

Fusion centers: Uniting forces against financial crime

Technological advancements within the Middle East financial services industry have given rise to a rapid transformation of the fraud landscape, rendering traditional prevention and detection methods increasingly inadequate. Fraud schemes, originally opportunistic in exploiting the vulnerabilities of individuals, have evolved into more intricate, complex, and syndicated enterprises, now targeting both individuals and organizations. Most financial institutions rely on a myriad of independent teams, operating primarily in their fields of expertise and relying on fragmented data sets from siloed systems to protect themselves and their customers from financial crime, fraud, cyber, and insider threats.

Fraud techniques are becoming increasingly sophisticated, making them harder to detect and mitigate using traditional methods. Inconsistent processes for identifying the technique, incident response, and recovery contribute to delays in addressing fraud risk effectively, leaving organizations vulnerable for longer periods to fraud and financial crime threats. Addressing these challenges requires a shift towards more integrated, proactive, and automated approaches for fraud prevention, more collaboration across departments, and investment in technology to enhance detection and response capabilities.

Globally, several leading financial institutions have begun to adapt to these challenges, implementing an emerging solution referred to as a "fusion center." This article explores the prevailing fraud typologies in the financial industry due to technology transformation. It examines the "fusion" model, discusses the advantages of fusion centers, explores their global adoption, regulatory drivers, relevance in the Middle East market, and offers suggestions for practical implementation.

Fraud techniques are becoming increasingly sophisticated, making them harder to detect and mitigate using traditional methods. Inconsistent processes for identifying the technique, incident response, and recovery contribute to delays in addressing fraud risk effectively, leaving organizations vulnerable for longer periods to fraud and financial crime threats.

The fusion model

The fusion center serves as a centralized hub of experts who might normally operate in silos, collaborating in real-time to analyze and respond to both traditional and technology-driven threats by developing actionable intelligence. The fusion center draws on the specialized skills of fraud, cyber, and financial crime teams, facilitating cross-functional cooperation to develop comprehensive action plans and incident management strategies. Comprehensive data is crucial, as fusion centers rely on having access to integrated data flows from across the institution's operations and technology stacks. When armed with enablers such as dashboards, interactive visualizations, and automated workflows, fusion centers can empower teams to swiftly detect, investigate, and respond to potential fraud and financial crime risks posed by evolving threat actors. ➤

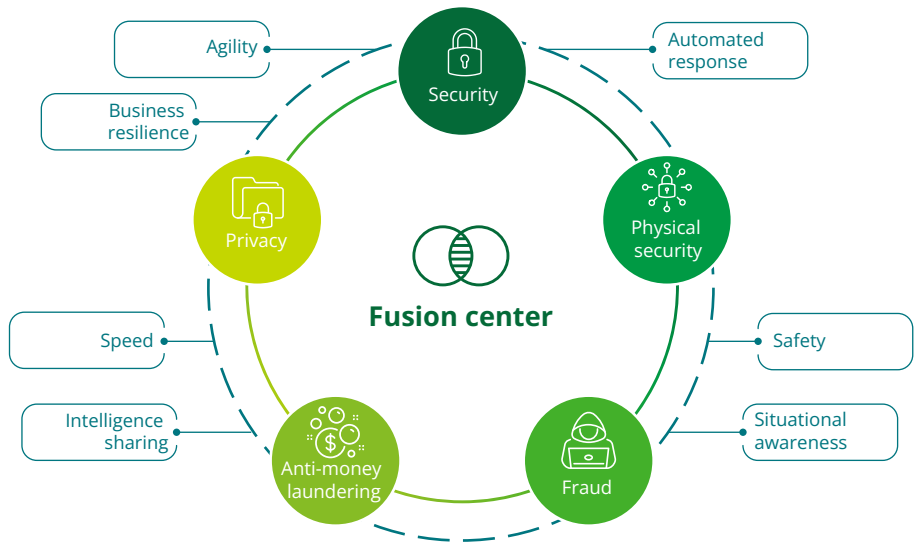








Figure 1: Transforming data into actionable intelligence

The fusion center draws on the specialized skills of fraud, cyber, and financial crime teams, facilitating cross-functional cooperation to develop comprehensive action plans and incident management strategies

Emerging fraud typologies in the financial industry

Digital transformation can significantly enhance customer experience and efficiency. However, it also introduces new fraud risks and vulnerabilities that, if not properly addressed, could erode customer confidence in financial services and products. Below is a selection of emerging fraud trends afflicting the global financial industry, illustrating the crossover between fraud, financial crime, and cyber threats.

Emerging fraud trends		
	Phishing and social engineering	Perpetrators mislead employees or customers into disclosing sensitive and confidential information through sophisticated and deceitful emails, evading traditional email security measures.
	Synthetic identity fraud	Criminals generate fake identities by combining both real and fabricated information, creating accounts, and committing fraudulent activities, which challenge traditional verification methods.
	Account takeover attacks	Perpetrators obtain unauthorized access to accounts using stolen credentials to carry out fraudulent transactions and steal funds, hindering detection by traditional security systems.
	Mule accounts	Perpetrators establish or seize legitimate accounts to facilitate the laundering of stolen funds and fraudulent transactions, obstructing traditional detection systems from tracing the money trail.
	Business email compromise	Cybercriminals exploit email communications by intercepting or mimicking actual email accounts to execute fraudulent transactions, often exploiting legitimate business operations.
	Insider threat	A key risk for financial institutions is posed by staff who have administrative levels of access to sensitive client data and who intentionally or unintentionally cause reputational and financial harm to the organization and its customers.

Benefits of fusion centers

Overall, the fusion concept enables a more coordinated and cohesive response to cybersecurity, financial crime, and fraud, enhancing the resilience and security of financial institutions. By adopting a fusion approach, organizations can address multi-layered threats that span across different domains. An integrated approach allows for shared visibility and costs among the different stakeholder teams (such as the Financial Crime, Fraud Risk Management, and CISO teams), promoting collaboration and efficiency. The fusion concept can enable faster and more efficient information sharing across these groups, leading to a better

understanding of threats when they arise and facilitating the development of more proactive defense measures. With cross-functional collaboration and the application of advanced analytics to integrated data sets, the fusion center can help institutions detect and mitigate a range of illicit activities more rapidly. By synthesizing data sources and strengthening information sharing, these centers allow institutions to remain vigilant against evolving fraud and financial crime tactics, enhancing their security in the digital age.

Global adoption of fusion centers in the financial industry

The key drivers behind leading financial sectors' push to adopt fusion centers:







- Rapid adoption of digital platforms by the financial industry to address customer needs during the pandemic;
- Risks associated with digital platforms and technological advancements such as artificial intelligence, machine learning, ransomware, phishing attacks, deepfake technology, etc.;
- Concerns of risks "falling through the cracks" if different stakeholders within financial institutions do not collaborate or share intelligence;
- Emerging trends of organized crime targeting specific attacks; and
- Regulatory requirements related to data privacy, penalties, and data security.

Relevance in the Middle East market

With the proliferation of digital banking services, transformation to open banking platforms, and the growing sophistication of cyber-attacks, the case for adopting fusion centers becomes clear in the Middle East. These developments come with challenges that necessitate a proactive and collaborative approach from all stakeholders within a financial institution. Although digital banking is rapidly growing

in the Middle East, the industry is still evolving. Therefore, customer awareness and education are crucial in ensuring the secure and effective use of these services. Many banks in the region are investing heavily to make these platforms safe and secure, gaining customer confidence through proactive monitoring activities. Meanwhile, regulators have begun to take a much more determined stance on topics like financial crime and fraud risk

management. For example, the Central Bank of the Kingdom of Saudi Arabia (SAMA) has issued a Counter Fraud Framework regulation as part of their Vision 2030, addressing many of these interrelated topics and acknowledging the need for more collaborative approaches to combating fraud. The UAE Central Bank is also actively working with financial institutions to make digital platforms safe and secure through technology innovation.

Steps	Description
 1. Establishing a centralized hub	Financial institutions should designate a central location or platform to serve as the fusion center. This hub should facilitate effective communication and collaboration among teams responsible for fraud, financial crimes, and security.
 2. Consolidating data	Fusion centers require an integrated data flow from across the institution's relevant operations. This allows data/alerts relevant to a particular customer or risk theme to be compiled and analyzed across the different businesses rather than individually within each silo.
 3. Integration of advanced analytics	Fusion centers should leverage advanced analytics tools to enable real-time threat detection and analysis. These tools can help identify patterns, anomalies, and potential threats across multiple data sources.
 4. Developing incident response protocols	Institutions should develop incident response protocols aligned with industry best practices and regulatory requirements. These protocols should outline procedures for identifying, triaging, and responding to threats effectively.
 5. Developing interaction models	Fusion centers should have strong interaction protocol covering stakeholders from fraud, cyber, and financial crimes. These protocols should outline accountabilities with levels of engagement, communication, identification, remediation, and control feedback.
 6. Continuous training and development	Fusion centers should prioritize ongoing training and skill development for staff members involved in threat management. This ensures that teams remain up to date on the latest threats, technologies, and best practices.

Fusion centers offer financial institutions a compelling, proactive approach to managing fraud and financial crime risk. This approach helps overcome internal barriers to information sharing between an institution's risk management teams. By fostering collaboration, integrating advanced analytics, and providing a platform for continuous training, these centers enhance an institution's ability to detect, respond to, and recover from evolving threats.

In the Middle East, embracing the fusion center model can help financial institutions strengthen their defenses, protect customer trust, and maintain financial stability as the region's financial services sector becomes increasingly digital and globally interconnected.

By **Collin Keeney**, Partner and **Farhana Aliya**, Manager, Forensic, Financial Advisory, Deloitte Middle East