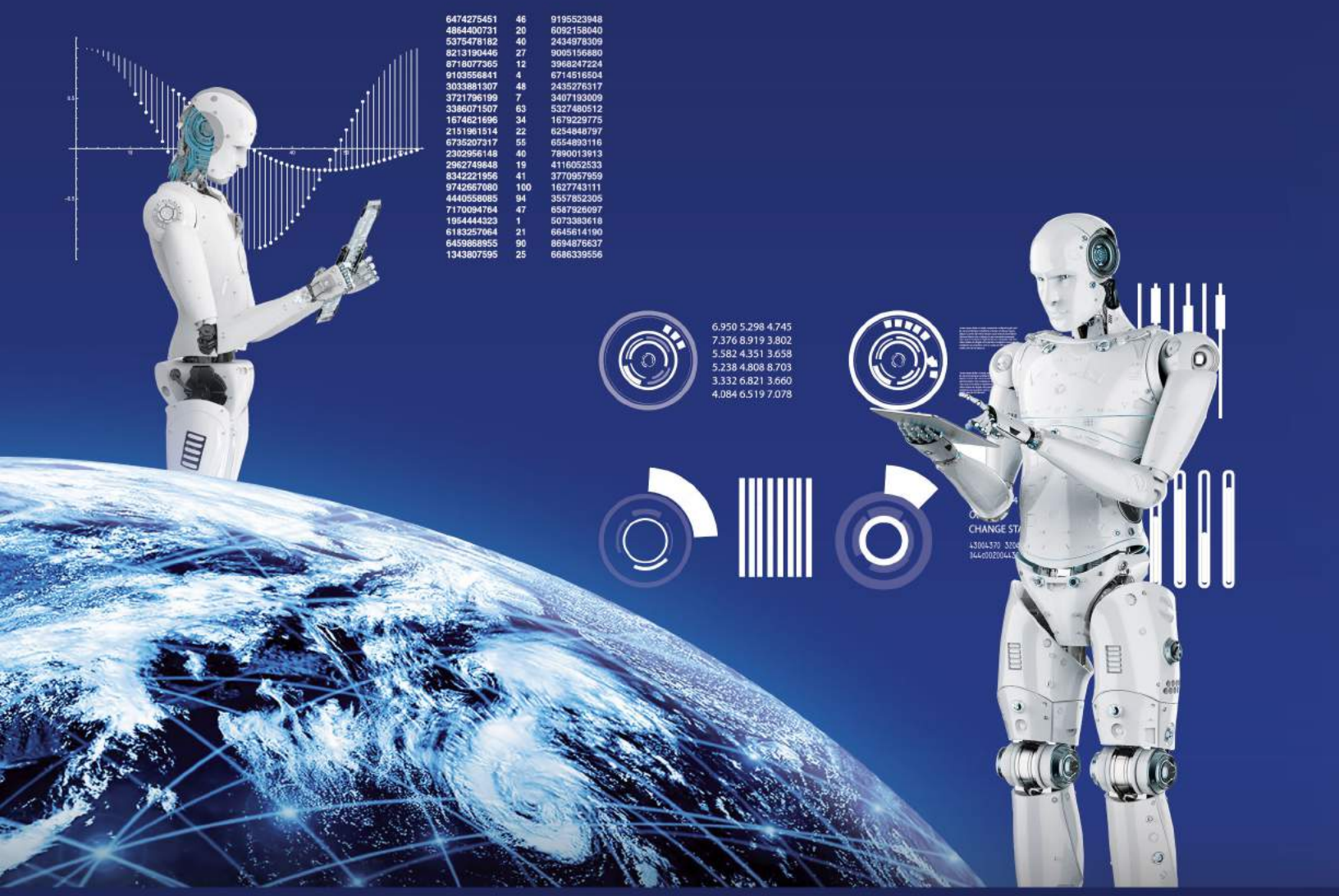
AI OASIS



NO FALSE NEGATIVES

The Minimum Standard for BSA/AML Compliance

On December 3, 2018, FinCEN and Federal Regulators issued a joint statement, recommending financial institutions to use Artificial Intelligence and Machine Learning for AML compliance. Awarded with over ten (10) patents, PATRIOT OFFICER® is empowered by the most advanced Artificial Intelligence and Machine Learning technologies.

In the field of Machine Learning, a negative is a set of data that has not been triggered as an alert. A true negative is a set of data that has not been triggered as an alert, and does not constitute a true case. **A false negative is a set of data that has not been triggered as an alert; however, it comprises a true case that the system has missed.** Similarly, a positive is a set of data that has been triggered as an alert. A true positive is an alert which is a true case. A false positive is an alert which is not a true case.

A false negative money laundering case may cause a financial institution to be penalized by the U.S. government if the false negative case (i.e., a true money laundering case) is discovered by the U.S. government later. **Therefore, the minimum standard for BSA/AML compliance is No False Negatives.**

Three different types of BSA/AML systems are analyzed below:

<u>Behavior-Based Systems</u>

Some vendors are promoting that their "behavior-based" systems produce fewer alerts than rule-based systems. This is a false promotion. Behavior-based systems use "changes of behavior" to trigger alerts. A behavior change may happen in a fraud case committed by a third party (e.g., stolen credit card, counterfeit check, etc.) because the victim and the fraudster are two different persons and it is very likely that they behave differently. **In reality, behavior-based systems have missed many true money laundering cases (i.e., behavior-based systems have a large number of false negatives) because money laundering can be conducted without any behavior change.** For example, a criminal or terrorist can routinely send funds to a remote accomplice without changing behavior. There are many money laundering activities that can be conducted without any behavior changes. **This is why behavior-based systems have failed regulatory examinations.**

The truth is that behavior changes only cover a small number of the branches of the decision tree which can produce rules to detect money laundering activities. Because behavior-based systems only cover a small portion of the money laundering risk, behavior-based systems trigger fewer alerts. At the same time, **because behavior-based systems only cover a small portion of the money laundering risk, behavior-based systems have many false negatives (i.e., they miss many true money laundering cases).**

In addition to missing many true money laundering cases, behavior-based AML systems often falsely detect fraud cases as money laundering cases because behavior changes often occur after the fraudsters have stolen the checks, credit cards, etc. from the victims. This is the reason why vendors of behavior-based systems must claim that their systems can detect money laundering cases and fraud cases together.

The truth is that, because behavior-based systems cannot distinguish between money laundering cases and fraud cases, these systems have no choice but to mix fraud cases together with money laundering cases.

For fraud cases committed by third parties, the persons detected by behavior-based systems are actually victims of fraud, not money launderers. In other words, behavior-based systems falsely detect innocent victims of fraud as money launderers. **The fact is that behavior-based systems not only have many false negatives (i.e., missing many true cases), but also have many false positives (i.e., producing many false alerts) when they are used for AML monitoring purposes.** It is predicted that behavior-based systems may disappear soon in the BSA/AML industry because government regulators and examiners have become more knowledgeable about the differences between money laundering and fraud. Many intelligent BSA/AML experts have already decided that they do not want to have anything to do with behavior-based systems.

When BSA/AML experts examine the detection algorithms of a behavior-based system, they can easily uncover the flaws in the behavior-based system. **To hide the flaws of behavior-based systems, behavior-based systems are usually designed like a black box so that no one can find out how alerts are actually triggered by the systems. As a result, the users of behavior-based systems do not even know the reasons behind each alert, and cannot determine whether the alert is a true money laundering case. This is another reason why behavior-based systems have failed regulatory examinations.**

Furthermore, behavior-based systems do not create a true risk score for each customer on an ongoing basis. Instead, behavior-based systems only create "behavior scores" (i.e., not risk scores) for those customers who have changes of behavior. Therefore, to comply with the BSA/AML Examination Manual, financial institutions that use behavior-based systems need to use spreadsheets to calculate the risk score of each customer in order to identify the higher-risk customers. This is a labor-intensive and time-consuming task that some financial institutions had tried and eventually gave up. **The failure to identify higher-risk customers on an ongoing basis is one more reason why behavior-based systems have failed regulatory examinations.**

Rule-Based Systems

Many financial institutions have used rule-based approaches which can trigger many alerts. For example, there are over two hundred countries in the world. If a financial institution uses a rule-based approach to monitor the wire transfers to, or from, each country, the financial institution may have over two hundred branches at the country decision node of the decision tree. As another example, there are thousands of industries. If a financial institution uses a rule-based approach to monitor the wire transfers to, or from, each industry, the financial institution may have thousands of branches at the industry decision node of the decision tree. Country and industry are two of many risk categories that have money laundering risk. Similarly, wire transfer is one of many types of transactions that have money laundering risk. For example, cash, check, ACH, ATM, credit card, debit card, letter of credit, etc. are other possible types of transactions.

There are many money laundering risk factors. If we use the terminology in Machine Learning to describe this challenge, there are millions of possible combinations of branches to form a path from the root of a decision tree to the leaf nodes of the decision tree. **In other words, millions of rules are required to cover the entire scope of money laundering risk if a rule-based system is used to detect suspicious money laundering activities.** A rule-based system with less than millions of rules may have many false negatives (i.e., the system has missed true

money laundering cases and cannot meet the minimum standard of BSA/AML compliance) and many false positives (i.e., the leaf nodes of the decision tree have very high impurity and cannot truly achieve the goal of classification). This is the reason why a financial institution needs to hire many BSA/AML experts to review a large number of alerts if a rule-based approach is used.

The reality is that all rule-based systems cannot comply with the minimum BSA/AML compliance standard of No False Negatives because financial institutions cannot afford to use a rule-based system that has millions of rules.

Risk-Based Systems

Thanks to the intelligence of the Federal Financial Institutions Examination Council (FFIEC), the BSA/AML Examination Manual was revised in April 2010 to provide an official guideline. In this revised manual, the FFIEC replaced the phrase "high-risk customer" with "higher-risk customer" throughout the manual. On page 57 of the BSA/AML Examination Manual published in February 2015, the title of the section is "Enhanced Due Diligence for Higher-Risk Customers." The manual further states that "…*Higher-risk customers and their transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship with the bank.*"

Financial institutions are required to conduct risk-based monitoring. In 2018, after a financial institution failed to conduct risk-based transaction monitoring, it was fined over $260 million by the U.S. government regulators. In order to fully comply with the BSA/AML Examination Manual, a financial institution must (1) identify the higher-risk customers, (2) conduct EDD on these higher-risk customers, and (3) monitor these higher-risk customers and their transactions more closely as long as their accounts are open.

By conducting Risk Scoring (U.S. Patent) at account opening and on an ongoing basis throughout the term of a customer's relationship with the financial institution, PATRIOT OFFICER can automatically and dynamically calculate a risk score for each customer based on the most comprehensive scope of risk factors, including products, services, customers, entities, transactions, and geographic locations, etc. as required by the BSA/AML Examination Manual.

Once a risk score of a customer is obtained through the Risk Scoring process, a financial institution can easily identify the customer as having a higher risk if the risk score is higher than a threshold determined by the policy of the financial institution, and can conduct EDD on the customer. The effect of a risk score is similar to the effect of a credit score. Thirty years ago, a financial institution might need to spend a week to investigate a person's background before the financial institution issued a car loan to this person. Today, a decision to issue a car loan can be made within a few minutes based on the credit score of the loan applicant.

Similarly, a BSA/AML expert can use the risk scores to quickly identify the higher-risk customers without spending a lot of time to investigate all the potential risk factors associated with each customer. Because PATRIOT OFFICER has included all the money laundering risk factors of a customer into the Risk-Scoring process, PATRIOT OFFICER has equivalently consolidated the effects of countless rules into one risk score, and effectively eliminates the need of using these rules. More importantly, by eliminating these rules, PATRIOT OFFICER has eliminated all the false alerts associated with these rules.

PATRIOT OFFICER is the only BSA/AML solution that covers all money laundering risk factors while all behavior-based systems and rule-based systems in the marketplace can only cover a very small number of money laundering risk factors. In other words, behavior-based systems and rule-based systems not only produce many false positives, they also have many false negatives (i.e., they have missed many true money laundering cases).

Neither behavior-based systems nor rule-based systems can meet the minimum BSA/AML compliance standard of No False Negatives. Furthermore, neither behavior-based systems nor rule-based systems can comply with the risk-based requirements mandated by the BSA/AML Examination Manual. Only the risk-based solution provided by PATRIOT OFFICER fully complies with the BSA/AML Examination Manual published by the FFIEC.

PATRIOT OFFICER uses Machine Learning technology, which is the most advanced technology in the field of Artificial Intelligence, to produce the most comprehensive Risk Model, which eliminates the need to use millions of rules. **PATRIOT OFFICER is the only BSA/AML System that has No False Negatives.**

The Risk Model of PATRIOT OFFICER has been implemented in the field for over ten (10) years and has been proven to be the most powerful solution to BSA/AML compliance. Furthermore, the PATRIOT OFFICER system is designed to be transparent. Many examiners and auditors have already examined the Risk Model of PATRIOT OFFICER. **The Risk Model and detection scenarios are user-configurable, viewable, verifiable, and auditable.**

PATRIOT OFFICER has incorporated over 10 patents to provide users with the most advanced A.I. powered technologies, including **Risk Scoring, Multidimensional Risk-Based Detection, Multidimensional Risk-Directed Detection, Multidimensional Risk-Based Data Mining, and Multidimensional Risk-Based Peer Group Analysis**. These Risk-Based technologies are the next-generation technologies which empower financial institutions to comply with the Risk-Based requirements mandated by the BSA/AML Examination Manual published by the FFIEC. Most importantly, PATRIOT OFFICER has No False Negatives. Because of the patent protection, no other vendor can copy the design of PATRIOT OFFICER.

In addition to PATRIOT OFFICER, AI Oasis has proudly delivered the world's first and only financial crimes alarm system, ENQUIRER OFFICER®, which empowers a financial institution to discover hidden information about its customers, non-customers, and beneficial owners; receive early warnings about potential financial crimes; and block criminals from opening accounts with the financial institution. Moreover, we have delivered the most advanced and comprehensive fraud prevention system, GUARDIAN OFFICER®, which empowers a financial institution to detect all types of fraud in advance and protects the financial institution against losses and damages. Furthermore, we offer the most innovative consumer protection system, CHAMPION OFFICER®, which protects consumers against identity theft and financial crimes.

PATRIOT OFFICER®, GUARDIAN OFFICER®, ENQUIRER OFFICER®, and CHAMPION OFFICER® have jointly established the most powerful United AI Network™ to protect financial institutions against all types of financial crimes, losses, and damages. Contact AI Oasis today to ensure your success in the future.

GLOBAL SHIELD

The World's First and Only Financial Crimes Alarm System

Imagine a future where once a person commits a financial crime, a global alarm goes off, and a spotlight shines and tracks wherever the criminal goes. Imagine that any financial institution which has this criminal as a customer would be immediately notified by the global alarm. Imagine that every financial institution which this criminal tries to approach would immediately see the spotlight and could stay far away from this criminal.

This future has arrived.

Never before has this been possible. Until today, with ENQUIRER OFFICER®, whether perpetrators have committed money laundering, terrorist financing, white-collar crimes (accounting fraud, embezzlement, IT fraud, etc.), Ponzi schemes, bank fraud, security fraud, insurance fraud, tax fraud, or any other schemes, *they can no longer hide.*

How does this happen?

The Anti-Money Laundering laws and regulations in the United States are very advanced and stringent. For example, the regulatory penalties for failing to file a SAR on Bernie Madoff exceeded $2 billion dollars. A financial institution may receive a huge regulatory penalty if the illegal proceeds of a customer are deposited at or transferred through the financial institution without being detected and reported to the U.S. government.

Financial crimes collectively produce hundreds of billions of dollars in illegal proceeds every year. These illegal proceeds are transported through financial institutions since criminals cannot physically move hundreds of billions of dollars. When the illegal proceeds are transferred through a financial institution, they become "money laundering proceeds." The biggest challenge for a financial institution is detecting all illegal proceeds that are deposited at or transferred through the financial institution. *With five (5) technology patents*, ENQUIRER OFFICER empowers financial institutions to effectively detect the illegal proceeds of many types of financial crimes. Because of the patent protection, no vendor can copy ENQUIRER OFFICER.

Why now, and why ENQUIRER OFFICER?

Financial crimes are rampant and increasing globally at an alarming rate. The Gramm-Leach-Bliley Act prohibits financial institutions from disclosing non-public personal information. ENQUIRER OFFICER uses patented technologies to send legitimate alarm signals which do not contain any non-public personal information. Financial institutions can only receive these legitimate alarm signals through ENQUIRER OFFICER – the world's first and only legitimate Financial Crimes Alarm system.

How does it work?

Powered by advanced AI technology, ENQUIRER OFFICER is the most robust system to combat financial crimes. An ENQUIRER OFFICER system receives updates through the Global Communication Protocol which is also used to update regulatory lists (e.g., OFAC, etc.). Therefore, any financial institution which receives OFAC

updates from AI Oasis can also receive ENQUIRER OFFICER updates. Moreover, the ENQUIRER OFFICER updates use a much higher security standard than OFAC updates.

First, all the ENQUIRER OFFICER updates are encrypted messages which, even if successfully decrypted by a malicious third party, do not contain any non-public personal information. Therefore, ENQUIRER OFFICER fully complies with the Gramm-Leach-Bliley Act.

Second, only those financial institutions which are truly exposed to the specific ***money laundering*** or ***terrorist financing*** risk described by the update will receive an alarm signal from ENQUIRER OFFICER. Because of these precise alarm signals, financial institutions can ensure effectiveness and efficiency in their respective Financial Intelligence Units (FIU).

Third, when ENQUIRER OFFICER informs users at different financial institutions that they have a common interest, they can communicate with one another privately and confidentially via email or by phone, while ENQUIRER OFFICER stays out of the communication. Each user can independently determine whether to communicate with the counter party, and make sure that the counter party has valid registration with FinCEN for information sharing under Section 314(b). By using ENQUIRER OFFICER, financial institutions can *discover hidden information and receive early warnings of various types of financial crimes and their associated illegal proceeds in a timely manner.*

Similar to the OFAC list, ENQUIRER OFFICER also produces an ENQUIRER OFFICER list consisting of historical encrypted messages received by ENQUIRER OFFICER. Because ENQUIRER OFFICER automatically scans new customers (or members) and beneficial owners against the ENQUIRER OFFICER list during the account opening process, *any perpetrator who has cheated one financial institution before will not be able to cheat any financial institutions again.*

Who can use it?

Any kind of financial institution (e.g., bank, credit union, insurance company, security firm, stock brokerage firm, private equity firm, investment company, loans company, trust company, money services business, etc.) qualifies for using ENQUIRER OFFICER regardless of its existing infrastructure. ENQUIRER OFFICER is compatible with all brands of data processing systems, BSA/AML systems, FIU systems, etc. ENQUIRER OFFICER complies with all laws, regulations, and rules. ENQUIRER OFFICER already covers *120 million individuals and 15 million businesses*, and the coverage continues to expand rapidly.

Even if a financial institution does not participate in Section 314(b) information sharing, the financial institution will still benefit tremendously from the ENQUIRER OFFICER alarm signals which are triggered because of specific ***money laundering*** or ***terrorist financing*** risks. ENQUIRER OFFICER empowers the financial institution to effectively detect the illegal proceeds from numerous financial crimes through these alarm signals so that the financial institution can comply with the BSA/AML laws, regulations, and rules.

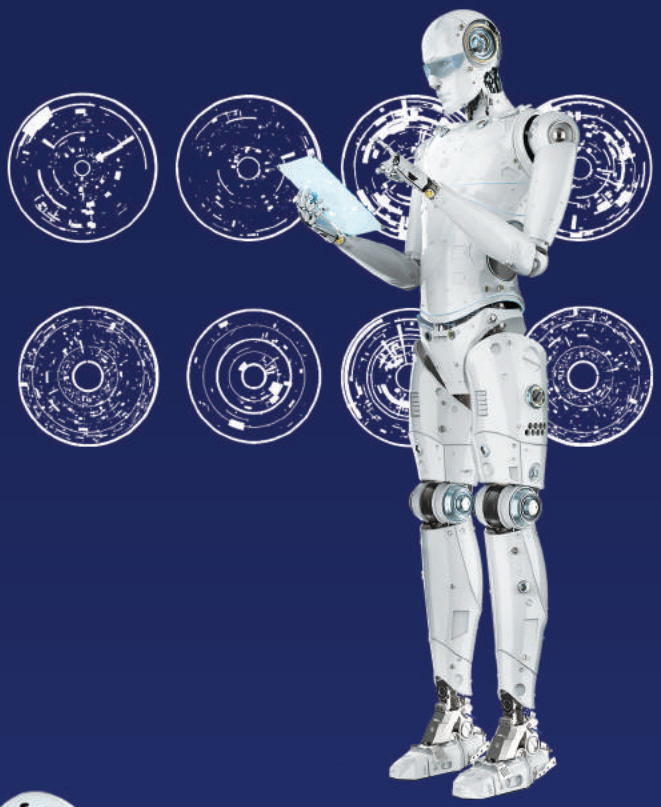
Stop fighting money laundering, terrorist financing, and other types of financial crimes with primitive tools. Call AI Oasis today to install the Financial Crimes Alarm System – ENQUIRER OFFICER.

ENQUIRER OFFICER is the essential and ultimate "Financial Crimes Alarm System" that all financial institutions must have.

AI OASIS

AI OASIS is an Artificial Intelligence technology center of the renowned GlobalVision Systems Group, the largest independent supplier of Anti-Money Laundering, counter terrorist financing, fraud elimination, financial crimes prevention, regulatory compliance, law enforcement, and consumer protection solutions in the world.

AI OASIS uses many patented technologies to set up the innovative and powerful United AI Network™ which consists of thousands of machine-based officers. These officers are deployed under the reputable products: Patriot Officer®, Guardian Officer®, Enquirer Officer®, and Champion Officer®. AI OASIS has established the de facto standards in the financial industry, the law enforcement industry, and the consumer protection industry.



Patriot Officer®
is the #1 BSA/AML/CFT/OFAC solution

Guardian Officer®
is the #1 Anti-Fraud/FACTA solution

Enquirer Officer®
is the #1 Anti-Financial Crimes solution

Champion Officer®
is the #1 Consumer Protection solution

sales@ai-oasis.com (888) 227-7967 9401 Oakdale Avenue, Chatsworth, CA 91311