With Precautions, AI Can Help With Suspicious Activity Filings

By **Laurel Loomis Rimon, Gina Shabana and Ben Seelig** (November 26, 2024)

Laurel Loomis Rimon

Gina Shabana

Ben Seelig

As artificial intelligence takes the world by storm, potential use cases proliferate by the day. Compliance professionals are looking closely at the tasks that AI technology may be able to perform, supplement and improve in their compliance processes.

In this article, we examine the considerations around the use of AI in one important area in the regulatory and enforcement environment affecting financial services businesses — suspicious activity reports, or SARs.

The filing of SARs, and failures related to the filing of SARs, factor in many criminal and regulatory anti-money laundering, or AML, enforcement actions.

In September, the Office of the Comptroller of the Currency took an AML-related enforcement action against Wells Fargo Bank NA for SAR filing failures, among other things.[1] Similarly, TD bank was also fined approximately $3 billion in October in multiple parallel actions by regulators for, among other things, willful failures to file SARs on $1.5 billion in transactions.

We review the legal requirements and expectations applicable to SAR filings, areas of deficiencies that can lead to an enforcement action, and how AI may help — or not.

SAR Filing Obligations

Financial institutions are statutorily obligated to file SARs within 30 calendar days of detecting facts that would require a filing of a SAR.

Financial institutions subject to these obligations include banks, casinos and card clubs, money services businesses, brokers or dealers in securities, mutual funds, insurance companies, futures commission merchants, and introducing brokers in commodities, among others, per Title 31 of the Code of Federal Regulations, Section 1010.100(t).

Pursuant to Title 31 of the Code of Federal Regulations, Chapter X, Subpart C et seq., a financial institution is required to report transactions conducted, or attempted, by, at or through the financial institution that involve or aggregate to at least $5,000 ($2,000 for money services businesses), where the financial institution knows, suspects, or has reason to suspect the transaction or pattern of transactions:

- "Involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity," per Title 31;

- Is conducted in a manner to evade any requirement of Title 31 of the Code of Federal Regulations, Chapter X or the Bank Secrecy Act, e.g., evade reporting of currency transaction reports;

- Lacks a business or apparent lawful purpose or is not within the expected normal course of business of a specific customer with no reasonable explanation; or

- Involves the use of the financial institution to facilitate criminal activity.

Further, financial institutions with SAR reporting obligations may also file a continuing SAR — a follow-up report that covers related activity that postdates the initial filing — instead of separate SARs for each suspicious transaction.

The SAR submission itself must be accurate and complete, incorporating all relevant data points in order for it to serve its purpose, which is to aid law enforcement in the fight against money laundering and the financing of terrorism.

Banks, fintechs and other financial institutions often find it challenging to meet this requirement in light of the volume of data they need to cull and accurately condense into a single report.

Federal and state financial regulators regularly examine financial institutions for SAR quality and completeness, and it is not uncommon for a financial institution to be faulted on this basis in either the supervisory or enforcement context. Issues may include:

- Failure to fully document the who, what, when, where and why in the SAR narrative;
- Failure to include in a SAR all related or connected parties; or
- Failure to timely file SARs due to investigation or decisioning backlogs.

How AI Can Help

For now, at least, the decision about whether to file a SAR in a particular instance remains squarely a task for compliance staff and leadership, as that is certainly a regulatory expectation.

However, as in many other areas, large language models used in generative AI and machine learning software can serve as useful tools to increase the speed, quality and efficiency of SAR filings. For instance:

- AI can ingest and analyze large volumes of data to make recommendations on what data constitutes an anomaly or appears suspicious, and may necessitate the filing of a SAR. This analysis can be based on predetermined elements such as transaction monitoring alerts or connections to other suspicious activity, thus saving time and resources — especially during resource-intensive periods such as when a financial institution is performing a lookback review where it expects to analyze extensive data amounts that will result in a large volume of SAR filings.

- Similarly, AI tools can also help financial institutions in the preparation of comprehensive and cohesive narratives, or at least first drafts, that condense extensive data in a concise manner. Preparation of concise and complete narratives

is often a challenge facing financial institutions and their compliance resources, especially when faced with a backlog of data. AI tools can provide financial institutions a medium to improve the speed and quality of their SAR narratives.

- AI can also serve as a tool to potentially identify connections between multiple players or narratives where parallel or separate reviews may otherwise miss the connection because the reviews are performed independently or siloed.

- Finally, AI tools can analyze new information to correct or update a filing, or to determine whether a continuing SAR should be filed.

What to Consider Before Using AI for SAR Filings

Financial institutions should consider the completeness and accessibility of their data sources to ensure that the right data (e.g, customer due diligence or know-your-customer files) can be properly ingested and analyzed by AI software.

In training, tuning or refining the large language models, companies should also consider how those processes will be documented and communicated to regulators.

AI tools are typically owned by a third party. Therefore, the rules of third-party due diligence apply.

As such, as with any third-party reliance, the financial institution remains liable to meets its obligations, i.e., the financial institution cannot shift the SAR reporting liability on the third party that owns the AI tool.

This means that financial institutions will still need to perform due diligence, testing, and quality control before and during the contracting period. This may take place, among other ways, by reviewing SAR narratives to ensure accuracy, completeness and conciseness.

Further, when performing initial due diligence, financial institutions must ensure that their use of the AI tool does not result in violating the SAR confidentiality provision.

Specifically, SARs and any information that would reveal the existence of a SAR are strictly confidential and may not be shared with other parties except in very limited circumstances, e.g., sharing with a regulator.

When analyzing data for the purposes of SAR filings, large language models and machine learning tools by nature access this data, and a financial institution remains responsible to meet its SAR confidentiality obligations.

AI tools could also raise similar privacy law concerns. In order to perform their functions fully, large language models and machine learning tools inherently ingest a large volume of data, and this data often contains very sensitive material that could trigger privacy obligations.

For example, the data could include personal identifiable information, account statements, and similar information that will be considered personal or sensitive under applicable federal and state laws.

Therefore, a financial institution must ensure that it maintains ownership and control of the

data, including the prompts or other inputs that helped AI tools prepare SAR filings.

Financial institutions must also fully understand:

- Where the data will be housed;
- How it will be protected from unauthorized use or access, including use in further training large language models or machine tools, or for providing services to other customers of the AI tool;
- How the financial institution's data will be segregated from other customers' data or instances of the AI tool; and
- Who has access to the data to ensure that there are no data security gaps that would risk potential SAR confidentiality violations or violations of privacy laws.

With these considerations in mind, AI provides a substantial opportunity to enhance both the substance and efficiency of SAR processes, one of the core regulatory obligations financial institutions must meet on a day-to-day basis.

Laurel Loomis Rimon is a partner and co-chair of the fintech and crypto-assets practice at Jenner & Block LLP. She previously served as head of litigation for the U.S. Department of Justice's Asset Forfeiture and Money Laundering section and as assistant deputy enforcement director for the Office of Enforcement at the Consumer Financial Protection Bureau.

Gina Shabana is practice counsel at the firm. She previously served as associate director of data privacy and protection in the Financial Industry Regulatory Authority's Office of General Counsel.

Ben Seelig is an associate at the firm.

[1] https://www.occ.gov/static/enforcement-actions/eaAA-ENF-2024-72.pdf.