

WHITE PAPER

How Banks Can Get Ahead on Fraud Risk Management

August 2023

By Hanjo Seibert (BCG), Dr. Lue Wu (BCG), Dr. Bernhard Gehra (BCG), Ross Aubrey (Quantexa)

Management of fraud risk goes hand in glove with the business of banking¹. Indeed, as creators of money and trusted intermediaries, banks are inherently exposed to deceits that harm both the business and its customers. To combat fraud, banks have invested heavily in tools and resources. However, these efforts have been only partially successful. In fact, fraud losses are rising—in the US, for example, losses from internet scams rose from \$2.7 billion in 2018 to \$10.3 billion in 2022²—while in the UK, financial fraud has been characterized as a threat to national security³.

Traditionally, most banks have viewed fraud as a pure economic risk, defined by the twin parameters of risk appetite and controls. These, in turn, are closely aligned with cost/benefit considerations. However, attitudes are changing. Regulators in the UK, Sweden, and Australia, among others, increasingly view fraud as a consumer protection matter, holding banks liable for frauds committed against customers as well as other institutions. The UK regulator, for example, now holds both sending and receiving banks liable, with both required to reimburse victims.

Fraud challenges are exacerbated by the changing 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 voice authentication controls.

In the face of these dynamics, banks need to take actions now to prevent financial losses and protect their customers. But how should banks best respond? The answer lies in the data they hold in relation to customers, devices, behaviors, transactions and networks. This is the raw material for more effective fraud risk management, feeding powerful analytical models that can prevent, detect, or investigate potential issues. The good news for banks is that regulatory support for data-driven initiatives is more robust than for anti-money laundering activities. The task for leaders is to take advantage of this support and build the operating models and controls that will be effective as the threat landscape evolves.

Current Approaches are Insufficient

Fraud comes in many guises, which are constantly evolving. To try to keep track, most banks have defined fraud taxonomies, comprising concrete fraud scenarios that act as foundations for fraud risk management. These preparations are tailored to individual business models, channel strategies, and footprints, but most cover a basic inventory of risks that includes:

- Card fraud, including transactions using lost / stolen cards, or card not present
- Payment fraud, including account takeover, impersonation, and authorized push payments (scam)
- Application fraud, including loan application using a fake identity and/or forged documentation.

There is a recent trend away from classical fraud schemes (e.g., card fraud) to more sophisticated frauds such as authorized push payments. In the latter, the payment is initiated by legitimate users / customers, simplifying the task of circumventing controls and making fraud harder to detect and prevent.

In their organizational management of fraud risk, most banks still follow a legacy approach based on siloes. This means separate platforms, tools, and models to assess and detect different fraud types. Banks also have distinct operations teams for different fraud types to perform fraud investigations, often with limited information exchange across the bank.

In the modern context, the siloed approach is insufficient, and fails to cover different attack vectors across products and channels. The reality is that focusing on a single fraud risk type and only leveraging a limited set of data often cannot generate sufficient intelligence to determine if a certain transaction is fraudulent or not.

1. The focus of this paper is on external fraud rather than fraud committed by employees.

2. Source: FBI – Internet Crime Report 2022

3. Source: UK Finance

Breaking Silos and Joining the Dots

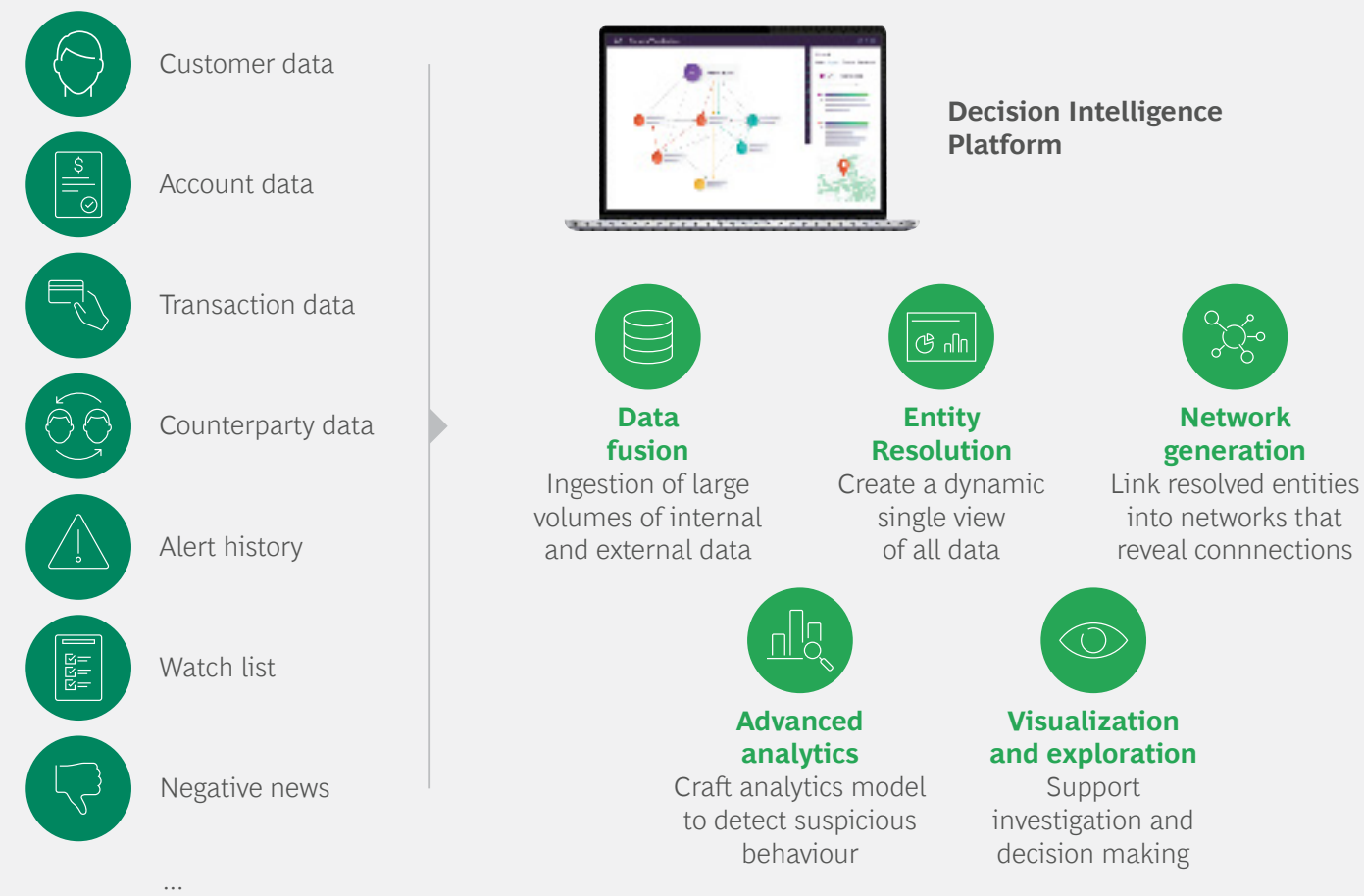
To take fraud risk management to the next level, a subset of banks has adopted a zero-based approach. This means redesigning risk management to apply a unified lens across fraud types, channels, and products, while leaning into advanced data and analytics. The redesign is focused on four key elements:

- **Data foundation:** Banks build a data model around the nucleus “client”, integrating all relevant data, both static and behavioral, to produce deeper insights.
- **AI:** The relationship between human and machine will become increasingly important and, due to the scale and complexity of data, the insight and context needed to drive the right decisions would be impossible without AI. Using AI without context means high false positives, intensive resource costs and material control gaps. Leading banks are creating a single view of internal and external data to drill down into the relationships between entities, behaviors, control, and ownerships. Some are leveraging a decision intelligence platform, enabling a 360° view, improving detection rates, reducing costs, and boosting productivity.
- **Technology:** No single tool can cover every fraud type across channels and products. Leading banks are building state-of-the-art anti-fraud systems that are based on open architectures and form part of ecosystems. This integration and interoperability bring together output and signals to be able to react on constantly evolving fraud schemes.
- **People:** To drive innovation, more data scientists and tech specialists must be recruited to fraud risk functions. A good approach is based on agile principles, bringing together multidisciplinary teams from operations and risk management, alongside advanced analytics expertise to perform complex investigations.

Case example: Leading global bank used Decision Intelligence to detect mule accounts

With the cost of financial crime compliance rising fast, a global bank turned to contextual **decision intelligence** to detect unusual patterns and behaviors. Using machine learning (ML), the bank incorporated multiple features into models, each representing a different behavior. It used these to determine patterns associated with mule accounts– for example, a large single payment in the context of the overall account balance. With this more nuanced analysis it was able to more accurately identify outliers and raise risk flags. The bank 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. One learning was that a balance needs to be struck between using very complex models that are difficult to explain to enforcement agencies and the higher number of false positives associated with simpler models.

Figure 1: Illustration of the Decision Intelligence approach



Some banks have gone a step further and put in systems to jointly manage fraud, AML and cyber risk (the so-called FUSION approach). In practice, these three risk types are often interconnected, with the same criminal organizations focusing on cyber-attack / data theft to establish mule accounts and use them to misappropriate funds and launder money. Some banks have established FUSION centers to holistically address these threats, bringing together the data platform, analytics capabilities, and case management.

Getting Started

As fraud proliferates around the world, leading banks have put innovation in fraud risk management at the top of their agendas. For those still in the starting blocks, a new approach is required, ideally based on integrated controls across fraud types, products, and channels.

To create a holistic lens, the first step should be to build out a fraud risk taxonomy and set an ambition level for the integrated approach. Based on this target state, banks can then define the capabilities required, leveraging the four key pillars of data, analytics, technology and people. These will support construction of a modeling workbench and adoption of agile principles focused continuous integration and continuous deployment (CI/CD). Banks will need to carefully consider whether to build internal solutions or partner with vendors.

Once the basic elements are put in place, banks can build a backlog of use cases. Roll out should be predicated on cost-benefit considerations, so that use cases with the highest impact are scaled first. Once these are in place, the priority should be to continue to develop and innovate, as well as track the fraud landscape, ensuring that defenses are sufficiently strong and flexible to stay one step ahead of attackers.

A large white quotation mark icon, positioned to the left of a text box, indicating a quote.A photograph of a group of people in a meeting room, silhouetted against a large window with a grid pattern. The people are standing and appear to be in a discussion. The window looks out onto a city skyline.

To take fraud risk management to the next level, banks need to apply a unified lens across fraud types, channels, and products, while leaning into advanced data and analytics.



bcg.com
quantexa.com

BCG + quantexa