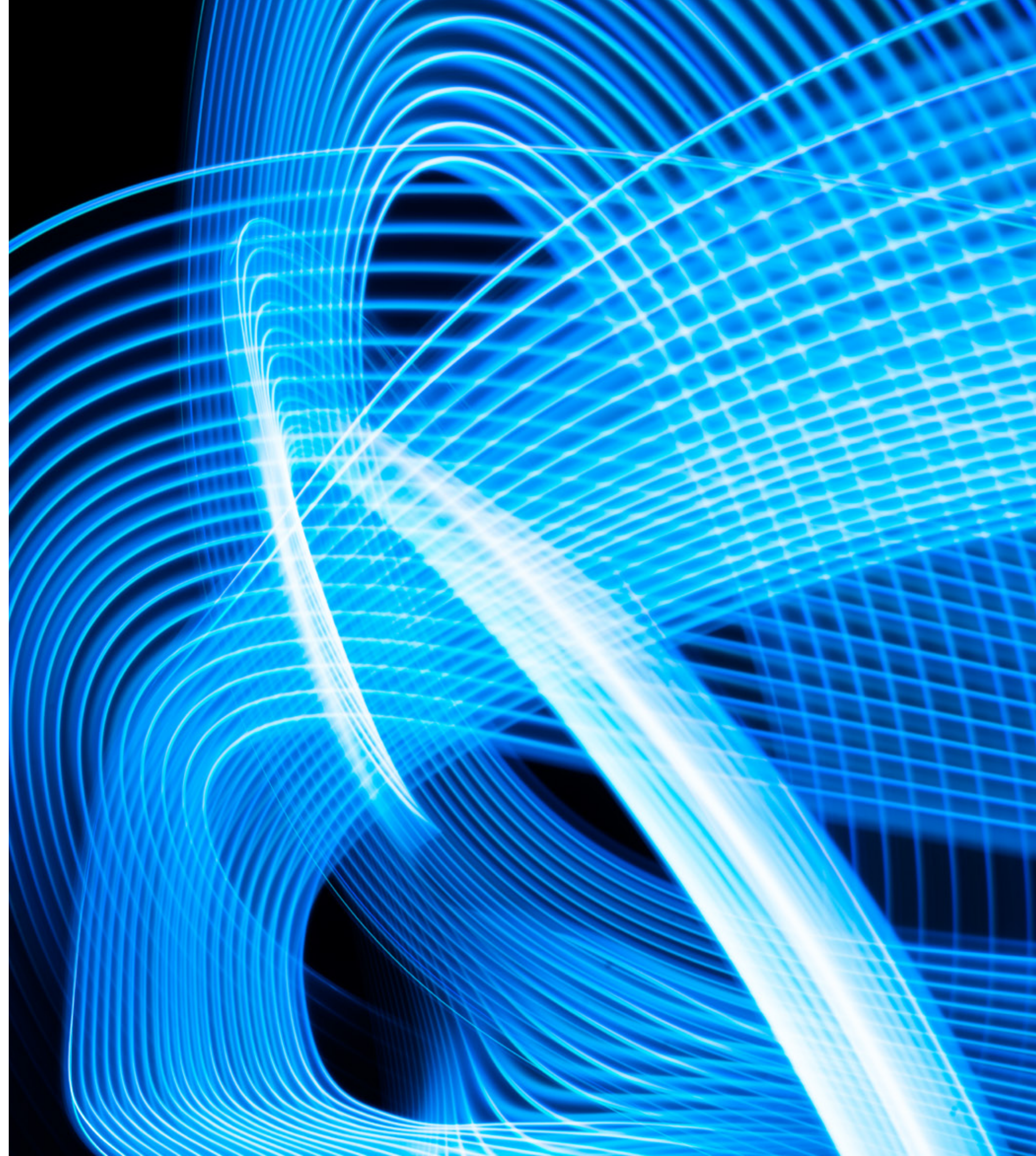
Foreword

Quickly-evolving technological and digital advancements paved the way for a series of opportunities in the financial industry including but not limited to improved efficiency, connectivity and consumer satisfaction. On the other side, financial criminals benefitted from these technological improvements and misused them for fraudulent purposes. 2023 was a year focusing and elaborating on this discrepancy between the positive and negative effects of the technology in the financial environment.

Both the problem and the solution were rooted in the same source. As the technological, geopolitical, regulatory and criminal areas dynamically changed and evolved with the new digital developments, financial institutions had to find new, technological solutions to monitor data, analyze the risks, remain compliant with the regulations, fight against financial crime and meet customer requirements.

In line with this increasing complexity in the financial industry, which is intensified by the exploitation of the new technological enhancements by the criminals, in 2024, money laundering, terrorist financing, identity fraud, sanctions evasions and other new emerging crimes related to cybersecurity, data breaches and virtual currencies will likely remain as the primary problems to be tackled by the financial stakeholders.

Ahmet Vefik Dinçer, CEO



Index

Foreword	2
Index	3
Summary	3
1. Financial crime risks are expected to increase in 2024	4
2. Technology is a double-edged sword in the fight against financial crime, as it can both enable and prevent illicit activities	5
3. Importance of anti-money laundering (AML) and anti-bribery and corruption (ABC) functions	6
4. Sanctions compliance	7
5. Rise in cryptocurrencies and related risk	8
6. Data Integrity	9
7. Environmental, social and governance (ESG) reporting and transparency	10
References	11
Contact Us	12
About Us	13

This whitepaper investigates and analyzes the financial crime trends that were prevalent in 2023 focusing on the reflections of 2023 in the upcoming year, the constructive and destructive effects of technological enhancements, increasing importance of the fight against the money laundering and related crimes, current status of the compliance framework, digital assets and their stance in the financial crime topic, challenges about data integrity, and the concepts of sustainability and transparency in the financial industry in relation to environmental crimes. In 2023, all the stakeholders of the financial world - banks, nonbanks, fintechs, regulators and all other organizations and individuals - are struggling to create a balance between ensuring a transparent, efficient, user-friendly and digitally adapted financial environment and keeping strong and safe in the fight against fraud, money-laundering and other financial crimes.



1. Financial Crime Risks are Expected to Increase in 2024



Global Financial Crime Surges, Projecting \$485.6 Billion in Losses from Fraud and Bank Schemes in 2023, with Rising Threats in 2024.

According to the Global Financial Crime Report of Nasdaq, approximately \$3.1 Trillions were circulated in the global financial ecosystem illegally. Money laundering as the primary source, funded other criminal activities with estimated \$1.1M for human and drug trafficking and \$11.5B for terrorist financing. The total amount lost due to the fraud scams and bank fraud schemes was \$485.6B in 2023.

Under the shadow of the rising trend of the fraud and financial crime in 2023, the financial industry players expect that the risks are not to be mitigated in 2024 due to the growing complexity and exposure in the financial area that are fed by the misuse of technological developments and interdependent networks by the financial criminals. Money laundering, terrorist financing, identity fraud, sanctions evasions and other new emerging crimes related to cybersecurity, data breaches and virtual currencies will likely remain as the main problems of the financial regulators. Therefore, the importance of the compliance related actions taken by the financial institutions for anti-money laundering (AML) and combating financing of the terrorism (CFT) functions will be highlighted more than ever in 2024.



2. Technology is a Double-Edged Sword in the Fight Against Financial Crime, as It Can Both Enable and Prevent Illicit Activities.



Technological Advances in Financial Services: Boosting Efficiency and Compliance, Yet Increasing Fraud Vulnerability.

The adoption of technological developments and new digital solutions in the financial payments space holds a controversial status as it caused a paradigm shift in the industry in two opposing directions. On the one hand, it boosted the levels of convenience, efficiency, security and satisfaction in the financial transactions and other operations. However, on the other hand, it increased the vulnerability of the financial industry by paving new methods for the fraudsters to exploit the system. The evolving popularity of digital wallets, cryptocurrencies, and other new digital payment methods encouraged fraudsters to discover and exploit this freshly forming, complex digital financial landscape.

Technological transformation in the financial industry was both essential and beneficial for improving the effectiveness of the anti-money laundering (AML) and combating the financing of terrorism (CFT) efforts and enhancing the strength of the fight against money-laundering and terrorist financing crimes in the digital world. Therefore, in 2023, most of the financial institutions started to understand the significance of adoption of the recent technologies into their AML compliance programmes to support their operational workload and to remain compliant with the ever-evolving regulatory requirements. In addition to the help in operational efforts, the integration of technological solutions also reinforced the risk detection and management for the AML/CFT processes especially with the introduction of artificial intelligence (AI) and machine learning (ML). There are still some challenges that the technology poses in terms of the operational and regulatory aspects. The essence of the regulatory environment and accordingly the compliance requirements for AML and CFT still remain traditional in various ways in comparison to the pace of innovation the new technologies offer. Therefore, the enhancements, implementation and adoption of the technological solutions might not be answered by the financial institutions and the industry in some cases.

3. Importance of Anti-Money Laundering (AML) and Anti-Bribery and Corruption (ABC) Functions



Anti-money laundering (AML) and anti-bribery and corruption (ABC) programs are two distinct functions focusing on fighting with financial crimes globally. However, by the nature of the financial crimes they combat against, the AML and ABC programs share overlapping methods, skills and tools. Although money laundering, bribery and corruption are offenses that are separate from each other, legally, they are all financial crimes. By adopting a holistic approach, AML and ABC functions should collaborate in order to increase the efficiency by merging their expertise and resources for the monitoring, evaluation and risk assessments against these crimes.

The recent criminal trends demonstrated that behind the schemes of money laundering activities, there is often a case of corruption and bribery involved. Combinations of these crimes are usually committed by private sector or governmental administrative officials and they end up with reputational and financial damage and hefty governmental or regulatory penalties. In the majority of the cases, the institutions involved were not aware of what was happening within their own organization. In order to be ahead and prevent these crimes in advance, it is crucial to embrace the holistic point of view of the risks and unite the powers of the AML and ABC programs.

Integrating AML and ABC Programs Is Essential to Counteract Complex Financial Crimes Effectively.

4. Sanctions Compliance



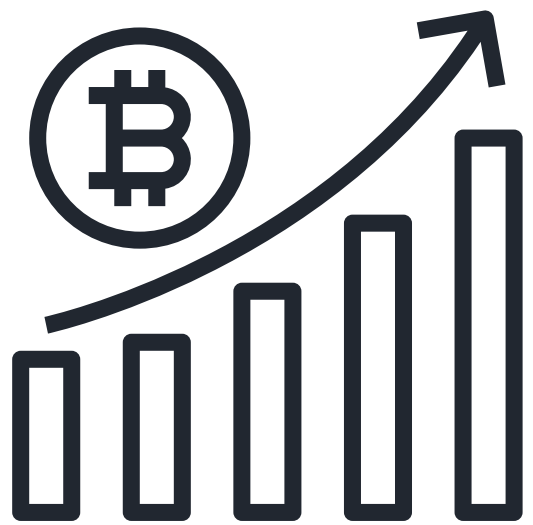
Sanctions are a vital element of successful and effective AML and CFT activities as they empower governments to impose fines and restrictions on specific individuals or organizations that are related to illegal activities. Financial institutions are responsible for ensuring a complete sanctions compliance by being extra cautious not to interfere with sanctioned individuals or nations. The transaction monitoring is also covered by the sanctions compliance so that transactions with sanctioned persons or organizations can be tracked, detected and prevented.

Just as the regulatory landscape, sanctions compliance challenges financial institutions in different ways including geographical inconsistency, privacy issues, quickly changing regulations and finding the right and high-end technological screening solutions to support sanctions compliance. The organizations that failed to remain compliant with sanctions encountered extensive financial and reputational damage, while on the other hand those that put extra effort for the sanctions compliance processes by employing effective and continuous due diligence processes combined with technological screening solutions enjoyed the advantage of cost-efficiency in terms of operations and penalties.

Ensuring Rigorous Sanctions Compliance Is Crucial for Financial Institutions to Mitigate Reputational and Financial Risks.



5. Rise in Cryptocurrencies and Related Risks



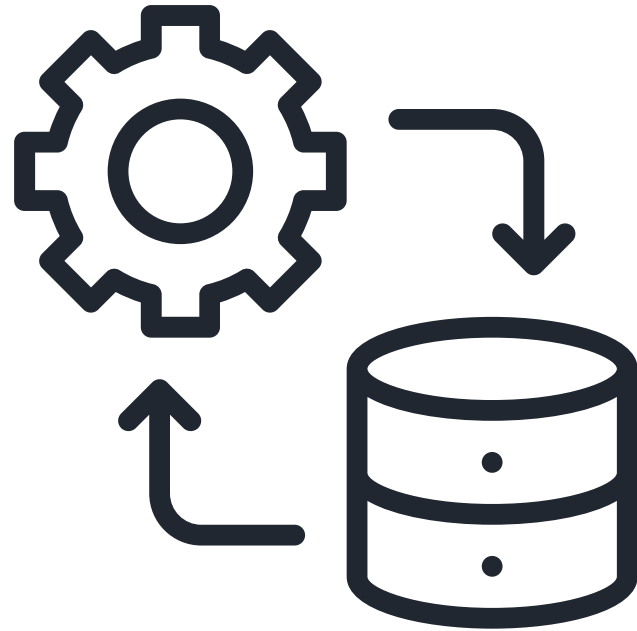
Lack of KYC Processes in Cryptocurrencies Poses Significant Challenges for AML Compliance.

Decentralized payment systems, in other words cryptocurrencies, do not request any personal identity data of their users which means they do not collect information needed for due diligence and Know Your Customer (KYC) processes. Therefore, as opposed to the centralized exchange systems, it is not possible to suspend or freeze the funds in cryptocurrencies which eventually leaves them vulnerable to the risks and threats of money-laundering crimes. Additionally, because cryptocurrencies are not included in sanction screenings or blacklists, they offer a suitable environment for the financial criminals to refrain from specific sanctions. The gaps in the regulatory framework to cover cryptocurrencies resulted in financial criminals misusing the crypto world as a new harbor for money laundering activities.

In 2023, procuring AML compliance for the cryptocurrencies was another challenge that needed to be addressed and tackled urgently by the regulators. For the AML protocols, an effective KYC process is one of the essential components in the fight against the crimes. Therefore, implementing intense KYC requirements into the system of virtual currencies was seen as an efficient solution in managing risks and fighting money laundering via cryptocurrencies.



6. Data Integrity



Data integrity was one of the main challenges of the financial institutions in 2023 while they were struggling to implement new technological solutions into their systems. A data strategy must be put in place when a new IT strategy is settled because the breaches in data integrity generally occur during the processes of relocation or replication of data.

Organizations that decided to benefit from cloud technology to store data could solve the problem of efficiency; however, they are still struggling with data integrity because simply moving data in a poorly organized way from a legacy platform to cloud does not offer a valid solution. In order to be able to functionally utilize data to combat against financial crimes, it is essential that it is stored in a consistent and coherent way. Financial institutions need to find and apply new methods to ensure customer data integrity to put effective AML and CFT programs in place and remain compliant with the regulatory requirements.

Ensuring Data Integrity Crucial for Financial Institutions Amid Technological Transitions and Compliance Challenges.

7. Environmental, Social, and Governance (ESG) Reporting and Transparency



Sustainability was an important and popular concept in the global financial world in 2023 fuelled by the increasing risks related to environmental crimes and new regulations related to that. As a result, more financial institutions started to give weight to environmental, social and governance (ESG) programs with an aim to fortify their credibility in the industry. Changing customer expectations and priorities also affected the tendency of the institutions to implement the ESG programs with transparency and integrity at the core. However, the operational challenges in the ESG reporting and ensuring privacy and transparency at the same time have become notable for the financial institutions. The methods and data management used in the transparent disclosures of the ESG reporting put pressure on the institutions although the current environmental issues are more obvious than ever.

Regulators are determined to make sure that the organizations are carrying out their ESG liabilities in a transparent way and by reporting to the related bodies. Documentation of the compliance related activities, data storage and management, transparency about the disclosures and limits is expected to be submitted in cases of inquiries.

Financial Institutions Embrace ESG Programs Amid Challenges in Reporting Transparency and Data Management.



References

KPMG. (2022). Ten Key Regulatory Challenges of 2023. Retrieved from <https://kpmg.com/us/en/articles/2022/ten-key-regulatory-challenges-2023-fraud-financial-crime.html>

Kroll. (2023). Fraud and Financial Crime Report: Can technology stop the threat of economic, crypto and ESG crimes?. Retrieved from <https://www.kroll.com/-/media/kroll-images/pdfs/2023-fraud-and-financial-crime-report.pdf>

Nasdaq. (2024). Global Financial Crime Report: Insights at the Intersection of Financial Crime Data & Real Survivor Stories. Retrieved from <https://www.nasdaq.com/global-financial-crime-report>

<https://www.fatf-gafi.org/>


Contact Us

Get in touch with our industry expert executives for further details.



 **Tuncay Çoruh**
Product Development Director
tuncay.coruh@fineksus.com



 **Murat Kurtulmuş**
Implementation & Support Director
murat.kurtulmus@fineksus.com



 **Necati Yavaş**
Sales & Business
Development Director
necati.yavas@fineksus.com




 **Serkan Arslan**
Sales & Business
Development Director
serkan.arslan@fineksus.com



 **Gökçe Gence**
Solution & Project Director
gokce.gence@fineksus.com



 **Burçin Güney**
Senior Manager, Sales
burcin.guney@fineksus.com



 **İbrahim Başer**
Senior Software Development
Manager, AML
ibrahim.baser@fineksus.com



 **Emrah Öztürk**
AI Manager
emrah.ozturk@fineksus.com

About Us

Milestones

Fineksus was founded in Istanbul, Turkiye in 2002 as a software and professional service provider to deliver technical consultancy, outsourcing services, standalone / SaaS AML and payment software solutions for banks, brokers and corporations. In the beginning of 2013, Fineksus started managing its ongoing GCC Region operations at its new office in Dubai, UAE.

Fineksus is the market leader of compliance and financial messaging solutions in Turkiye by providing its products and services for more than 95% of the banking industry, and aims to expand its offerings global wide which makes the company at the forefront for providing AML solutions and financial messaging tools.

PayGate™ Suite as AML trademark

Fineksus provides products and services across 29 countries from Hong Kong to the UK with offices in Istanbul, Dubai and Qatar. By meeting ever-changing demands of RegTech industry with 18 years of know-how, Fineksus develops cutting edge tools to bring value for more efficient and effective way of AML compliance and financial messaging. PayGate™ Compliance package covers all the fundamental operations based on AI and machine learning to maintain surveillance of financial systems.



PayGate™ KYC
Know your customer.
Know your risk.



PayGate™ Analyzer
Next generation transaction
monitoring.



PayGate™ Inspector
AI-powered blacklist
filtering.

Follow us on
Social Media!



www.fineksus.com

Request a Demo

Copyright © 2024 Fineksus

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owners.