DR. SEBASTIAN HETZLER

Staying ahead of crime: Real-Time AML as the next frontier

In their attempt to combat financial crime more effectively and avoid financial harm, fines and reputational damages, financial institutions are looking for a more proactive approach to uncover illicit behavior. With good reason, as the global financial system has accelerated tremendously over the past decade. And so has financial crime. Here is what you need to know to make real-time AML effective for your institution.

The Accelerating Pace of the Global Financial System

"Once upon a time," you might tell your children, domestic payments took several days to be fully executed and cross-border payments almost two weeks. Actually, it wasn't that long ago, yet today we're so accustomed to sending and receiving payments in real- or near to real-time that the old delays already feel like a distant memory.

This significant acceleration of the global financial system over the past decade has been fueled by consumers and businesses alike moving to new digital channels, platforms, or cryptocurrencies. They are embracing real-time and instant payments not just for the speed of execution, but also for the lower transaction costs enabled by digital platforms.

According to Grand View Research, a market research firm, real-time payments are projected to grow globally by 30% year over year through 2030.

The speed and intensity of this shift have compelled central banks in many countries to act in order to protect the strategic autonomy and interests of their financial systems, and to avoid heavy reliance on foreign financial institutions and infrastructures. That's why, as of May 2024, 84 countries, including all major economies, have implemented fast or real-time payment networks according to a recent study.

The European Union (EU) has gone furthest in this endeavor, making instant payment mandatory for all payment providers across the bloc. Effective January 2025, the new regulation is causing obligation for all payment providers to transfer money within ten seconds at any time of the day, including outside business hours, not only within the same country but also to another EU member state.

However, the accelerated speed of the financial system not only brings benefits. Particularly when it comes to financial institutions meeting their obligation to comply with international and local anti-financial crime regulations.

Compliance's New Challenge: Moving at High Speeds

While financial institutions are encouraged to prevent fraud by actively intervening during or before the fraudulent activity occurs, regulators take a different approach when it comes to money laundering. In this case, the banks are not mandated to stop money laundering from happening but are required to report suspicious activities that have taken place in their accounts to the Financial Investigation Units (FIU). The reason for this is that FIUs aim to identify the backers of the large criminal networks rather than punish the low-level money mules who often unknowingly provide their accounts for money laundering purposes.

However, this paradigm has begun to rock on the grounds of digitization and the acceleration of payments for three reasons:

Firstly, it's not just consumers and businesses who benefit from this new era of fast money flows, but fraudsters, criminals, and money launderers are also exploiting these capabilities for their own purposes. Historically, the "dark side" has been quick to adopt new technologies, identify loopholes, and exploit them for criminal gain. It's unlikely that this time will be any different.

The digital financial world hasn't just made financial crime faster and more efficient. In fact, it has unleashed a new category of financial crimes that can be executed at industrial scale, with unprecedented speed and high precision. Artificial Intelligence will accelerate this process and supercharge criminals' abilities to come up with ever more complex criminal patterns and in high-speed.

Secondly, many financial institutions are seeking a more proactive approach to combating financial crime to protect their reputation and brand. This is especially true in a world where consumers and businesses alike place great importance on "good corporate citizenship" and ESG (Environmental, Social, and Governance) responsibility when choosing their financial partners.

The view that anti-financial crime compliance is not just a "tick-the-box" exercise, but a key success factor in the market is gradually gaining traction in the financial industry.

Lastly, but most importantly, the global system is widely perceived as ineffective in fighting financial crime and money laundering. Only 4% of all Suspicious Activity Reports (SAR) filed with FIUs lead to investigations, and a mere 2% of all illicit proceeds are confiscated by law enforcement, according to Europol's "European Financial and Economic Crime Threat Assessment 2023. This is why many experts question whether detecting and stopping all illicit activities, including money laundering, in real-time would make the world safer and better.

Contrary to widespread belief in the financial industry, the real-time revolution in AML is already underway.

A New Real-time Paradigm

The European Banking Authority (EBA) took the first steps towards a real-time transaction monitoring approach by publishing guidelines as early as March 2021.

According to the EBA, the extent to which real-time transaction monitoring should be implemented depends on the nature, size, and complexity of a firm's business. As a general guideline, the EBA requires three key elements to be included in an effective system for detecting unusual and suspicious behavior:

As a starting point, firms should use a **risk-based approach** to decide which transactions to monitor in real-time and which to review afterwards (ex-post). As part of this, firms should identify which **high-risk factors** (or combinations thereof) will always trigger real-time monitoring. Firms must ensure that all transactions associated with higher money laundering or terrorist financing risk are monitored in real-time.

In addition to real-time monitoring of identified transactions, firms must regularly conduct **ex-post reviews** on a sample of all processed transactions to identify trends, assess the effectiveness of their monitoring system, and to make necessary improvements.

With this guidance the EBA has added "time" as a new dimension to the risk-based approach. This initiative is consistent, considering the acceleration of the financial system described above. However, given the low adoption rate of real-time AML programs in the financial industry, financial institutions appear to have difficulties implementing EBA's recommendations effectively.

More specifically, many struggle when it comes to the scope of real-time monitoring and its technical implementation. One thing is clear: the deeper you delve into this topic, the more apparent the fundamental shift becomes when transforming an ex-post AML program into a real-time one.

Transformation at Work

In a nutshell, financial institutions must undergo five transformative steps that will fundamentally change how anti-financial crime compliance is conducted:

As a first step, financial institutions must establish event-triggered KYC processes to keep their risk-assessments and monitoring aligned with the real-world risks posed by their clients and their behavior. Secondly, they need to shift transaction sanctions screening from batch processing to real-time screening. Thirdly, they need to implement real-time transaction screening programs to prevent high-risk transactions from being executed.

The fourth step is to leverage Artificial Intelligence (AI) and machine learning to detect known illicit transactions and patterns in real-time. Last but not least, financial institutions have to detect unknown suspicious and changing customer behavior.

But let's start from scratch and explore what is required for an effective real-time AML program.

The Baseline: Real-time Transaction Sanctions Screening

At the core of each real-time AML program is the single transaction. In itself, a transaction doesn't reveal a lot of information about the risk associated with it. A transaction involves a sending account and its owner, a receiving account and its owner, an amount to be transferred, and sometimes a reference.

This information is sufficient to screen a transaction against sanctions lists and perform rule-based checks for potential illegal activity in the reference or free-text fields.

Traditionally, financial institutions have conducted transaction screening in batch overnight, before transactions leave the bank's network for national and international clearing.

With the rise of fast- and instant-payments, sanctions screening must transition to real-time processing.

Additionally, based on a transaction —or better yet a series of transactions— financial institutions can detect illicit behavior in real-time, such as wire-stripping. This refers to the deliberate removal or alteration of information from a blocked wire transfer until it is released and processed by the bank. In an instant or real-time payment environment, this tactic becomes more common, as criminals receive immediate feedback on whether their manipulation was successful.

Beyond the immediate risk of a single transaction, its true nature becomes apparent when risk-related information about the sender and/or receiver, their accounts, and overall behavior is added. This information helps build the risk-context around a transaction.

The Power of Connected Data: Stopping High-risk Transactions

Over the course of a clients' lifecycle, financial institutes collect a vast amount of data. While static information such as nationality or date of birth plays a role, the greatest value for compliance lies in dynamic behavioral data. A customer's past transaction patterns, peer group clustering, transactional networks, and interconnections create the context against which a single transaction can be assessed as expected or suspicious. In other words, to make real-time AML effective, financial institutions must integrate all available data, including customer profiles, account activities, network relationships, behavioral patterns, and peer group comparisons at the exact moment a transaction is processed, in order to provide the necessary context and accurately assess its risk.

A first step towards this holistic view is to enrich each transaction with risk- related data that the financial institution holds about the sender, receiver, and their accounts, and to apply this information in transaction screening rules. Data such as PEP status, confirmed adverse media hits, involvement in hidden economic networks, risk categories or scores, customer profiles and account statuses can be evaluated using complex yet highly targeted rules. Financial institutions must determine which factors, or their combinations of factors, they consider high-risk and therefore warrant real-time intervention.

To illustrate, consider a dormant account that suddenly becomes active again. Most would agree that this is a suspicious behavior requiring the immediate attention of the financial institution holding this account. Moreover, in certain jurisdictions, banks are prohibited from wiring money from dormant accounts.

However, if a single transaction involves a dormant account, the account's status is usually not visible to a transaction screening system. With the kind of data integration recommended here, a transaction from a dormant account can be identified in real-time, flagged, put on hold, and alerted for further investigation and decision.

Or consider the example of a Politically Exposed Person (PEP) receiving a wire transfer from a medium risk country involving a large amount, a case that occurred in Germany and garnered significant media attention in 2024.

There are numerous examples showing how data integration enables financial institutions to detect high-risk transactions in real-time and significantly supports efforts to de-risk their business.

However, the most important step in implementing real-time AML is transforming batch-oriented transaction monitoring and detection with after-the-fact decisions into true real-time operations powered by Artificial Intelligence.

Predicting Money-laundering Patterns with AI

Before we dive into the details of this next layer of complexity, let's first understand the nature of machine learning techniques and how they can be especially useful as part of a real-time AML program.

The traditional approach to decision-making in transaction monitoring involves running overnight batch scoring and making decisions on false- and true positives with hindsight, once all facts are clear and suspicious patterns are fully visible.

Machine learning changes this logic: based on past decisions a model is trained that predicts the likelihood of a specific event given recent input factors.

In other words, machine learning can make predictions based on past assessments made by humans. It is precisely this ability to predict that makes AI a key enabler for real-time transaction monitoring.

The first model required for real-time AML is based on a class of machine learning-techniques called supervised learning. A model is trained on past transactions and their classification as either suspicious or unsuspicious. The score assigned to a specific transaction reflects the likelihood that it is part of a nefarious pattern previously confirmed as a true hit. Transactions with high scores are flagged as high risk. This technique enables the identification and blocking of known suspicious transactions or patterns.

However, this is only one side of the coin and must be complemented by a second technique focused on detecting unknown suspicious behavior.

Detecting Suspicious Behavioral Changes

The second approach belongs to a class called unsupervised learning. It clusters customers based on their actual transactional behavior, grouping clients with similar patterns together. Using these behavioral clusters generated during model training, the current behavior of a client can be compared to both their past behavior and the typical behavior of their peer group. The AI-score, known as Entity Deviation Score, measures how much a recent transaction deviates from these established expectations. The higher the score, the more suspicious the transaction is likely to be. Transactions with high deviation scores should also be blocked by a real-time AML system.

With that we have covered the key elements of an effective real-time transaction screening system and the necessary conditions for real-time AML. But is this already sufficient? What happens if the Entity Deviation Score signals a behavioral change in the client or if a series of high-risk transactions suggests riskier behavior of the client than the financial institution is willing to accept? This shifts the focus to KYC.

Keeping Clients' Risk Assessment Up-to-date with Event-triggered KYC

The accuracy of real-time AML depends heavily on timely, updated, contextual data about the client and their individual risk profile. To achieve this, financial institutions must shift their KYC-review processes from periodic to event-triggered. Instead of conducting at fixed intervals based on a client's risk-class, e.g. every 5, 3 or every year, they should focus on specific triggers that indicate a review is necessary. The benefits of this approach are clear: in addition to significantly reducing the time, effort, and cost of routine KYC-reviews, it ensures a consistently accurate risk-classification across the entire client base.

There are three main sources of event-triggers for a KYC-review: The first category includes static triggers that may initiate a review process for a client such as regulatory requirements to execute reviews, internal requirements for periodic checks or master data changes like a change of address, name, or legal status.

The second category involves dynamic triggers, which may arise from events such as new or updated watchlist hits, changes in company ownership structures (UBO), or a reassignment of the customer to a higher risk category. Finally, some KYC-reviews are initiated by behavioral changes in a customer's activity or account usage. AI can support detecting such shifts, for example, by flagging a high Entity Deviation Score for a specific client.

Real-time AML, as introduced here, is a comprehensive methodological approach that not only enhances the detection of money laundering, but also strengthens the fight against a broader spectrum of financial crimes. In doing so, it addresses a long-discussed but rarely implemented concept in the industry: Financial Crime Convergence.

The Blurring Lines of Financial Crime Categories

In a digital world, the lines between different financial crime disciplines are beginning to blur. Fraud, money laundering, terrorism financing, and other illicit activities increasingly merge into indistinguishable patterns. Often, a single transaction or a series of them, can simultaneously exhibit characteristics of multiple types of financial crime.

The reason lies in the very nature of digital crime compared to its real-world counterpart. In traditional crimes, the criminal act and laundering of its proceeds are two separate stages: first, cash is earned through illegal means like drug trafficking, and only afterwards does the process of placing, layering, and integrating that money into the financial system begin. In the digital world, however, both steps must occur simultaneously. When a criminal drains an account, the obfuscation of the funds must be built into the act itself. Digital criminals design their schemes backwards, starting from the desired end state and engineering every step to get there without detection.

Addressing the multifaceted nature of financial crime simultaneously is one of the most significant advantages of the real-time AML approach.

Key Challenges for Financial Institutions

The real-time approach to transaction monitoring presents two major challenges for compliance—one technical, the other operational.

From a technical perspective, financial institutions must have the infrastructure and systems in place to connect data silos, enrich transactions with contextual information, and run AI-models within milliseconds. But the reality is far from ideal. Customer data is scattered across siloed systems, making it difficult for financial institutions to fully leverage the insights they already possess about a client.

Beyond integrating data, financial institutions must establish robust and high-performing IT-infrastructures that can scale with increasing workloads while maintaining consistent performance.

Both goals can be achieved with modern, integrated AML software built on scalable architecture.

What is more difficult to manage are the operational challenges: when transactions are processed in real-time, compliance teams must also operate in real-time, meaning 24/7. It's clear that if a real-time detection system halts transactions round the clock, compliance teams must keep pace—reviewing and resolving alerts continuously, and within very short timeframes.

This becomes especially challenging in jurisdictions with strict labor laws that limit or prohibit regular weekend and night shifts. At the same time, data residency and privacy regulations often prevent financial institutions from outsourcing alert and case handling to countries with more flexible labor rules, making 24/7 operations difficult to scale.

And finally, financial institutions will face challenges finding qualified staff in tight labor markets willing to work weekends and night shifts.

One way to ease this operational challenge is to use Artificial Intelligence and automation in the decision-making processes. Based on rich data, machine learning models can be trained to replicate past decisions on alerts, significantly reducing the volume of real-time alerts and leaving only exceptional cases for manual investigation and intervention. In addition, automation of workflows can reduce the time and effort needed for data gathering and investigation.

Another issue is the missing regulatory guidance on how to deal with blocked real-time transactions. What happens if an instant payment cannot be processed within 10 seconds because it requires further investigations due to suspicious activity? This is where clear regulatory guidance becomes essential to provide financial institutions with a legally protected framework in which to operate.

Prepare for the Real-time Financial System

Real-time or fast financial transactions are on the rise and are set to soon dominate the global financial system. The benefits for both consumers and corporates are clear. But they also bring financial crime risks stemming from the speed and complexity of digital transactions. These risks demand new approaches, processes and tools, as outlined here.

Despite the challenges, real-time AML offers many benefits not only for each individual financial institution but also for the effectiveness of the global financial system and its capacity to protect itself against financial crime.

More recently, FATF, the world's financial crime watchdog, has launched its first consultations on real-time AML.

The race is on.

[ABOUT THE AUTHOR]

Dr. Sebastian Hetzler joined IMTF as a Co-CEO in December 2022 with the acquisition of the Siron business from FICO. At FICO, he has been a VP Product Management for FICO's Compliance Solutions. Before the acquisition of TONBELLER AG in 2015 Sebastian has been the managing director of this company. With more than 15 years' experience in the Anti-Financial Crime sector, he is one of the leading domain experts in this space. Previously, Sebastian worked in top-management consulting companies focused on strategy and organization for many years. Sebastian holds a doctorate in System Theory and Cybernetics from the University of St. Gallen, Switzerland.

[IMTF]

IMTF group (HQ)
Route du Bleuet 1
1762 Givisiez / Switzerland
Phone +41 26 460 66 66

IMTF Siron GmbH
Stubenwald-Allee 19
64625 Bensheim / Germany
Phone +49 6251 826 27 90

IMTF Dubai
Reef Tower, Unit R30-20 / 30-21
Jumeirah Lake Towers
Dubai 5003308 / UAE
Phone +971 4 448 7570

IMTF Luxembourg
12, rue du Château d'eau
3364 Leudelange / Luxembourg

IMTF Banking Software Pte. Ltd.
Level 6 Republic Plaza
19 Raffles Place
Singapore 048619
Phone +65 6735 61 50

Informatique MTF Services GmbH
Mariahilfer Strasse 123/3
1060 Vienna /Austria

IMTF Software Pte. Ltd.
No. 6, Ground Floor, IndiQube Plaza
Wind Tunnel Road, Kaveri Nagar,
Murgesh Pallya,
Bengaluru - 560017
Karnataka / India

info@imtf.com
www.imtf.com

[OUR MISSION]

Helping fight financial crime and make the world a safer place.