



In today's global, interconnected environment, economic crime risk remains a pervasive challenge. Governments around the world are signaling their rising expectations that compliance programs become more sophisticated. The way financial institutions defend themselves against risks like fraud, money laundering, terrorist financing and cyberattacks has changed significantly as a result of the use of artificial intelligence (AI), particularly through advanced connected analytics. This article summarizes how AI is boosting banking security (and at the same time cost efficiency), showcasing a concrete use case and analyzing the industry's ramifications.

## THE IMPERATIVE FOR AI IN BANKING SECURITY

The financial sector remains a prime target for criminal activities, as banks face increasingly sophisticated threats that are exacerbated by the continuously growing and evolving commercial landscape. For example, the proliferation of new payment rails and demand for faster payments mean that banks have smaller windows of opportunity to detect unusual transactions. Meanwhile, when in the wrong hands, large language models and AI applications can be powerful enablers of fraud, for example helping fraudsters bypass traditional authentication mechanisms. Traditional control measures, while still essential, often fall short in countering the dynamic nature of modern economic crimes. This reality necessitates a more proactive and intelligent approach to threat detection and prevention, making greater use of data that banks hold in relation to counterparties, devices, behaviors, transactions and networks. AI, in particular advanced connected analytics, provides a powerful solution by enabling banks to connect and analyze vast amounts of data from multiple sources in real-time. This capability allows institutions to detect anomalies, identify potential threats, and respond swiftly to inherent risks. Advanced connected analytics enable banks to transform raw data into actionable insights on customers and connected parties, payments and transfers, products and technology – all of this to protect assets and maintain customer trust.

## ADVANCED CONNECTED ANALYTICS: A NEW ERA OF SECURITY

Connected analytics involves integrating disparate data sources to provide a much better view of potential threats. In a banking context, this means synthesizing information from static data, transactional data, customer interactions, social media, and external threat intelligence sources. AI algorithms, such as machine learning, entity resolution and network analytics, play a crucial role in analyzing and interpreting this data. These advanced connected analytics models can identify more complex and sophisticated patterns indicating potentially fraudulent behavior, beyond the traditional indicators such as unusual transaction volumes or deviations from typical spending habits. Moreover, AI systems can continuously learn and adapt from new data, improving their predictive power over time. This capability of dynamic learning is crucial for countering the constantly evolving strategies used by criminals in a cost-efficient manner.

## REAL-LIFE EXAMPLE: AI-POWERED MONEY MULE DETECTION

To fight against sophisticated financial crime schemes, a leading global bank has invested significantly in AI to detect unusual patterns and behaviors. Using machine learning, the bank incorporated multiple features into models, each representing a different behavior. It used these to determine patterns associated with mule accounts which is usually very hard to detect based on a single data source. For example, a large single payment in the context of the overall account balance is not sufficient to pinpoint mule accounts. But combining different indicators such as recent change of address, adding new phone numbers for authentication, transactions to several new beneficiaries, spike in funds received, etc., and based on more nuanced analysis the bank was able to more accurately identify truly suspicious activities and raise risk flags. The bank also discovered that an approach based on continuous evolution worked best, and it was able to feed data back into models to make more accurate predictions over time. Using these models based on advanced connected analytics, the bank was able to detect 3x more mule accounts than before.



**Figure 1: Using advanced connected analytics to identify mule accounts**

## IMPLICATIONS AND FUTURE DIRECTIONS

There are various implications for the banking sector from the incorporation of AI in security. First of all, it emphasizes how important it is for banks to make investments in cutting-edge technology and data infrastructure. The caliber and variety of data that AI systems may access determines how effective they are. Therefore, in order to effectively utilize AI's potential, banks need to give data integration and management top priority. Second, implementing AI in banking security calls for a change in corporate culture and expertise. Financial institutions need to have a staff that is proficient in AI and data science and can create and oversee complex analytical models. In order to solve security issues, banks must also promote an innovative and cooperative culture that encourages interdisciplinary teams to collaborate.

Looking ahead, the future of AI in banking security is a given. Technological developments like deep learning and natural language processing have the potential to improve threat detection even more. Through the analysis of unstructured data, including emails and social media posts, these technologies have the ability to give banks a better understanding of possible risks. Furthermore, AI in banking security has both potential and challenges as a result of the

development of quantum computing. Although quantum computing has the ability to crack existing encryption techniques, it also presents the opportunity to create more effective AI algorithms that can process large, complicated data sets with previously unheard-of speed and accuracy.

## IN ESSENCE

AI-driven connected analytics is a powerful tool in the arsenal of modern banks trying to protect themselves from illicit behavior. By using AI, financial institutions may better identify and prevent threats, safeguarding their resources and maintaining the trust of their customers. The incorporation of AI into banking security will undoubtedly usher in a new era of intelligent protection in the financial services industry, which will become even more important as the financial environment evolves.

## SOURCES

**HSBC Holdings plc “Annual Report and Accounts 2023.” HSBC, 2023** , pages 45-47

**Financial Stability Board. “Artificial Intelligence and Machine Learning in Financial Services: Progress Report.” FSB, 2022**, pages 10-15

**European Banking Authority. “Report on the use of big data and advanced analytics in the banking sector”. EBA, 2023**, pages 22-30

**PwC. Global survey on white-collar crime and fraud, 2024**

<https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html>

**Deloitte. “AI and banking: Moving with the times”. Deloitte Insights, 2023**, pages 5-9

**Accenture. “The New Age of Banking: Using AI for Competitive Advantage”. Accenture, 2023**, pages 14-19

---

## AUTHORS



### **Dominik Käfer**

Partner/ Geschäftsführer,  
European Head of Risk and  
Regulatory  
*strategy&*



### **Dr. Lue Wu**

Director, Risk and  
Regulatory  
*strategy&*