

5 TRENDS POISED TO SHAPE THE FINANCIAL CRIME COMPLIANCE LANDSCAPE IN 2026

Change is inevitable. Whether sparked by regulations, new technology, politics or economic factors, financial institutions need to adapt to survive.

The rapid pace of emerging threats and complexity of issues – from sanctions and shadow fleets to sophisticated cybercrime – will force institutions to recalibrate their approach to financial crime and compliance in 2026.

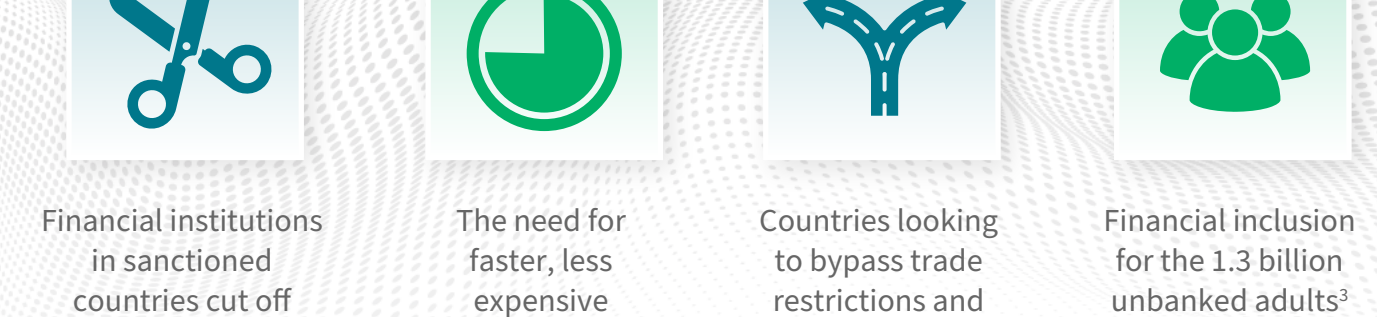
Here are five key trends to watch as the year unfolds.

1 Shifting geopolitics create new vulnerabilities and financial crime risks

Geopolitical events are rapidly driving sanctions and export controls and impacting how countries access financial systems. Sanctioned and non-sanctioned countries alike are reducing their reliance on global payment infrastructure, causing exploitable gaps in an increasingly fragmented financial landscape.

With alternative payment systems on the rise¹ and greater regulatory scrutiny on dual-use goods, vessels, trade-based money laundering and tariff evasion, enhanced monitoring of trade flows is as crucial as “following the money.” Agility to adapt will be key for 2026.

Sanctioned vessel profiles have exploded²



Factors driving the rise in alternative payment systems

- Financial institutions in sanctioned countries cut off from Swift
- The need for faster, less expensive payment options
- Countries looking to bypass trade restrictions and tariffs
- Financial inclusion for the 1.3 billion unbanked adults³

2 Cyberthreats continue to reshape risk

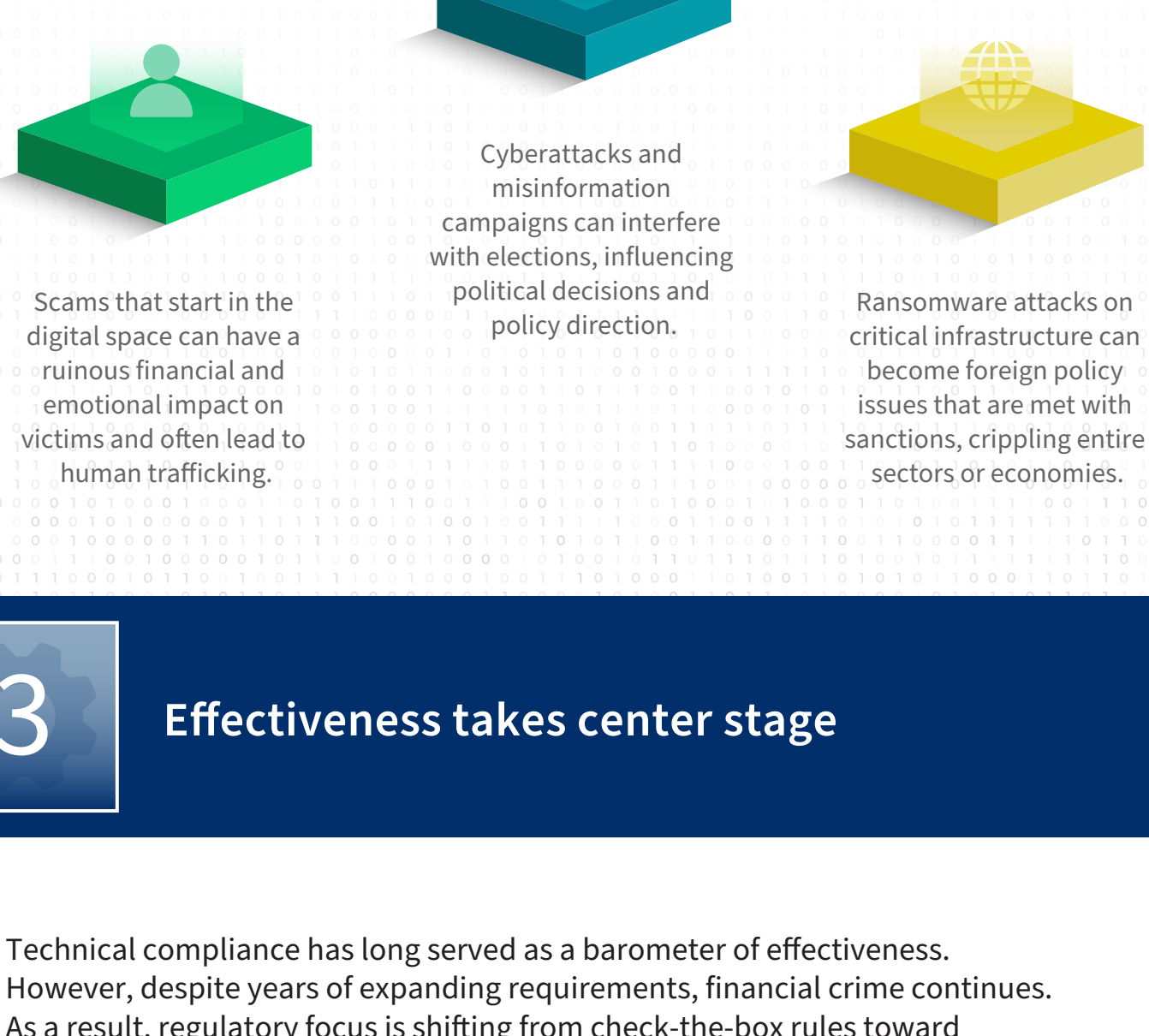
Malign cyber activities erode digital trust. They skew politics, disrupt critical services, open the door for security breaches and serve as a breeding ground for scams, fraud, ransomware attacks, money laundering and other financial crimes.

In response, regulators are increasingly coordinating cyber-related sanctions programs: OFAC, the EU and the UK have all issued designations under cyber frameworks, targeting state-linked actors and large-scale fraud schemes.

Cost of cybercrime worldwide



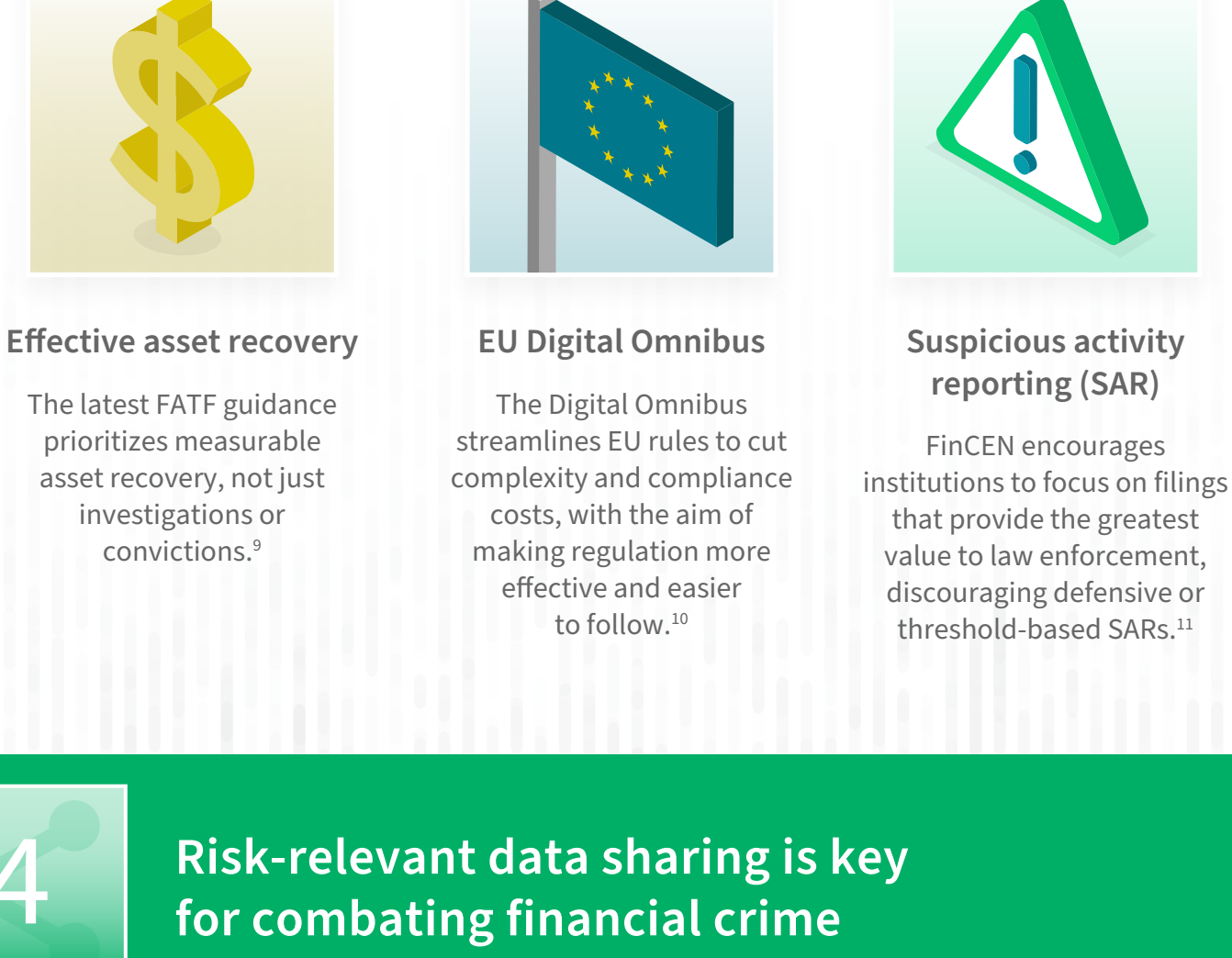
The fallout from malicious cyber activities



3 Effectiveness takes center stage

Technical compliance has long served as a barometer of effectiveness. However, despite years of expanding requirements, financial crime continues. As a result, regulatory focus is shifting from check-the-box rules toward achieving meaningful outcomes.

Outcome-based regulations reduce the cost and complexity of compliance by prioritizing effectiveness over prescriptive requirements. This strategic shift enables financial institutions to allocate resources more effectively, explore new opportunities, invest in emerging technology and boost financial inclusion, while continuing to recognize the benefits of efficiency.



4 Risk-relevant data sharing is key for combating financial crime

Sharing information – whether through public/private arrangements or consortia – is essential for fighting increasingly sophisticated financial crime. But disparate privacy and data protection regulations, anti-competition rules and liability concerns can hinder collaboration. That opens the door for criminals who increasingly weaponize privacy laws to obscure beneficial ownership and challenge disclosure requirements, fueling money laundering and other financial crimes.

Evolving regulations are moving the industry toward mutualization of risk-relevant data, a trend that is likely to pick up speed as 2026 unfolds.

Data sharing developments



5 AI powers both crime and compliance

Artificial intelligence (AI) is a double-edged sword. Malicious actors are weaponizing generative AI for scams, deep fakes, identity fraud and money laundering. Institutions are fighting back by incorporating AI-based tools into compliance workflows to enhance detection.

The challenge for the industry in 2026 will be to strike the right balance – leveraging AI's financial crime fighting potential through strong data quality and governance frameworks without imposing excessive controls that stifle innovation. All while ensuring transparency and explainability.



The value of AI in financial crime compliance

- ✓ Streamlined workflow automation for operational efficiency
- ✓ Enhanced data capture and synthesis for improved KYC and due diligence
- ✓ Stronger sanctions screening with more accurate matching models
- ✓ Sophisticated analytics and automated alert remediation to reduce false positives
- ✓ Behavioral analysis and anomaly detection to capture more true risk

Discover how global risk intelligence and advanced technology from LexisNexis® Risk Solutions can help your organization adapt to change, boost compliance and toughen your fight against financial crime. Visit risk.lexisnexis.com/fcc for more information.