Nasdaq Verafin

Financial Crime Insights: Europe

Special Edition of the 2024 Global Financial Crime Report

Message from the Head of Nasdaq Verafin

Stephanie Champion
EVP & Head of Nasdaq Verafin, Financial Crime Management Technology, Nasdaq

In today's interconnected world, the financial sector plays a pivotal role in ensuring economic stability and growth. However, the industry faces significant challenges as it confronts a financial crime epidemic with $3.1 trillion in illicit funds moving around the globe in 2023, threatening the integrity of the financial system. As fraud and money laundering impact the growth and security of economies globally, the human impact of crimes, including elder abuse, human trafficking and terrorism, is immeasurable.

This special edition of our 2024 Global Financial Crime Report[1] takes a deeper dive into the scale of financial crime across Europe, where our research estimates $750.2 billion in illicit funds moved through the financial system and fraud losses topped $103.6 billion in 2023. Expert research and industry insights gathered for this report reveal key trends and priorities facing the financial industry in the United Kingdom, European Union, and Nordic region.

Despite regional variation in priorities, banks across Europe are operating in an increasingly complex environment. Our report echoes Nasdaq and Boston Consulting Group's 2025 Complexity Report,[2] highlighting how the speed of evolving financial crime threats and mounting regulatory expectations are placing considerable demands on financial institutions' compliance and financial crime management programs.

> "There is immense potential for industry stakeholders to work together, building on the positive momentum across Europe, and deliver on a step change in the fight against financial crime."

Criminals have adapted to the real-time and cross-border nature of the payments systems in Europe and beyond, targeting consumers, with Authorized Push Payment (APP) and other fraud scams, and moving funds faster and further than ever. Bad actors and criminal enterprises are exploiting the highly interconnected global financial system to move the proceeds of these frauds and other predicate crimes, laundering funds internationally on a massive scale. For Europe, cross-border illicit flows represent more than a quarter of the region's total money laundering activity by value – a staggering $194.9 billion in illicit funds moving in or out of European countries. An estimated $58.2 billion in money laundering activity can also be attributed to money mules — threat actors moving proceeds on behalf of criminals to mask the nature of illicit transactions.

Amid the many money laundering threats and fraud trends facing European financial institutions, this report provides an incisive perspective on the priorities and opportunities needed to propel the industry forward. Our survey of financial crime professionals from across Europe found that while only 22% of respondents have adequate resources, including personnel or technology, to combat

financial crime, banks across the region can see the value in embracing data-driven, innovative solutions and collaborative approaches for a step change in anti-money laundering and countering the financing of terrorism (AML/CFT) measures and fraud prevention capabilities. There is immense potential for industry stakeholders to work together, building on the positive momentum across Europe, and deliver on a step change in the fight against financial crime.

Banks are harnessing the power of innovative technologies and data-driven approaches to improve their fraud prevention and respond more effectively to criminal threats. In our survey, 74% of respondents indicated plans to invest in artificial intelligence (AI) technology in the near term, as the industry leans into this new era of innovation. With the power of AI, machine learning, and consortium analytics, and consortium data analytics, banks can streamline fraud and compliance operations, more accurately detect anomalies, and uncover hidden criminal connections across banks and borders.

Aligning with a global trend of modernizing AML regulations, Europe's new regulatory frameworks for sharing information are providing opportunities for the financial industry to collaborate to disrupt fraud and money laundering. Information sharing initiatives, supported by innovative technology can enable banks to operationalize collaboration and effectively prevent financial crime, while also preserving privacy and ensuring regulatory compliance. Alignment across the public and private sectors, will enable a range of collaborative approaches to help root out criminal activity, disincentivize fraudsters and dismantle the criminal networks that threaten the security of the financial system.

Industry stakeholders, from both private and public sectors, have the opportunity to look beyond their own borders and towards a unified vision — to protect Europe and the world from financial crime. With banks at the forefront of this effort, it is critical that government, policymakers, regulators and supervisors work with the private sector to break down the siloes that currently exist between banks and across borders. The industry must come together in the fight against fraud and money laundering, to align on key priorities including cross-border payments risk, modernizing regulations, fostering greater industry collaboration, supporting adoption of AI and advanced technologies.

This united front will not only serve to more effectively address the current challenges but will also pave the way for a more secure, trusted and resilient financial future for the region, and beyond. Through collective efforts to innovate, Europe is poised to be a world leader in the fight against financial crime and safeguarding the integrity of the global financial system.

Table of Contents

About this Report

Last Updated March 31, 2025

This Special Edition of the 2024 Global Financial Crime Report focuses on financial crime trends and perspectives in Europe, including the European Union (EU), the United Kingdom (UK) and the Nordic region (Sweden, Finland, Norway, Denmark).

This report provides new analysis of the data from the 2024 Global Financial Crime Report, with further examination by Celent Research to provide European-specific insights. For more information on the original data modeling, see the Methodology section in the 2024 Global Financial Crime Report.[1] Unless otherwise stated, the currency used in this report is shown in US dollars (USD).

Exclusively for this report, Celent Research built on the original data by calculating estimates of cross-border and domestic illicit funds movement, and illicit funds moved by money mules, using country and region datapoints. Key sources for this analysis included the Basel AML Index, European Union Drugs Agency (EUDA), and Europol. These new data points are defined as follows:

- **Cross-Border Illicit Funds Movement:** The flow of illegal funds from one country to another. This includes outgoing funds to any international destination or incoming funds originating from an international jurisdiction.
- **Domestic Illicit Funds Movement:** The flow of illegal funds strictly within a single country's borders.
- **Funds Moved by Money Mules:** The estimated value of illicit funds moved and laundered by individuals who transfer funds on behalf of criminals. Money mules may be complicit in the money laundering activity, as individuals or part of a mule network; or an unwitting participant in the crime, deceived through scams or exploitation.

The data estimates on the scale of financial crime for Europe, previously amalgamated with the Middle East and Africa as the EMEA region in the 2024 Global Financial Crime Report, is now presented separately for this special edition report. This report provides separate data for some EU Member States and independent European countries. In the maps and tables, results for the remaining countries are presented together in the following amalgamated groups:

- **Rest of EU:** Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Estonia, Greece, Hungary, Ireland, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Romania, Slovakia, Slovenia.

- **Other Europe:** Albania, Andorra, Armenia, Azerbaijan, Belarus, Bosnia and Herzegovina, Channel Islands, Faroe Islands, Georgia, Iceland, Kosovo, Liechtenstein, Moldova, Monaco, Montenegro, North Macedonia, Russian Federation, San Marino, Serbia, Turkmenistan, Ukraine.

This report estimates fraud losses in two categories: third-party/authorized fraud and first-party/unauthorized fraud. These categories are based on insights and data modelling from the 2024 Global Financial Crime Report.

- **Third-Party/Authorized Fraud** — Fraud where losses are incurred by a consumer or a business. This includes cyber-enabled scams (i.e., business email compromise, phishing and data breaches), impersonation scams (i.e., charity, business, government and law enforcement impersonation scams), confidence scams (i.e., romance, family and relative impersonation scams), advance fee scams (i.e., lottery, prize, grant and non-delivery scams), and employment scams.
- **First-Party/Unauthorized Fraud** — Fraud where losses are incurred by the bank. This includes payments fraud (i.e., credit transfers and direct debits), check fraud, and credit card fraud.

To capture industry perspectives in the region, our partner, Celent Research also conducted a survey of 270 anti-financial crime professionals from financial institutions across Europe — 105 from the United Kingdom, 109 from the Nordic region, and 56 from other European jurisdictions. These financial institutions ranged from under €10 billion to over €500 billion in assets. Celent Research also conducted deep-dive interviews with senior executives for a greater understanding of industry perspectives.

As in the 2024 Global Financial Crime Report, we recognize that the scope of the modelling used for this report is not inclusive of all financial crime typologies and data is limited to current regional detection and reporting capabilities and/or law enforcement interdiction. The numbers within this report can only represent a fraction of criminal activity and victims of financial crime.

Additional methodology is available in the 2024 Global Financial Crime Report.[1]

Executive Summary

No region is immune from the multi-trillion-dollar global epidemic of financial crime. The heinous crimes underpinning these illicit flows, such as elder abuse, fraud scams, human trafficking, drug trafficking and terrorist financing, have deep economic and societal impacts, posing a significant threat to Europe — and to financial systems around the world.

This special European edition of the 2024 Global Financial Crime Report takes a deeper dive into financial crime trends and industry insights from across Europe, including the EU, UK, and the Nordic region.

In 2023, an estimated **$750.2 billion in money laundering activity** and illicit funds flowed through Europe's financial system, **representing 2.3% of total GDP** in the same year.

Contributing to these illicit flows are the proceeds of bribery, corruption, organized crime and other nefarious activities, including an estimated:

- **$178.0 billion** in drug trafficking activity
- **$82.2 billion** in human trafficking activity
- **$2.7 billion** in terrorist financing activity

Fraud is a significant threat to Europe's financial industry, with an estimated **$103.6 billion in fraud losses** from a range of scams and bank fraud scenarios.

Criminals are exploiting the highly interconnected and real-time nature of payments in the global financial system to obscure their illicit money trails and move funds on a massive scale. New insights from our research reveals that of all funds laundered across Europe in 2023, **$194.9 billion was moved across borders, representing more than a quarter of the total estimates for money laundering activity** in the region. With cross-border transactions increasing globally,[2] pan-European and international financial flows are a significant vector for illicit activity. Recruited by criminals to transfer and obscure the flow of funds connected to fraud and other predicate crimes, **money mules moved $58.2 billion in illicit funds — both domestically and across borders,** adding further complexity to Europe's financial crime risk landscape.

Financial institutions across Europe are continuously enhancing their defenses by investing in people, processes and technology, to keep pace with evolving financial crime threats, while also ensuring compliance with changing obligations for various regulatory frameworks. This increasingly complex environment is contributing to banks' rising operational costs, which is exacerbated by the inefficiencies of manual processes and legacy technology systems. Our survey shows that institutions believe that their anti-financial crime programs would most benefit from improvements in regulation that deliver guidance on priorities, encourage technology innovation, and enable greater collaboration and information sharing across the industry.

Money Laundering

By Region:

European Union
$438.4B

United Kingdom
$98.7B

Nordic Region
$41.1B

Fraud Scams & Bank Fraud

By Region:

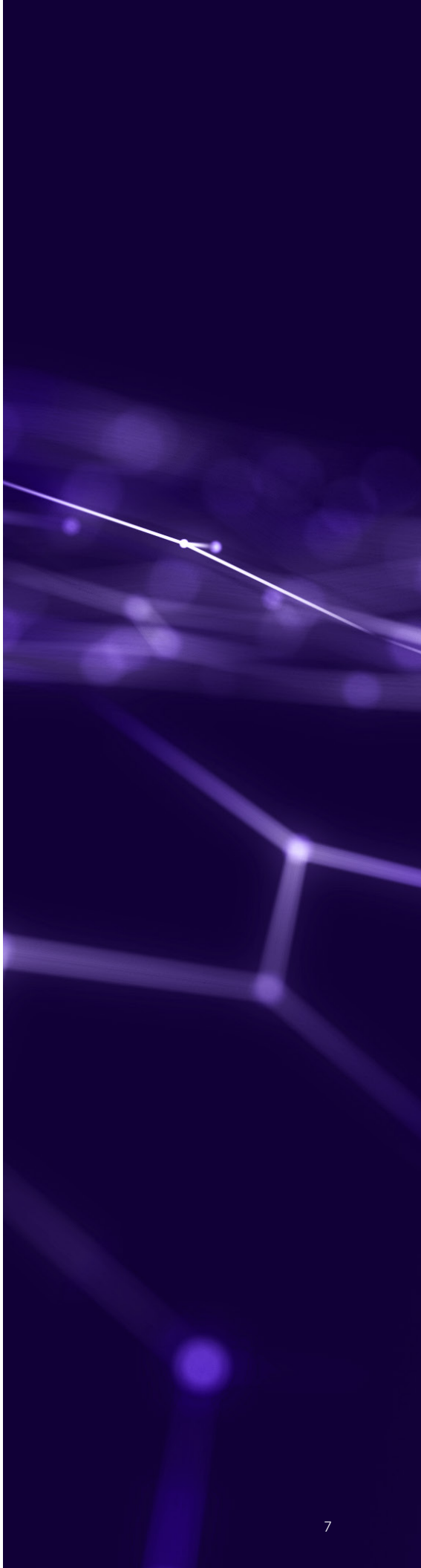
European Union
$61.5B

United Kingdom
$33.2B

Nordic Region
$3.4B

The industry is in the midst of a technology revolution. The convergence of new AI technologies, cloud capabilities, and consortium data approaches are delivering a step change in efficiency and effectiveness for anti-financial crime programs. In the EU, UK and around the world, new regulatory frameworks for information sharing are enabling the collective power of financial intelligence to break down barriers between banks and borders, and disrupt criminal activity. There is an opportunity for national governments, policymakers, and regulatory bodies to work with financial institutions to ensure alignment on European financial crime priorities, work towards harmonizing national frameworks, and take collective, decisive action against cross-border scams, fraud and associated money laundering. In doing so, Europe's financial industry could set a new standard of leadership in combating financial crimes across borders.

It is critical that public and private sector stakeholders across Europe are united in a shared vision that prioritizes innovative and collaborative approaches for financial crime prevention — and work together to safeguard the integrity of the global financial system.



The Scale of Financial Crime in Europe

Financial crime in Europe is staggering in scale and inextricably linked to a global crisis that undermines financial systems, economies and communities around the world.

Europe represented nearly a quarter of all money laundering activity worldwide in 2023. Within the region, over a hundred billion dollars was lost to fraud scams and bank fraud schemes. Money mules moved $58.1 billion, while hundreds of billions of dollars in illicit funds flowed across borders, circulating the proceeds of heinous crimes such as human trafficking, terrorist financing and drug trafficking throughout the continent.

This report reveals how money laundering, terrorist financing and other illicit activities such as fraud are pervasive threats to the European financial system — not bound by banks or borders.

The following estimates of financial crime in Europe were determined by Oliver Wyman and Celent Research, building on the original analysis and modeling from Nasdaq's 2024 Global Financial Crime Report.

$750.2 Billion in Illicit Funds Flow Across Europe

Fueling the world's financial crime epidemic

Terrorist financing, money laundering and the movement of proceeds of underlying crimes including human trafficking, drug trafficking, corruption, organized crime, fraud and other illicit activity.

24%
Europe represents nearly a quarter of the total flow of illicit funds globally

Breakdown by Country		Percentage of GDP
Germany	**$128.7B**	3.07%
UK	**$98.7B**	3.12%
France	**$80.2B**	2.80%
Italy	**$65.8B**	3.09%
Spain	**$44.3B**	3.03%
Netherlands	**$25.7B**	2.47%
Switzerland	**$24.6B**	2.91%
Sweden	**$15.3B**	2.51%
Norway	**$12.7B**	2.13%
Denmark	**$8.2B**	2.05%
Finland	**$5.0B**	1.78%
Rest of EU*	**$65.3B**	1.49%
Other Europe*	**$175.9B**	2.50%

$100 – 150B $50 – 100B $20 – 50B $0 – 20B

*A complete list of countries is detailed in the *About this Report* section. For this visualization, Norway and Switzerland are broken out individually, and excluded from Other Europe total.

Money Laundering and Related Activities Breakdown

Highlighted Regions:

EU $438.4B

Other* $281.9B
Drug Trafficking $107.1B
Human Trafficking $47.8B
Terrorist Financing $1.6B

UK $98.7B

Other* $64.0B
Drug Trafficking $22.4B
Human Trafficking $12.0B
Terrorist Financing $300.0M

Nordics $41.1B

Other* $25.8B
Drug Trafficking $10.5B
Human Trafficking $4.6B
Terrorist Financing $187.0M

By Country:

Germany $128.7B

Other* $84.9B
Drug Trafficking $29.7B
Human Trafficking $13.6B
Terrorist Financing $531.0M

France $80.2B

Other* $50.3B
Drug Trafficking $20.3B
Human Trafficking $9.3B
Terrorist Financing $363.0M

Italy $65.8B

Other* $40.2B
Drug Trafficking $17.2B
Human Trafficking $8.0B
Terrorist Financing $269.0M

Spain $44.3B

Other* $27.6B
Drug Trafficking $11.1B
Human Trafficking $5.5B
Terrorist Financing $123.0M

Netherlands $25.7B

Other* $14.0B
Drug Trafficking $8.4B
Human Trafficking $3.1B
Terrorist Financing $132.0M

Switzerland $24.6B

Other* $17.1B
Drug Trafficking $5.1B
Human Trafficking $2.3B
Terrorist Financing $98.0M

Sweden $15.3B

Other* $9.9B
Drug Trafficking $3.7B
Human Trafficking $1.6B
Terrorist Financing $77.0M

Norway $12.7B

Other* $8.0B
Drug Trafficking $3.0B
Human Trafficking $1.6B
Terrorist Financing $50.0M

Denmark $8.2B

Other* $4.9B
Drug Trafficking $2.4B
Human Trafficking $864.0M
Terrorist Financing $42.0M

Finland $5.0B

Other* $3.0B
Drug Trafficking $1.4B
Human Trafficking $533.0M
Terrorist Financing $18.0M

Rest of EU $65.3B

Other* $47.1B
Drug Trafficking $13.0B
Human Trafficking $5.3B
Terrorist Financing $25.0M

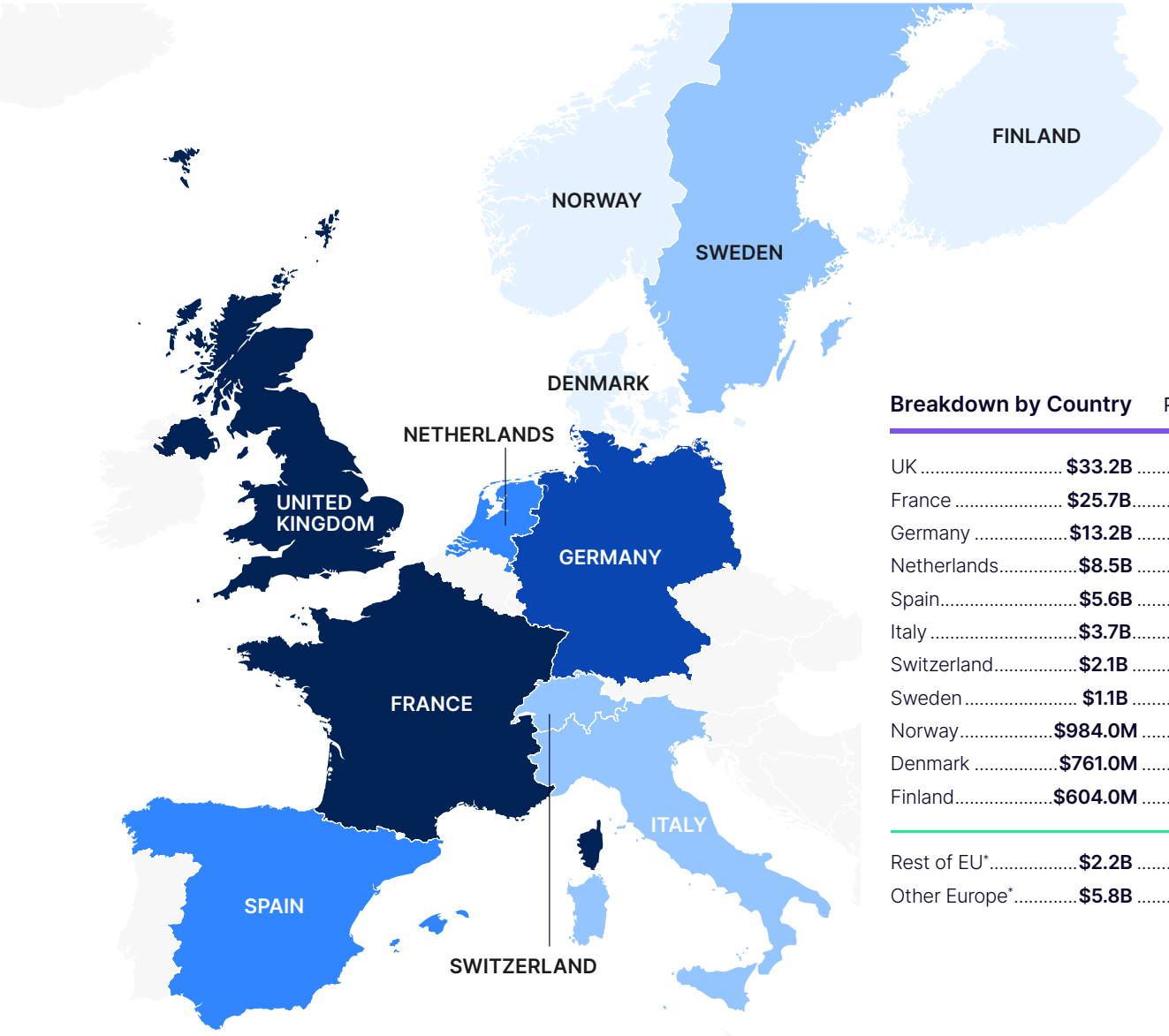
Other Europe $175.9B

Other* $116.2B
Drug Trafficking $40.5B
Human Trafficking $18.5B
Terrorist Financing $714.0M

*Organized Crime, Fraud, Corruption, etc.

$103.6 Billion in Fraud Losses Across Europe

Losses to consumers and businesses originating from impersonation, confidence, advance fee, employment, and cyber-enabled scams, as well as bank fraud losses from payments, check and credit card fraud.



Breakdown by Country		Percentage of GDP
UK	**$33.2B**	1.05%
France	**$25.7B**	0.90%
Germany	**$13.2B**	0.31%
Netherlands	**$8.5B**	0.82%
Spain	**$5.6B**	0.38%
Italy	**$3.7B**	0.17%
Switzerland	**$2.1B**	0.25%
Sweden	**$1.1B**	0.18%
Norway	**$984.0M**	0.17%
Denmark	**$761.0M**	0.19%
Finland	**$604.0M**	0.21%
Rest of EU*	**$2.2B**	0.05%
Other Europe*	**$5.8B**	0.08%

$20 – 35B | $10 – 20B | $5 – 10B | $1 – 5B | $0 – 1B

*A complete list of countries is detailed in the *About this Report* section. For this visualization, Norway and Switzerland are broken out individually, and excluded from Other Europe total.

Fraud Losses: Scams and Bank Fraud Breakdown

Highlighted Regions:

EU $61.5

Total Bank Fraud Losses $55.0B
Total Consumer and Business Fraud Losses $6.4B

- Payments Fraud $53.2B
- Advance Fee Scams $3.6B
- Cyber-Enabled Scams* $1.5B
- Credit Card Fraud $1.5B
- Impersonation Scams $711.0M
- Check Fraud $363.0M
- Confidence Scams $362.0M
- Employment Scams $228.0M

UK $33.2B

Total Bank Fraud Losses $30.5B
Total Consumer and Business Fraud Losses $2.7B

- Payments Fraud $29.7B
- Advance Fee Scams $2.0B
- Credit Card Fraud $793.0M
- Cyber-Enabled Scams* $328.0M
- Confidence Scams $181.0M
- Impersonation Scams $151.0M
- Employment Scams $76.0M
- Check Fraud $49.0M

Nordics $3.4B

Total Bank Fraud Losses $2.8B
Total Consumer and Business Fraud Losses $650.0M

- Payments Fraud $2.7B
- Advance Fee Scams $315.0M
- Cyber-Enabled Scams* $172.0M
- Impersonation Scams $84.0M
- Credit Card Fraud $74.0M
- Employment Scams $54.0M
- Confidence Scams $25.0M
- Check Fraud $18.0M

By Country:

France $25.8B

Total Bank Fraud Losses $24.7B
Total Consumer and Business Fraud Losses $1.2B

- Payments Fraud $23.6B
- Credit Card Fraud $790.0M
- Advance Fee Scams $589.0M
- Cyber-Enabled Scams* $297.0M
- Check Fraud $261.0M
- Impersonation Scams $137.0M
- Employment Scams $117.0M
- Confidence Scams $14.0M

Germany $13.2B

Total Bank Fraud Losses $11.4B
Total Consumer and Business Fraud Losses $1.8B

- Payments Fraud $11.3B
- Advance Fee Scams $917.0M
- Cyber-Enabled Scams* $435.0M
- Confidence Scams $265.0M
- Impersonation Scams $201.0M
- Credit Card Fraud $102.0M
- Check Fraud $5.0M
- Employment Scams ..... $-**

Netherlands $8.5B

Total Bank Fraud Losses $8.1B
Total Consumer and Business Fraud Losses $384.0M

- Payments Fraud $8.1B
- Advance Fee Scams $219.0M
- Cyber-Enabled Scams* $93.0M
- Credit Card Fraud $63.0M
- Impersonation Scams $43.0M
- Confidence Scams $15.0M
- Employment Scams $14.0M
- Check Fraud $1.0M

Spain $5.6B

Total Bank Fraud Losses $5.1B
Total Consumer and Business Fraud Losses $541.0M

- Payments Fraud $4.8B
- Advanced Fee Scams $307.0M
- Credit Card Fraud $248.0M
- Cyber-Enabled Scams* $131.0M
- Impersonation Scams $61.0M
- Check Fraud $45.0M
- Confidence Scams $23.0M
- Employment Scams $19.0M

Italy $3.7B

Total Bank Fraud Losses $2.9B
Total Consumer and Business Fraud Losses $769.0M

- Payments Fraud $2.7B
- Advance Fee Scams $448.0M
- Credit Card Fraud $197.0M
- Cyber-Enabled Scams* $191M
- Impersonation Scams $88.0M
- Employment Scams $28.0M
- Check Fraud $21.0M
- Confidence Scams $14.0M

Switzerland $2.1B

Total Bank Fraud Losses $1.8B
Total Consumer and Business Fraud Losses $308.0M

- Payments Fraud $1.8B
- Advance Fee Scams $177.0M
- Cyber-Enabled Scams* $76.0M
- Credit Card Fraud $49.0M
- Impersonation Scams $35.0M
- Employment Scams $11.0M
- Confidence Scams $9.0M
- Check Fraud $2.0M

**Losses to Business Email Compromise, phishing and data breaches.*
***No significant result based on data modeling.*

Fraud Losses: Scams and Bank Fraud Breakdown

Sweden $1.1B

Total Bank Fraud Losses $870.0M
Total Consumer and Business Fraud Losses $216.0M

- Payments Fraud $835.0M
- Advance Fee Scams $128.0M
- Cyber-Enabled Scams* $45.0M
- Credit Card Fraud $27.0M
- Impersonation Scams $25.0M
- Confidence Scams $10.0M
- Employment Scams $8.0M
- Check Fraud $8.0M

Norway $984.0M

Total Bank Fraud Losses $769.0M
Total Consumer and Business Fraud Losses $215.0M

- Payments Fraud $745.0M
- Advance Fee Scams $125.0M
- Cyber-Enabled Scams* $53.0M
- Impersonation Scams $25.0M
- Credit Card Fraud $21.0M
- Employment Scams $8.0M
- Confidence Scams $5.0M
- Check Fraud $3.0M

Denmark $761.0M

Total Bank Fraud Losses $600.0M
Total Consumer and Business Fraud Losses $161.0M

- Payments Fraud $591.0M
- Advance Fee Scams $53.0M
- Cyber-Enabled Scams* $45.0M
- Employment Scams $32.0M
- Impersonation Scams $22.0M
- Confidence Scams $9.0M
- Credit Card Fraud $8.0M
- Check Fraud $1.0M

Finland $604.0M

Total Bank Fraud Losses $545.0M
Total Consumer and Business Fraud Losses $59.0M

- Payments Fraud $525.0M
- Cyber-Enabled Scams* $30.0M
- Credit Card Fraud $18.0M
- Impersonation Scams $12.0M
- Advance Fee Scams $9.0M
- Employment Scams $6.0M
- Confidence Scams $2.0M
- Check Fraud $2.0M

Rest of EU $2.2B

Total Consumer and Business Fraud Losses $1.3B
Total Bank Fraud Losses $844.0M

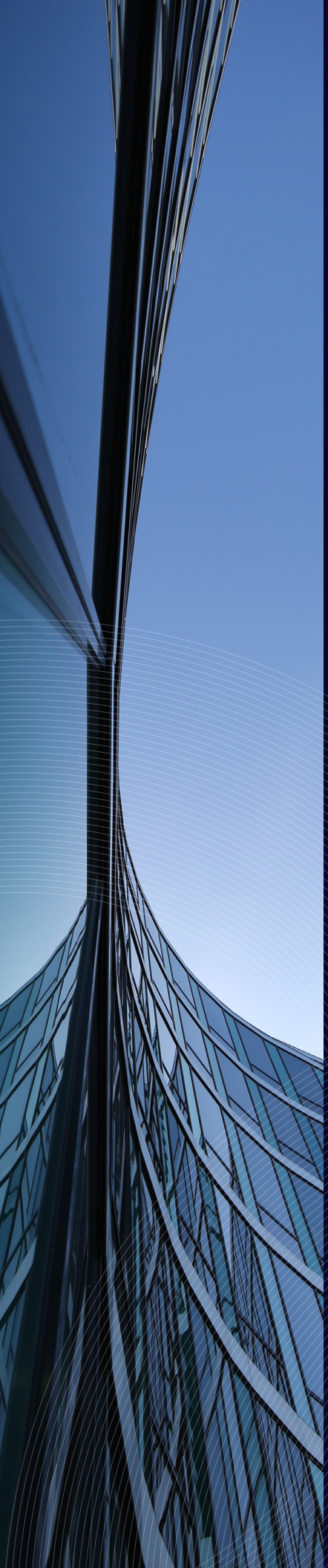
- Advance Fee Scams $934.0M
- Payments Fraud $814.0M
- Cyber-Enabled Scams* $272.0M
- Impersonation Scams $121.0M
- Check Fraud $19.0M
- Credit Card Fraud $11.0M
- Confidence Scams $10.0M
- Employment Scams $3.0M

Other Europe $5.8B

Total Bank Fraud Losses $3.8B
Total Consumer and Business Fraud Losses $2.0B

- Payments Fraud $3.2B
- Advance Fee Scams $939.0M
- Credit Card Fraud $570.0M
- Cyber-Enabled Scams* $564.0M
- Impersonation Scams $260.0M
- Confidence Scams $142.0M
- Employment Scams $133.0M
- Check Fraud $25.0M

**Losses to Business Email Compromise, Phishing and Data Breaches.*
***No significant result based on data modeling.*



Industry Insights

While threats and trends within the European financial system vary between regions, many share commonalities. Financial crime is rapidly evolving — a certainty as criminals leverage new tools, tactics and technology to maximize their gains while evading detection in today's complex risk and regulatory landscape.

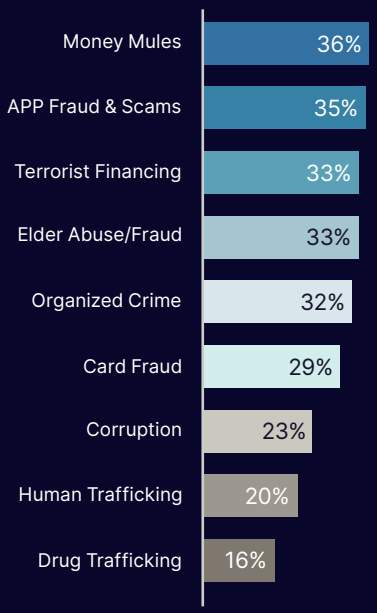
Through our survey with 270 industry professionals and deep dive interviews with three senior anti-financial crime executives, this report brings European industry insights forward to elevate regional threats and trends, and highlight the opportunities to overcome challenges facing financial institutions in their efforts to fight financial crime.

Threats & Trends

As criminals continuously adapt their tactics to evade detection, financial institutions are implementing stronger fraud controls and more stringent AML/CFT compliance programs to manage and mitigate evolving financial crime risks. Our data reveals that a range of financial crime trends are threatening financial institutions, their customers and the financial system. Of most concern to survey respondents across Europe overall were money mules, APP fraud and scams, terrorist financing, and elder fraud. From a regional perspective, ranking of these threats varied across the UK, EU, and Nordic respondents.

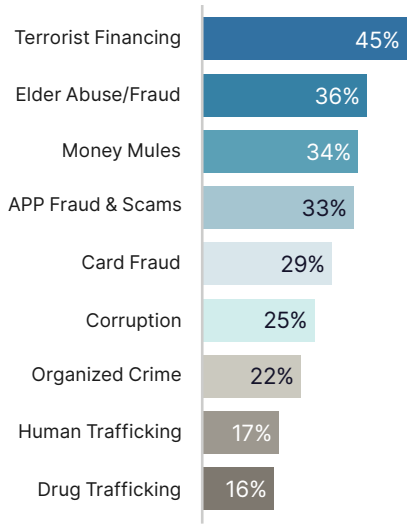
Financial Crime Threats of Greatest Concern:

All Europe Respondents

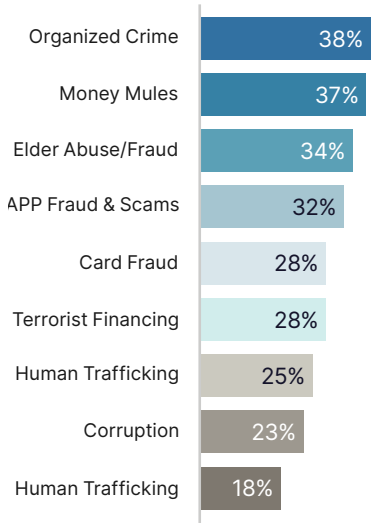


Financial Crime Threats of Greatest Concern:

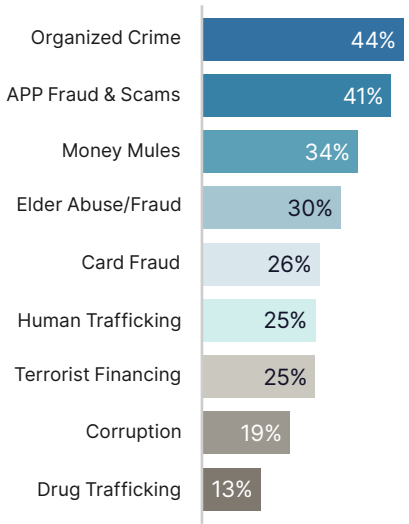
UK Respondents



EU Respondents



Nordic Region Respondents



Fraud Threats

Authorized Push Payment Fraud

Across the industry, banks have implemented controls for remote banking and account takeover, creating strong defenses against unauthorized account access, online takeover, and bank fraud. Fraudsters have adapted by turning to banks' customers as the target vector for their ill-gotten gains — fuelling a rise in fraud losses from scams.

In today's highly connected digital world, criminal networks are capitalizing on the speed and anonymity of online channels and popularity of social media platforms to execute consumer scams on a massive scale. This combined with the adoption of faster and instant payment rails across Europe and around the world, has created a perfect storm for APP fraud to flourish.

APP fraud is a highly effective scam where a customer is manipulated into transferring funds to a fraudster, who is posing as a genuine payee. Criminals often use social engineering to powerful effect, with victims led to believe they are engaging in legitimate activity until the funds are lost, often sent through irrevocable, faster payment channels.

Survey respondents across Europe were highly concerned about APP fraud scams and identified four typologies they perceived as the greatest threat to their financial institutions — investment scams (including those committed through cryptocurrency); impersonation scams; romance and confidence scams; and employment scams.

In recent years, APP fraud has proliferated across the globe, resulting in significant losses for consumers, as well as increased financial, regulatory and reputational risk for banks. More recently, various liability models for customer fraud losses are being considered and implemented in jurisdictions across Europe — most notably with the applicability of the UK's Payment Systems Regulator (PSR) Reimbursement model in late 2024.

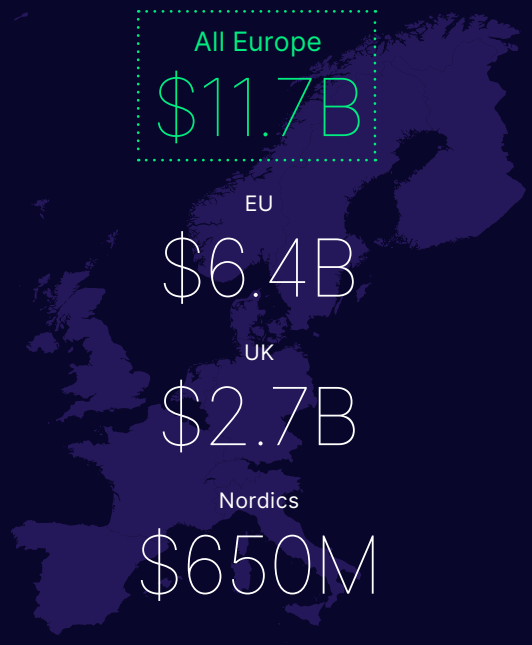
Hybrid Scams

As banks strengthen processes and fraud controls in response to APP fraud threats, criminals are rapidly adapting with more sophisticated techniques to evade detection. Multiple industry interviews noted examples of this growing trend, known as hybrid scams. By using multiple tactics together, fraudsters can further the deception and maximize illicit profits from their unwitting victim. An example of this scam evolution is when fraudsters combine romance and investment scam tactics into a broader, more lucrative scheme.

Losses from Scams

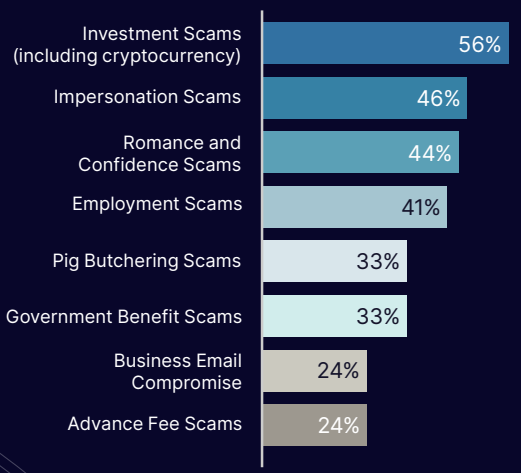
Consumer and Business Fraud

By Region:



APP Fraud Scams of Greatest Concern

All Europe



Another version of a hybrid scam sees the criminal baiting the victims into using alternative payment channels to avoid the heightened scrutiny banks are placing on push payments fraud. An interviewee noted that in the UK, there is a rise in criminals manipulating victims and exploiting card payments to profit from the scam.

By sharing intelligence and leveraging technology, banks can proactively monitor for changes in fraud typologies, patterns of activity and new threats to strengthen their fraud prevention programs and protect customers from loss.

Elder Fraud

According to the World Health Organization, an estimated 1 in 6 people aged 60 or older experience some form of abuse, including financial exploitation[3] and many victims hesitate to come forward due to guilt, shame or a desire to leave the experience behind.[1] Seniors are a favored target for scams given their perceived vulnerability and assumed wealth. Fraud against the elderly can be devastating, especially for individuals who may not be wealthy or survive on a fixed income. As criminals pursue greater profits and scams become more prevalent, so do instances of elder fraud.

> “It’s a very enticing proposition. The prospect of a relationship with a stock photo of a very attractive person and making millions of pounds. What’s not to love?”
>
> - Interviewee

This cruel crime also commonly intersects with other scam typologies such as romance scams. Victims may be exploited as money mules to transfer funds, unwittingly laundering the proceeds of other crimes.

In 2023, $19.9 billion or nearly 20% of all fraud losses across Europe were shouldered by elderly persons. Estimates of losses against senior citizens varied significantly across regions, with elderly victims accounting for 8% of losses in the UK and 19% in the EU, while in the Nordics, elderly fraud victims represented 38% of the total fraud losses in the region — underscoring a clear need to protect this vulnerable population from the threat of fraud.

Banks are rising to the challenge of combating this devastating crime. In our survey, 68% of all respondents said they have dedicated policies, procedures and controls specifically for their elder customers for fraud prevention, and 46% reported having customer education and internal training programs specifically designed to prevent elder fraud.

Fraud Against Elderly Victims

Compared to Total losses
By Region:

All Europe – Total Losses $103.6B

Nordics – Total Losses $3.4B

EU – Total Losses $61.5B

UK – Total Losses $33.2B

> An area of concern — and this is again about the maturity of the market in a way — is that because there's been so much focus on all the push payment scams, we're seeing a sort of shift back to hybrid-type scams. Scammers with the same techniques, just the payment channel is different.
>
> - Interviewee

There are opportunities for financial institutions to evaluate targeted detection strategies that employ advanced data-driven approaches and machine learning technology to further strengthen their efforts to protect elderly and vulnerable customers from exploitation.

Percent of Financial Institutions using Targeted Detection Strategies Specific to Elderly Victims

By Region:

> With the 50-50 liability split between the victims and the bank receiving the funds, there's much more focus and incentives on smaller banks... they need to have monitoring systems in place to detect new accounts, up their game on the KYC front, and ensure that they are able to deal with both the victims of APP fraud but also detect and monitor mule accounts.
>
> - Interviewee

Spotlight: Payments Fraud Liability in the UK

The prevalence of scams and APP fraud has spurred an industry-wide focus on fraud prevention for payment channels to protect consumers from losses. In response, many jurisdictions are implementing or evaluating liability regulations requiring financial institutions to reimburse their customers who were victimized by scams.

The UK was the first jurisdiction[4] to address authorized fraud through regulatory mandate. The UK's Payment Systems Regulator Reimbursement Policy[5] mandates an equal split of an APP fraud loss between the sending and the receiving institutions for domestic payments up to £85,000. This has resulted in many financial institutions strengthening monitoring of inbound payments to root out money mule activity, and outbound payments for risky destination accounts. On faster payment systems, APP scams are often characterized by high volumes of lower-value scam attempts, compared to other payment channels such as wires where the value of each fraudulent payment can be in the millions. With the sheer volume of APP fraud occurrences, banks are prioritizing fraud mitigation and optimizing customer experience — while also meeting new compliance obligations for reimbursement.

Prior to the PSR Reimbursement Policy, a portion of UK financial institutions adhered to the voluntary Contingent Reimbursement Model Code,[6] where signatory Payment Service Providers committed to reimbursing APP fraud victims.

Interviewees noted that in larger banks where reimbursement procedures were already in place, the shift to a shared liability model has added significantly burdensome dispute processes and compliance procedures, due to inadequate settlement infrastructure, as well as lack of clear guidance from regulators at the time the policy was implemented. The added administrative and compliance burden was noted by interviewees as a "distraction" from the intent of the regulations — to focus on true fraud scam prevention and protecting customers from loss.

Financial institutions that did not participate in the voluntary reimbursement model also experienced challenges adapting to the new shared reimbursement model. These institutions needed to establish new policies and procedures to return funds, as well as establish new fraud controls and monitoring for mules — requiring investment in people, processes and technology to comply.

With the PSR's Reimbursement Policy in effect as of October 2024, UK banks must have strong monitoring for APP fraud in place and robust operational processes to manage compliance. The nation's banking sector will no doubt be monitoring for the effectiveness of this model and whether it will meaningfully impact fraud and loss prevention — especially as other jurisdictions evaluate payment regulation and liability for banks.

In March 2025, the UK government announced its intentions to consolidate the PSR and its functionality primarily within the Financial Conduct Authority (FCA) with the aim of simplifying and clarifying payments regulation. Ahead of legislation, the PSR continues to be the independent regulator of UK payment systems, and financial institutions must maintain compliance with current regulatory requirements for payments.

Money Laundering and Terrorist Financing Risks

Financial crime is a global epidemic, spanning domestic and international borders, facilitating nefarious crimes have deep impacts on people, economics, security and society overall.

Across Europe, the top money laundering concerns included organized crime and corruption, as well as heinous crimes that these networks perpetuate, including human trafficking and drug trafficking. Prioritization of these threats varied from region to region — EU respondents were most concerned about money mules, while UK and Nordic respondents considered terrorist financing their leading threat.

These crimes are more often driven by deeply connected organized crime networks, rather than individual perpetrators. In interviews, senior executives noted the nexus between European and international criminal activity, emphasizing how financial crimes in one region of the world are often influenced by bad actors in another. From transnational criminal organizations to professional money laundering networks, criminal enterprises do not respect borders or the rule of law and actively conspire to obfuscate illegal activity and enable the flow of illicit funds in Europe and around the world.

> "We are human beings. And this is a humanitarian crisis that we are living right now."
>
> - Timea E. Nagy, Human Trafficking Activist & Survivor

The human impact of the crimes that underpin this activity, such as human trafficking and drug trafficking cannot be understated — often costing lives, livelihoods and the dignity of victims. Detecting illicit proceeds and the flow of funds supporting trafficking, terrorism, and other illicit activity is exceptionally challenging, but essential to protect society from the lasting consequences of these crimes.

Terrorist Financing

Europe's highly connected financial system enables a single market approach to fuel free movement of goods, services, capital and persons across the region — but can also be exploited for illicit purposes. Interviews with senior executives reinforced that, with the current geopolitical landscape, financial institutions in Europe are facing significant exposure from heightened risk of terrorist financing.

Terrorism prospers through fear and the funding to incite it, which may be derived indirectly through other illicit activities, such as fraud, trafficking or corruption.

> "Cash-based money laundering, terrorism, human trafficking and modern slavery — we've got big exposure there."
>
> - Interviewee

Terrorist Financing Flows

By Region:

All Europe
$2.7B

EU
$1.6B

UK
$300M

Nordics
$187M

In its many forms, terrorism is often associated with extreme political, religious, social or environmental ideologies, and can range from single acts of violence to large-scale threats. Even small volumes of funds can support acts of terror, such as lone wolf scenarios or small cell activities — with dire consequences. The threat from terrorism and terrorist financing extends beyond the borders of any single European country. Terrorist groups and their supporters are exploiting new technologies and the interconnectivity of communication and financial systems on a global scale to recruit, plan, fund and execute destructive acts — which endanger lives and undermine Europe's peace and security.

Financial institutions are critical in the fight against this heinous activity through their CFT efforts and adherence to compliance obligations and standards established by regulatory bodies. The Financial Action Task Force (FATF) has stressed[7] the importance for financial institutions to apply a risk-based approach to mitigate terrorist financing threats and vulnerabilities, establishing mechanisms for robust initial and ongoing customer due diligence, and enhanced due diligence of higher-risk customer types. Financial institution monitoring and reporting for other potentially suspicious activity is also critical to disrupt the financing of terrorist activity and safeguard the financial system.

Money Mules

Money mules are conduits through which the proceeds of crimes are laundered and reintegrated into the financial system. Survey respondents identified money mules as their top financial crime concern across Europe, with tens of billions of dollars being moved by money mules in 2023, and far more likely going undetected.

Complicit Money Mules: knowingly commit financial crimes and move the proceeds, often as part of a larger scheme and motivated by profit. As career criminals, these individuals may be part of professional laundering networks, helping to recruit other mules, operate funnel accounts, open new accounts at financial institutions to facilitate fraud, and ultimately launder massive volumes of funds domestically and internationally.

Unwitting Money Mules: may be unwitting victims of fraud scams or other schemes who believe they are performing legitimate financial activity, such as processing payments for an online job or helping a romantic partner. In interviews, industry experts reported that the number of unwitting mules in Europe is growing, as fraud and scams flourish, and that detecting these mules and their accounts is extremely difficult.

Money mules are agents for illicit activity, blurring the lines between fraud and money laundering as key enablers of financial crime. By rooting out money mules, the financial industry can disrupt flows of funds around the world that underpin the most heinous crimes imaginable.

> "A hot topic in the mule space is the inevitable growth in what we call unwitting mules — mules who've been recruited to launder money, who have no idea that they're breaking the law. You see more genuine bank accounts being used as a one-off payment so there's absolutely no indication or any red flag on the account that they're about to launder money. That's a challenge. You almost have to react to that single red flag in real time to be able to stop it."
>
> - Interviewee

Illicit Funds Moved by Money Mules

By Region:

All Europe
$58.2B

EU
$37.2B

UK
$6.9B

Nordics
$3.2B

Spotlight:
Cross-Border Illicit Activity

Cross-border transactions have tripled in the last decade,[2] signifying a growing exchange of funds between countries in an increasingly complex global financial system. In this highly interconnected environment, criminals are exploiting cross-border transactions to circulate funds for international criminal organizations and money laundering networks, moving the proceeds of drug trafficking and fraud, and facilitating terrorist and proliferation financing. Our report reveals that the scale of cross-border illicit funds movement is a significant risk to the European financial system.

Europe's cross-border illicit flows are estimated to be $194.9 billion, representing more than a quarter of the region's total money laundering activity.

Germany, France, Italy, and the UK represented more than half of all cross-border illicit funds.

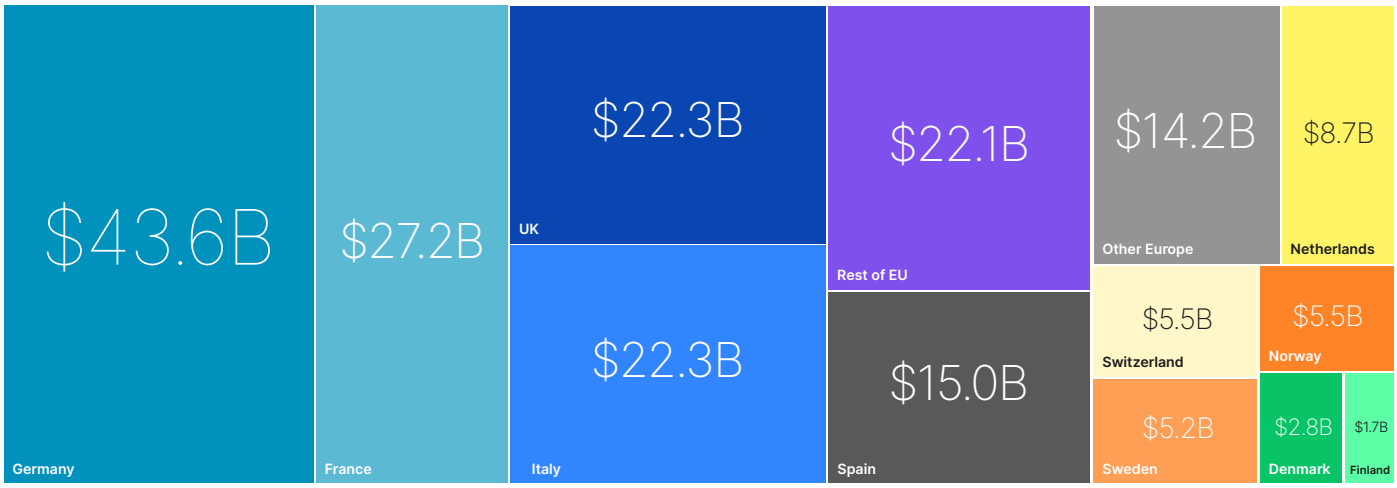
Criminals are moving illicit funds across borders to obscure the source or destination of funds and render recovery of funds more challenging. International illicit activity undermines the integrity of the financial system in both the sending and receiving countries and underscores the need for the global financial system to prioritize financial crime risk in cross-border transactions.

Moving forward, the adoption of the ISO 20022 international payments standard by fast and instant payments systems, including in the UK and EU, will facilitate greater interoperability of cross-border across the financial industry, and the G20 is aligned on a Roadmap for Cross-Border Payments,[8] endeavoring to improve the speed, transparency and cost of these transactions to promote economic growth and international trade. As Europe prioritizes innovation in the payments space, making cross-border payments faster and more accessible than ever, these vectors can be exploited by money mules and threat actors, unless the industry works together to prioritize effective fraud prevention and AML/CFT measures, to address the international nature of financial crime threats in cross-border payments.

$194.9B

Cross-Border Illicit Flows
Across Europe

Cross-Border Illicit Funds Movement By Region



Industry Insights: Challenges and Priorities

European banks are at the forefront of the fight against financial crime, facing many challenges that contribute to an increasingly complex operating environment. While responding to rapidly evolving fraud and money laundering threats, risk in real-time payments, and cross-border transactions, research from Nasdaq and Boston Consulting Group's 2025 Complexity Report[2] shows that in the last decade the financial industry has also experienced a two-times increase in annual changes to global regulations.

In managing this growing complexity, banks are contending with burdensome manual processes and the limitations of siloed data in complicated technology stacks, leading to rising operational costs. To further prioritize financial crime prevention, institutions are evaluating how people, process and technology investments can improve the efficiency of compliance operations and increase the effectiveness of their anti-financial crime efforts. European banks broadly recognize that the right investments in these areas can help them overcome evolving financial crime threats and the complexities of changing regulatory obligations.

Navigating Regulatory Change

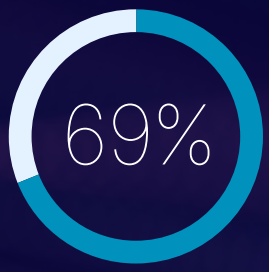
Europe is experiencing significant change in AML/CFT, sanctions and payments regulation. As policymakers aim to strengthen anti-money laundering measures and fraud prevention, and safeguard the broader financial system, substantial regulatory changes also place an onus on banks to navigate a wide range of compliance expectations from multiple authorities.

As these considerable regulatory changes unfold in Europe, banks are looking for clear guidance from regulators in implementing changes and ensuring compliance with the latest standards and new requirements. By fostering a supportive and transparent regulatory environment, regulators can help banks navigate the complexities of new regulations, ultimately enhancing the overall effectiveness of their crime-fighting efforts.

EU - AML Package: The publication of the EU's AML package in 2024 included the "Single Rulebook" regulation (AMLR), and set out to align national requirements, such as customer due diligence, while strengthening overall AML and CFT efforts across the region. One such provision in the regulations is Article 75 which allows for information sharing partnerships between institutions both nationally and across EU borders. Now, with a pan-EU authority, the AMLA will provide supervision and oversight, in coordination with national level authorities. AMLD6 will guide member states in implementing measures that aim for more robust money laundering protections while avoiding misalignment of rules at the national level.

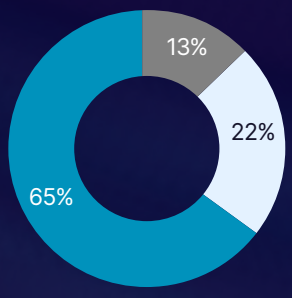
The transformation of the EU's AML regime will result in changes to AML programs with 69% of respondents saying they anticipate an increase in regulatory oversight with the new AMLA, and 65% noting that their institutions are preparing for changes to meet the new regulatory requirements established by the new AML regulations.

Impact of Regulatory Changes from AMLR on AFC Program (EU only)



Expect an Increase in Regulatory Oversight

Preparing for Regulatory Changes from AMLR
EU Only



EU - Payment Services Regulation (PSR) and Payments Services Directive (PSD3): Evolving consumer protections and open banking considerations from the former directive are being integrated into new requirements. With its final form currently being negotiated, policymakers are looking to the PSR to safeguard the payments system with stronger prevention for authorized payments fraud through technology adoption, sharing of intelligence, liability models, and other preventative measures. To support cross-border and cross-currency payments, PSD3 aims to establish increased transparency, anti-fraud controls and reporting requirements to allow for improved tracking, authentication, and validation of payments.

UK - Economic Crime and Corporate Transparency Act (ECCTA 2023): Since 2023, new provisions under the ECCTA have come into force to strengthen financial crime prevention in the UK. These new measures include reforms to improve transparency of corporations, as well as additional powers for law enforcement to recover crypto assets linked to proceeds of crime. A focus on fraud prevention in the UK is evidenced through a new failure to prevent fraud offence which will be applicable in September 2025, putting heightened emphasis on fraud risk assessments and controls for covered financial services organizations. In addition to other changes in the Act, new provisions to enable bank-to-bank information sharing came into force early in 2024, providing a new mechanism for the UK to root out fraud and financial crime, and work together to prevent illicit activity.

In our survey, 75% of UK respondents noted they were preparing for substantive changes to their financial crime program stemming from new regulatory requirements in the ECCTA.

Overcoming Operational Challenges: People, Process and Technology

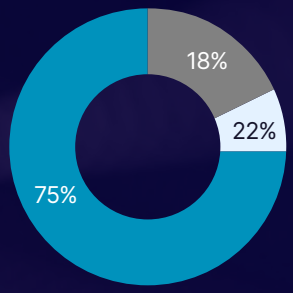
While addressing changes in regulations remains a priority for banks, investing in anti-financial crime programs to mitigate the growing complexity of financial crime and fraud threats is considered equally important.

Half of respondents felt their organization had a strong financial crime prevention culture within their institution, yet internally, banks face operational challenges that hinder their ability to be more efficient and effective. This includes a reliance on manual processes, while working with siloed data and outdated technology. Our research reveals that only 22% of respondents believe their institutions had adequate resources including personnel or technology to combat financial crime.

The constraints of siloed data, legacy technologies and manual processes create inefficiencies within banks. Managing multiple systems and data sources impedes workflows and without the advantage of automation, compliance processes can become laborious and time consuming. When respondents were asked to describe their anti-financial crime programs, 28% stated there were meaningful shortcomings within their organization. Legacy, rules-based solutions

Preparing for Regulatory Changes from the ECCT Act

UK only



Respondents' view of organization and operations

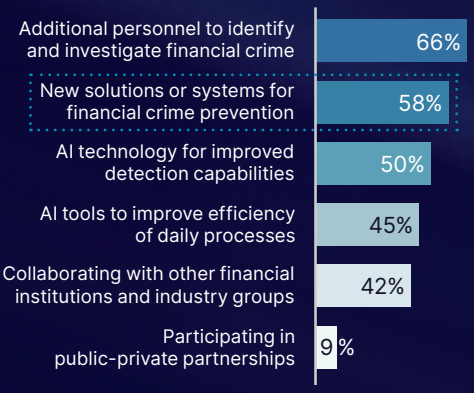
All Europe

22% My Institution has Adequate Resources to Combat Financial Crime

37% My Institution Takes a Risk-Based Approach with Tailored Controls

50% My Institution has a Strong Culture of Financial Crime Prevention

Planned Opportunities to Enhance Financial Crime Prevention



can produce high false positive rates pulling resources away from detecting and managing true high-risk activities and more critical investigations. To respond to these constraints, 66% of respondents named investing in additional personnel as their as their top opportunity to enhance financial crime prevention, followed closely by investments in technology and AI.

Focusing on Risk

Adopting a risk-based approach to financial crime helps banks to scale and allocate resources based on risk, allowing them to focus resources on higher-risk priorities. While 37% of financial institutions are taking a risk-based approach to financial crime compliance, there is a clear opportunity for the industry to support further adoption. This approach can help banks offset increasing costs, by concentrating resources and tailoring controls where they will have the greatest impact on anti-financial crime efforts.

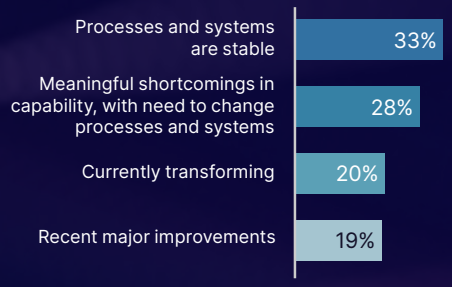
Moreover, in response to changing regulations, banks have implemented multiple solutions to maintain compliance and manage the complexity that comes with ever-changing rules resulting in increased operational costs, added complexity and fragmented processes. A transformative shift towards technology will help banks offset the need for additional headcount in daily compliance processes and allow experts to focus on higher-risk and critical areas of their business.

Integrating Fraud Prevention and AML

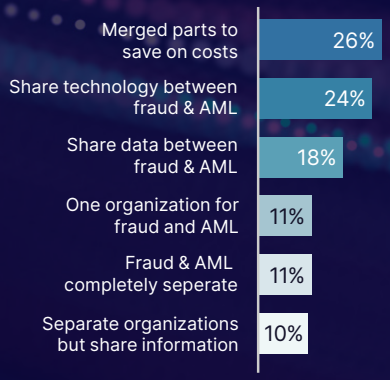
Within banks, integrating fraud and AML teams, combining processes, and leveraging shared technology systems across functions, can help break down silos across a financial institution, improve communication and coordination, increase efficiency, and enhance prevention efforts.

The approach of combining elements of fraud and AML operations to create an integrated anti-financial crime program is known as a FRAML approach and has not been readily adopted within banks in Europe based on survey responses.

Evaluation of Current AFC Program



Organizational Approach to Integrating Fraud and AML (FRAML)



Spotlight: Frameworks for Information Sharing

From repeat fraudsters and crime rings to networks of money mules moving proceeds of crime, criminals are exploiting the fragmented nature of the financial system to evade detection. More than ever, it is essential for the financial industry to break down siloes by embracing collaborative approaches and information sharing to keep pace with the sophisticated, evolving nature of financial crime.

Information sharing can help banks streamline operations, gain a more complete view of criminal networks, conduct stronger anti-financial crime investigations, improve reporting to law enforcement, and proactively prevent illicit activity and fraud. As criminals grow more connected, jurisdictions around the world are modernizing AML frameworks with regulatory policies to enable financial sector information sharing.

Until recently, there were limitations to industry collaboration on the range of financial crime risks that threaten Europe's financial system. There are mechanisms to enable banks to share intelligence specifically for fraud or cyber-related crimes, as well as highly localized legal gateways for banks to collaborate within EU countries, including Estonia, Latvia and Sweden. However, new legislative and regulatory changes in Europe can enable greater bank-to-bank information sharing and deliver on a step change in financial crime prevention, including terrorist financing, money laundering, fraud and other predicate crimes.

UK: ECCTA

Provisions in the UK's Economic Crime and Corporate Transparency Act came into force in early 2024, to disapply civil liability for private-to-private information sharing domestically for the purposes of preventing, investigating, or detecting money laundering, terrorist financing, bribery, sanctions evasion, tax evasion, market abuse and fraud. In implementing these measures, the UK Home Office[9] underscores the value of sharing customer information to improve the accuracy of detection and quality of reporting, as well as to "gain a network view of the economic crime risk" and "a greater ability to take upstream preventative action and disrupt illicit activity."

Guidance on the ECCTA information sharing measures also highlights the potential for banks and other regulated firms to leverage technology platforms and consortium approaches for the various methods of sharing information.

Despite the intent of these measures to provide clarity and promote confidence for financial institutions in sharing information with protections from liability, only 50% of UK respondents were more likely to share information

Information Sharing Case Study: USA PATRIOT Act

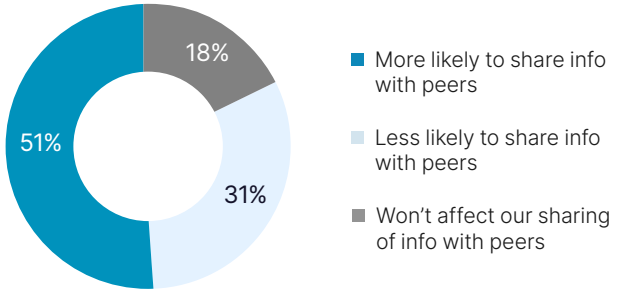
Information sharing has proven effective in jurisdictions such as the United States where section 314(b) of the USA PATRIOT Act offers a safe harbor for banks to engage in private-to-private information sharing.

Enacted in 2001, this framework enables a wide range of approaches to improve the efficiency and effectiveness of anti-financial crime efforts, including bank-to-bank messaging services; joint investigations; adverse incident alerting; as well as public-private information sharing investigations and joint reporting to law enforcement.

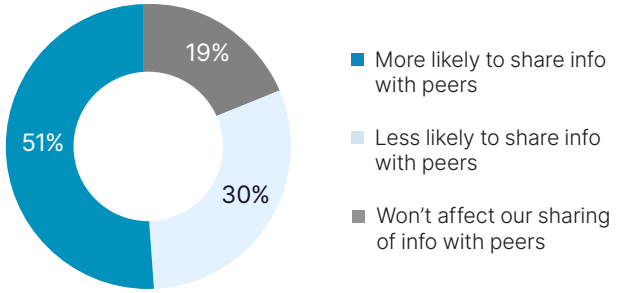
with their peers. A significant portion of those that were *less* likely to collaborate cited concerns over competition as their main reason for not sharing information, followed by a lack of regulatory guidance, as well as legal and privacy risks. The perceived burden of implementing new procedures raised concerns among respondents due to inadequate resources, budget or technology.

With this recent pan-EU regulation, banks surveyed are looking to benefit from information sharing to strengthen their AML/CFT programs, with more than half of EU respondents noting a greater likelihood of sharing information with other banks.

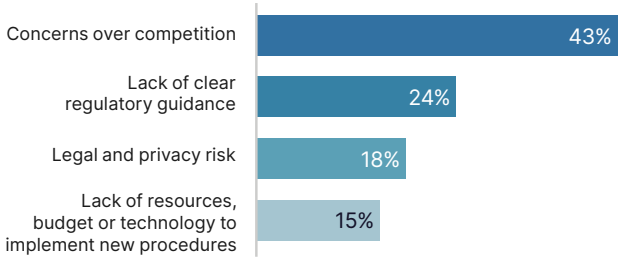
Plans to Share Information with Banks Under the ECCT (UK Only)



Plans to Share Information with Banks Under AMLR Article 75 (EU Only)



Barriers to Sharing Information with Banks
(UK respondents who were less likely to share information)



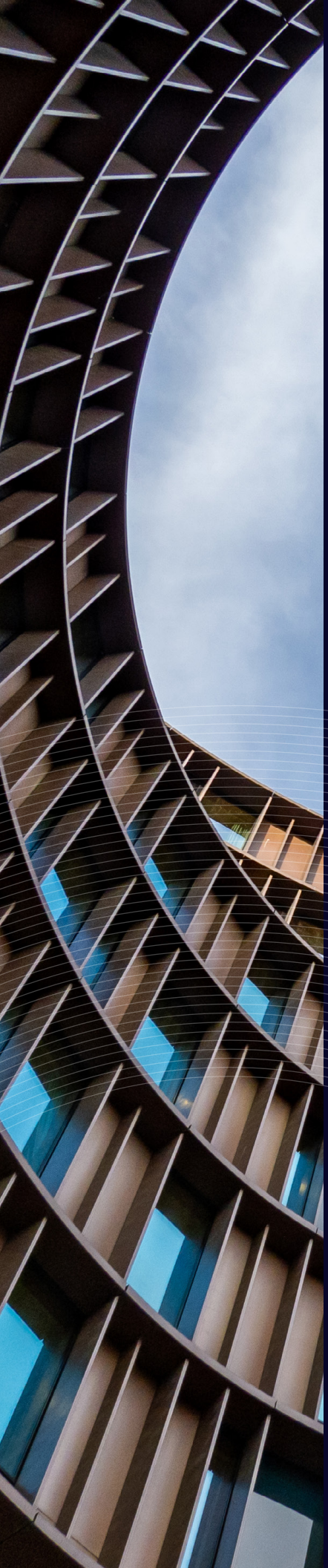
Barriers to Sharing Information with Banks
(EU respondents who were less likely to share information)

EU: AMLR Article 75

Under Article 75 provisions within the newly adopted AML Regulation, financial institutions in EU member states are now able to form partnerships to share information as part of their AML/CFT and financial crime compliance programs, including cross-border partnerships within the EU. These partnerships can also extend beyond private-to-private (bank-to-bank) information sharing, with allowances for partnerships with public sector participants such as AML/CFT supervisors, Financial Intelligence Units (FIUs) and other competent authorities. In addition, participants must verify their partnerships with their AML supervisory authority for compliance with expectations, in advance of operationalizing any sharing of information. By enabling greater collaboration across the EU's public and private sector, these new provisions for information sharing represent a significant opportunity for a step change for banks' anti-financial crime efforts.

However, reflecting the complexity of bank's current operating environment, 30% of respondents were less likely to share information, citing a lack of clear regulatory guidance as the primary reason, as well as concerns over legal and privacy risk, competition, and a lack of resources, budget and technology to implement changes to their program.

As the UK and EU make significant progress toward enabling collaboration, it is critical that industry stakeholders, including policymakers, regulators and supervisors, are aligned on priorities for prevention, and elevate information sharing as a valuable tool. in the fight against financial crime. Continued support and clarity from national authorities is needed to empower banks to take full advantage of this opportunity with confidence.



Insights: Opportunities for the Industry

There are opportunities for the industry to progress in its fight against financial crime. Survey respondents were aligned on the need to improve and modernize regulations, remove barriers to collaboration, and invest in innovation for greater effectiveness in their efforts to address financial crime threats.

Aligning & Modernizing Regulations

Banks are facing an increasingly complex regulatory landscape with multiple, fragmented standards which can hinder innovation and cooperation across jurisdictions. Regulations often lag behind the latest developments in technology and lack flexibility to adapt to changing market dynamics and emerging financial crime trends.

Anti-financial crime professionals are emphasizing the need to address outdated compliance regulations, with a focus on greater support for banks to innovate with technology. For financial crime management programs, this can include a range of AI capabilities and use cases. When asked about the threat of APP fraud specifically, 21% of respondents noted that consortium and big data technologies, as well as data-driven advanced analytics, were among the most effective means to combat losses from authorized push payment scams.

> "Ultimately a long-term sustainable model is about being able to collaborate, to share information, to try and get to that place where not only are you sharing with other institutions and with law enforcement, but also online platforms and tech companies."
>
> - UK FIU Interviewee

Clear guidance from regulators on the implementation of typology-specific priorities is crucial for banks to navigate the complexities of compliance, while effectively mitigating risk. By identifying and communicating priorities, regulators can empower banks to allocate resources more efficiently, shifting resources from low-value tasks and focus on activities that pose highest risk to their institution. Regulators' endorsement of risk-based methodologies can encourage banks to develop tailored solutions that address specific priorities, ultimately enhancing overall program efficacy.

Breaking Down Barriers to Collaboration

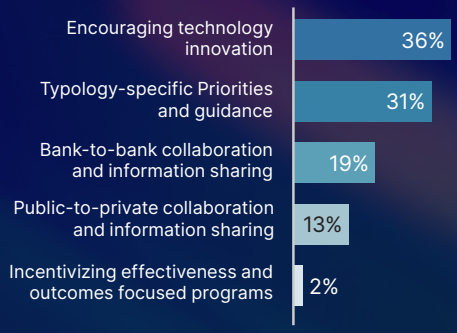
Within Europe there has been a shift towards more collaboration within the financial industry. Given the interconnected nature of the financial system and the speed which with money moves today, collaboration between financial institutions and public sector entities is crucial to disrupt criminal organizations and safeguard the financial system.[10]

As crimes grow more sophisticated, there is a growing need to share information between financial institutions and with the public sector — to more effectively detect criminal activity that spans banks and borders.

Banks highlighted the impact of working with law enforcement to understand emerging threats; engaging with regulators on financial crime priorities and typologies; and sharing information with other institutions, emphasizing the importance of industry collaboration.

> "The regulator needs to come to the table, frankly."
>
> - Interviewee

Areas for Improved Regulation



> "While the policy consensus to enable private sector entities to collaborate in response to economic crime threats is now well established at the domestic level in major economies and financial centres, policy-discussions about cross-border private sector collaborations are less well developed – particularly in the fraud and scams domain of economic rime risk."
>
> - Nick J. Maxwell
> Future of Financial Intelligence Sharing (FFIS) research programme
>
> *A new era for private sector collaboration to fight economic crime* (2025)[10]

The need for regulatory clarity and guidance to support private-private and public-private information sharing was a top concern for banks across the UK and EU. Policymakers and public sector stakeholders play a key role in helping to break down the barriers to adopting collaborative approaches, and bolstering banks' crime-fighting effectiveness.

Investing in Innovation

Investments in AI, big data, and technological innovations are poised to revolutionize financial crime detection and prevention, driving significant advancements in the industry's ability to combat sophisticated threats.

European financial institutions recognize the potential of these innovations to help save time and resources and optimize their compliance programs for operational efficiency. Banks are looking to policymakers and regulators to provide clear frameworks, guidance and support as they incorporate more advanced technology solutions and systems into their financial crime management programs.

Banks are seizing the opportunity to innovate with AI, with respondents viewing machine learning and AI technology as having the biggest potential impact on transaction monitoring and fraud prevention. Most institutions surveyed were exploring use cases or using generative AI (GenAI) today and see significant potential in using GenAI for compilation and analysis of risk profiles, beneficial ownership information and analysis, copilots and assistants for analysts, and alert explanation/ narrative building.

Across Europe, banks are planning to increase their spending on AI and/ or machine learning in the next one to two years, to help overcome the limitations of manual processes and legacy solutions, streamline operations and strengthen prevention efforts.

Banks are adopting cloud technology that powers consortium data approaches and network-level analytics. Consortium analytics provide insights into financial crime risk across a network of financial institutions, without sharing personally identifiable information between banks. Consortium-based technology can be deployed as an integrated system or through APIs and while effective for all types of financial crime detection, it is most effective for fraud detection. This detection approach, which is not possible for a single bank, is especially powerful for payments fraud as it identifies risk at a network level and determines the likelihood of fraud associated with the receiving side of a payment.

In addition to improving detection rates for payments fraud, consortium insights can lower false positives, reduce customer friction, and protect consumers and institutions from loss. Adopting a consortium-based approach is particularly salient for European banks today, given the rise in APP fraud scams, money mule activity, and cross border flow of funds.

Plans to invest in AI in the next 1–2 years

By Region:

All Europe

UK

EU

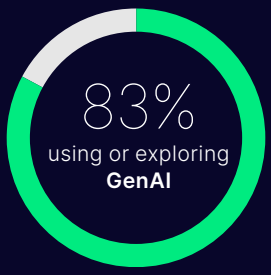
Nordics

With the right investments in technologies such as cloud, consortium data analytics and AI, banks can reduce time spent on manual processes and the inefficiencies of disconnected legacy solutions. The advanced analytical and automation capabilities these solutions can help offset unnecessary hiring and increasing operational spend for compliance processes and allow for better resource allocation towards higher value risk activities. Research from Nasdaq and BCG[2] estimates that by employing new technology systems that can streamline processes and enhance overall efficiency, banks can reduce operational costs by 10–20% for risk and compliance functions.

> "Through its collective efforts to innovate, Europe is poised be a world leader in the fight against financial crime and safeguarding the integrity of the global financial system."
>
> - Stephanie Champion,
> EVP & Head of Nasdaq Verafin,
> Financial Crime Management Technology, Nasdaq

Use of GenAI in AFC Processes

All Europe



Banks can reduce operational costs by

10–20%

for risk and compliance functions

A Unifying Call to Collective Action

Now is the time for industry stakeholders across Europe to take collective action in the fight against financial crime and innovate ahead of evolving criminal threats. Through a unified effort, industry stakeholders can come together to protect society from criminal exploitation, ensure strong and resilient economies across the region, and safeguard the wider financial system from harm.

Align on Priorities for Financial Crime Prevention.
Financial crime has significant impacts on both the economy and society. To effectively combat fraud and money laundering, a unified approach involving all stakeholders—regulators, supervisors, law enforcement, and banks—is essential. By prioritizing financial crime prevention and fostering collaboration across the public and private sectors the industry can work together to safeguard the integrity of the European financial system.

Collaborate Across Sectors and Borders to Root Out Crime.
It is crucial that the financial industry embrace industry-wide collaboration and foster networks to break down siloes that hinder anti-financial crime efforts across banks and borders. Europe's new frameworks for information sharing are creating opportunities for the financial industry to collaborate in disrupting fraud and money laundering, ensuring compliance, and fostering public-private sector alignment for rooting out crime in Europe.

Accelerate Innovation Through Advanced Technology.
Adopting technology is vital for managing the complexity of financial crime as it eases operational burdens, reduces costs, and allows the industry to focus on higher-priority concerns — with the support of regulators and supervisors driving significant change. By embracing new technologies and capitalizing on innovative, consortium data approaches, European financial institutions can revolutionize crime fighting.

Europe is poised to establish a new standard of innovative, collaborative leadership in combating financial crime — within and beyond its borders. With collective effort and a shared vision, the industry can work together to create a more secure, trusted and resilient future for the region and safeguard the integrity of the global financial system.

References & Footnotes

[1] *2024 Global Financial Crime Report*, Nasdaq, 2024

[2] *The New Growth Imperative: Cutting Through Complexity in the Financial System*, Nasdaq and Boston Consulting Group, 2025

[3] *Abuse of Older People*, World Health Organization, 2024

[4] *Authorised Push Payment Reimbursement Models, Fighting Fraud in Global Real-Time Payment Systems*, Nasdaq Verafin & Jonathan Frost, 2024

[5] *APP Fraud Reimbursement Protections*, Payment Systems Regulator, 2025

[6] *Government Approach to Authorised Push Payment Scam Reimbursement*, HM Treasury, 2022

[7] *The Wolfsberg Group on Countering Terrorist Financing*, The Wolfsberg Group, 2024

[8] *G20 Roadmap for Enhancing Cross-Border Payments: Consolidated Progress Report for 2024*, Financial Stability Board, 2024

[9] *Guidance on the information sharing measures in the Economic Crime and Corporate Transparency Act 2023*, Government of the United Kingdom, 2024

[10] *A new era for private sector collaboration to fight economic crime*, Future of Financial Intelligence Sharing (FFIS) research programme, Maxwell, N (2025)

Appendix A – Regional & Country Level Estimates

Developed by Celent Research and Oliver Wyman as referenced in the Methodology section of this report.

Financial Crime: Global Overview

2023 (Millions of USD)		Total Global	Europe	Middle East	Africa	Asia-Pacific	Americas
Consumer & Business Fraud (Third-Party/Authorized)	**Aggregate Total**	**43,611**	**11,720**	**2,035**	**1,732**	**14,292**	**13,831**
	Business Email Compromise/ Phishing/Data Breach	9,973	2,561	355	146	1,906	5,005
	Business Email Compromise	6,679	1,715	238	98	1,277	3,351
	Phishing	368	95	13	5	70	185
	Data Breach	2,927	751	104	43	559	1,469
	Impersonation Scams: Charity, Business, Government, Law Enforcement	6,821	1,182	164	68	3,814	1,593
	Confidence: Romance, Family Relative Impersonation	3,776	698	257	212	1,677	932
	Advance Fee/Lottery/Prize/Grant Fraud	19,146	6,824	955	395	6,249	4,723
	Employment Fraud	3,895	456	304	912	646	1,578
Bank Fraud (First-Party/ Unauthorized)	**Aggregate Total**	**441,966**	**91,838**	**4,157**	**1,596**	**207,130**	**137,246**
	Payment Fraud: Credit Transfers and Direct Debits	386,835	88,499	4,025	1,525	190,171	102,615
	Check Fraud	26,589	442	19	0	5,101	21,027
	Credit Card Fraud	28,542	2,897	113	71	11,857	13,603
Total Fraud		**485,577**	**103,558**	**6,192**	**3,328**	**221,422**	**151,077**
Fraud Against Elder Victims (Subset of Total Fraud)		**77,703**	**19,921**	**3,521**	**1,658**	**28,244**	**24,359**
Money Laundering	**Aggregate Total**	**3,099,166**	**750,205**	**136,064**	**65,362**	**1,092,252**	**1,055,282**
	Terrorist Financing: Arms Trafficking, Foreign, Domestic, Domestic Violent Extremist (DVE)	11,472	2,742	651	308	2,665	5,106
	Human Trafficking: Sex Trafficking, Forced Labor (not Forced Marriage)	346,725	82,210	17,087	8,307	130,057	109,064
	Drug Trafficking & DTOs	782,944	178,036	32,220	16,192	268,751	287,745
	Other Crimes: Organized Crime, Fraud, Corruption, etc.	1,958,024	487,217	86,106	40,555	690,779	653,367
	GDP		**32,603,422**	**4,115,789**	**2,539,835**	**36,067,384**	**34,864,637**
Ratio: Consumer & Business Fraud / GDP			0.036%	0.049%	0.068%	0.040%	0.040%
Ratio: Bank and Card Fraud / GDP			0.28%	0.10%	0.06%	0.57%	0.39%
Ratio: Money Laundering / GDP			2.30%	3.31%	2.57%	3.03%	3.03%

Financial Crime: Europe Overview

2023 (Millions of USD)		Total Europe	UK	EU	Other Europe
Consumer & Business Fraud (Third-Party/Authorized)	**Aggregate Total**	**11,720**	**2,717**	**6,443**	**2,561**
	Business Email Compromise/Phishing/Data Breach	2,561	328	1,540	693
	Business Email Compromise	1,715	220	1,031	464
	Phishing	95	12	57	26
	Data Breach	751	96	452	203
	Impersonation Scams: Charity, Business, Government, Law Enforcement	1,182	151	711	320
	Confidence: Romance, Family Relative Impersonation	698	181	362	155
	Advance Fee/Lottery/Prize/Grant Fraud	6,824	1,980	3,603	1,241
	Employment Fraud	456	76	228	152
Bank Fraud (First-Party/ Unauthorized)	**Aggregate Total**	**91,838**	**30,492**	**55,017**	**6,329**
	Payment Fraud: Credit Transfers and Direct Debits	88,499	29,650	53,189	5,660
	Check Fraud	442	49	363	30
	Credit Card Fraud	2,897	793	1,464	640
Total Fraud		**103,558**	**33,208**	**61,460**	**8,890**
Fraud Against Elder Victims (Subset of Total Fraud)		**19,921**	**2,618**	**11,527**	**5,776**
Money Laundering	**Aggregate Total**	**750,205**	**98,654**	**438,406**	**213,145**
	Terrorist Financing: Arms Trafficking, Foreign, Domestic, Domestic Violent Extremist (DVE)	2,742	300	1,580	862
	Human Trafficking: Sex Trafficking, Forced Labor (not Forced Marriage)	82,210	11,956	47,826	22,427
	Drug Trafficking & DTOs	178,036	22,363	107,091	48,582
	Other Crimes: Organized Crime, Fraud, Corruption, etc.	487,217	64,034	281,909	141,273
	Cross Border Illicit Funds Movement	**194,920**	**22,287**	**148,558**	**24,075**
	Money Mules (Cross Border)	19,776	2,162	15,034	2,580
	MM as a % of Cross Border Illicit funds	10.1%	9.7%	10.1%	10.7%
	Cross Border MM as a % of total ML	2.6%	2.2%	3.4%	1.2%
	Domestic Illicit Funds Movement	**555,285**	**76,368**	**289,848**	**189,070**
	Money Mules (Domestic)	38,390	4,784	22,184	11,423
	MM as a % of Domestic Illicit funds	6.9%	6.3%	7.7%	6.0%
	Domestic MM as a % of total ML	5.1%	4.8%	5.1%	5.4%
	Money Mules Total	**58,167**	**6,946**	**37,218**	**14,003**
	MM as a % of Total ML	7.8%	7.0%	8.5%	6.6%
	GDP	**32,603,422**	**3,162,788**	**17,140,634**	**8,475,054**
	Ratio: Consumer & Business Fraud / GDP	0.036%	0.086%	0.038%	0.030%
	Ratio: Bank and Card Fraud / GDP	0.28%	0.96%	0.32%	0.07%
	Ratio: Money Laundering / GDP	2.30%	3.12%	2.56%	2.51%

Financial Crime: European Union

2023 (Millions of USD)		EU	Denmark	Finland	Sweden	France	Germany	Italy	Neth.	Spain	Rest of EU
Consumer & Business Fraud (Third-Party/ Authorized)	**Aggregate Total**	**6,443**	**161**	**59**	**216**	**1,155**	**1,817**	**769**	**384**	**541**	**1,341**
	Business Email Compromise/ Phishing/Data Breach	1,540	45	30	45	297	435	191	93	131	272
	Business Email Compromise	1,031	24	17	28	199	291	128	63	88	193
	Phishing	57	3	1	4	11	16	4	3	5	9
	Data Breach	452	18	12	13	87	128	56	27	38	72
	Impersonation Scams: Charity, Business, Government, Law Enforcement	711	22	12	25	137	201	88	43	61	121
	Confidence: Romance, Family Relative Impersonation	362	9	2	10	14	265	14	15	23	10
	Advance Fee/Lottery/Prize/Grant Fraud	3,603	53	9	128	589	917	448	219	307	934
	Employment Fraud	228	32	6	8	117	-	28	14	19	3
Bank Fraud (First-Party/ Unauthorized)	**Aggregate Total**	**55,017**	**600**	**545**	**870**	**24,660**	**11,374**	**2,903**	**8,147**	**5,074**	**844**
	Payment Fraud: Credit Transfers and Direct Debits	53,189	591	525	835	23,609	11,268	2,685	8,083	4,780	814
	Check Fraud	363	1	2	8	261	5	21	1	45	19
	Credit Card Fraud	1,464	8	18	27	790	102	197	63	248	11
Total Fraud		**61,460**	**761**	**604**	**1,086**	**25,816**	**13,191**	**3,672**	**8,530**	**5,615**	**2,185**
Fraud Against Elder Victims (Subset of Total Fraud)		**11,527**	**269**	**190**	**409**	**2,056**	**3,472**	**1,432**	**699**	**982**	**2,017**
Money Laundering	**Aggregate Total**	**438,406**	**8,193**	**5,018**	**15,254**	**80,214**	**128,699**	**65,752**	**25,654**	**44,302**	**65,320**
	Terrorist Financing: Arms Trafficking, Foreign, Domestic, Domestic Violent Extremist (DVE)	1,580	42	18	77	363	531	269	132	123	25
	Human Trafficking: Sex Trafficking, Forced Labor (not Forced Marriage)	47,826	864	533	1,642	9,288	13,591	8,048	3,088	5,521	5,251
	Drug Trafficking & DTOs	107,091	2,425	1,424	3,686	20,268	29,658	17,204	8,402	11,063	12,962
	Other Crimes: Organized Crime, Fraud, Corruption, etc.	281,909	4,861	3,044	9,850	50,296	84,919	40,230	14,033	27,595	47,082
	Cross Border Illicit Funds Movement	**148,558**	**2,776**	**1,700**	**5,169**	**27,181**	**43,611**	**22,281**	**8,693**	**15,012**	**22,134**
	Money Mules (Cross Border)	15,034	260	151	476	2,637	4,481	2,401	919	1,543	2,166
	MM as a % of Cross Border Illicit funds	10.1%	9.4%	8.9%	9.2%	9.7%	10.3%	10.8%	10.6%	10.3%	9.8%
	Cross Border MM as a % of total ML	3.4%	3.2%	3.0%	3.1%	3.3%	3.5%	3.7%	3.6%	3.5%	3.3%
	Domestic Illicit Funds Movement	**289,848**	**5,417**	**3,318**	**10,085**	**53,033**	**85,088**	**43,471**	**16,961**	**29,290**	**43,186**
	Money Mules (Domestic)	22,184	384	224	702	3,855	6,679	3,508	1,312	2,220	3,299
	MM as a % of Domestic Illicit funds	7.7%	7.1%	6.8%	7.0%	7.3%	7.8%	8.1%	7.7%	7.6%	7.6%
	Domestic MM as a % of total ML	5.1%	4.7%	4.5%	4.6%	4.8%	5.2%	5.3%	5.1%	5.0%	5.1%
	Money Mules Total	**37,218**	**644**	**375**	**1,178**	**6,492**	**11,160**	**5,909**	**2,231**	**3,764**	**5,465**
	MM as a % of Total ML	8.5%	7.9%	7.5%	7.7%	8.1%	8.7%	9.0%	8.7%	8.5%	8.4%
	GDP	**17,140,634**	**400,167**	**281,887**	**608,122**	**2,866,392**	**4,194,357**	**2,128,981**	**1,039,681**	**1,460,334**	**4,382,749**
	Ratio: Consumer & Business Fraud / GDP	0.038%	0.043%	0.028%	0.038%	0.040%	0.043%	0.038%	0.038%	0.038%	0.031%
	Ratio: Bank and Card Fraud / GDP	0.32%	0.15%	0.19%	0.14%	0.86%	0.27%	0.14%	0.78%	0.35%	0.02%
	Ratio: Money Laundering / GDP	2.56%	2.05%	1.78%	2.51%	2.80%	3.07%	3.09%	2.47%	3.03%	1.49%

Financial Crime: Nordic and Other European Countries

2023 (Millions of USD)		Nordic Countries	Denmark	Finland	Norway	Sweden	Switzerland
Consumer & Business Fraud (Third-Party/Authorized)	**Aggregate Total**	**650**	**161**	**59**	**215**	**216**	**308**
	Business Email Compromise/Phishing/Data Breach	172	45	30	53	45	76
	Business Email Compromise	105	24	17	36	28	51
	Phishing	9	3	1	1	4	1
	Data Breach	59	18	12	16	13	22
	Impersonation Scams: Charity, Business, Government, Law Enforcement	84	22	12	25	25	35
	Confidence: Romance, Family Relative Impersonation	25	9	2	5	10	9
	Advance Fee/Lottery/Prize/Grant Fraud	315	53	9	125	128	177
	Employment Fraud	54	32	6	8	8	11
Bank Fraud (First-Party/ Unauthorized)	**Aggregate Total**	**2,788**	**600**	**545**	**769**	**870**	**1,803**
	Payment Fraud: Credit Transfers and Direct Debits	2,696	591	525	745	835	1,752
	Check Fraud	18	1	2	3	8	2
	Credit Card Fraud	74	8	18	21	27	49
Total Fraud		**3,438**	**761**	**604**	**984**	**1,086**	**2,111**
Fraud Against Elder Victims (Subset of Total Fraud)		**1,293**	**269**	**190**	**399**	**409**	**567**
Money Laundering	**Aggregate Total**	**41,131**	**8,193**	**5,018**	**12,666**	**15,254**	**24,550**
	Terrorist Financing: Arms Trafficking, Foreign, Domestic, Domestic Violent Extremist (DVE)	187	42	18	50	77	98
	Human Trafficking: Sex Trafficking, Forced Labor (not Forced Marriage)	4,643	864	533	1,603	1,642	2,276
	Drug Trafficking & DTOs	10,533	2,425	1,424	2,999	3,686	5,109
	Other Crimes: Organized Crime, Fraud, Corruption, etc.	25,768	4,861	3,044	8,014	9,850	17,067
	Cross Border Illicit Funds Movement	**13,938**	**2,776**	**1,700**	**4,292**	**5,169**	**5,546**
	Money Mules (Cross Border)	1,293	260	151	407	476	561
	MM as a % of Cross Border Illicit funds	9.3%	9.4%	8.9%	9.5%	9.2%	10.1%
	Cross Border MM as a % of total ML	3.1%	3.2%	3.0%	3.2%	3.1%	2.3%
	Domestic Illicit Funds Movement	**27,194**	**5,417**	**3,318**	**8,374**	**10,085**	**19,004**
	Money Mules (Domestic)	1,910	384	224	600	702	1,242
	MM as a % of Domestic Illicit funds	7.0%	7.1%	6.8%	7.2%	7.0%	6.5%
	Domestic MM as a % of total ML	4.6%	4.7%	4.5%	4.7%	4.6%	5.1%
	Money Mules Total	**3,203**	**644**	**375**	**1,006**	**1,178**	**1,804**
	MM as a % of Total ML	7.8%	7.9%	7.5%	7.9%	7.7%	7.3%
	GDP	**1,922,177**	**400,167**	**281,887**	**593,727**	**608,122**	**842,979**
	Ratio: Consumer & Business Fraud / GDP	0.036%	0.043%	0.028%	0.038%	0.038%	0.038%
	Ratio: Bank and Card Fraud / GDP	0.15%	0.15%	0.19%	0.13%	0.14%	0.21%
	Ratio: Money Laundering / GDP	2.14%	2.05%	1.78%	2.13%	2.51%	2.91%

Cautionary Note Regarding Forward-Looking Statements:
Information set forth in this report contains forward-looking statements that involve a number of risks and uncertainties. Nasdaq cautions readers that any forward-looking information is not a guarantee of future performance and that actual results could differ materially from those contained in the forward-looking information. Forward-looking statements can be identified by words such as "can" and "will," and other words and terms of similar meaning. Such forward-looking statements include, but are not limited to, statements related to anticipated efficiencies, cost savings, and loss reductions. Forward-looking statements involve a number of risks, uncertainties or other factors beyond Nasdaq's control. These risks and uncertainties are detailed in Nasdaq's filings with the U.S. Securities and Exchange Commission, including its annual reports on Form 10-K and quarterly reports on Form 10-Q which are available on Nasdaq's investor relations website at http://ir.nasdaq.com and the SEC's website at www.sec.gov. Nasdaq undertakes no obligation to publicly update any forward-looking statement, whether as a result of new information, future events or otherwise.

Nasdaq, a leading global technology company, is committed to advancing anti-financial crime efforts by delivering world-leading solutions that safeguard the financial system and strengthen the integrity of the world's economy.

Nasdaq Verafin provides cloud-based Financial Crime Management Technology solutions for Fraud Detection, AML/CFT Compliance, High-Risk Customer Management, Sanctions Screening, and Information Sharing. More than 2,600 financial institutions globally, representing nearly $10 trillion in collective assets, use Nasdaq Verafin to prevent fraud and strengthen AML/CFT efforts. Leveraging our unique consortium data approach and targeted typology analytics with artificial intelligence, Nasdaq Verafin significantly reduces false positive alerts and delivers context-rich insights to fight financial crime more efficiently and effectively.

To learn how Nasdaq Verafin can help your institution fight fraud and money laundering, visit www.verafin.com or call 1-877-368-9986.

Nasdaq
Verafin