ANTI-MONEY LAUNDERING POLICY & PROCEDURES : INDEX

DEFINITIONS

Company:

Ole Group Inc.

17800 Castleton Street, Suite 586

City of Industry, CA 91748

United States

EDD: an acronym for Enhanced Due Diligence: additional steps of examination and caution to identify consumers and confirm that their activities and funds are legitimate

Client or Consumer: a Client or Consumer is any individual, partnership, corporation, limited liability Company, association, or other legal entity that utilizes The Company's services.

Negotiable Instrument: a Negotiable Instrument is any item including but not limited to a cashers check, payroll check, government or any other item the Company cashes on behalf of a consumer or group of related consumers or Company.

Monetary Instrument: a monetary instrument is a money order.
Wire Transfer: a wire transfer is monies sent or received via the wire transfer system.

Pre-Paid Debit Card: a prepaid debit card is a loadable debit card provided by the Company as an Agent which allows the consumer to purchase and load debit cards.

Digital or E-Wallet: A digital wallet refers to an electronic device that allows an individual to make electronic commerce transactions.

Client or Customer: For the purpose of this policy, a Client or Customer is any individual, partnership, corporation, limited liability Company, association, or other legal entity that utilizes The Company's services for financial transactions.

Check Cashing transaction: For Purposes of this policy, a check cashing transaction is the cashing of a negotiable instrument and providing value to a customer for the cashing of that negotiable instrument.

OFAC: Office of Foreign Assets Control who publishes a list of those persons, entities and countries that are blocked from doing business with any U.S. Company.

OVERVIEW OF BANK SECRECY ACT / ANTI-MONEY LAUNDERING COMPLIANCE POLICY

It is the policy of the Company mentioned herein to comply with all applicable anti-money laundering laws and regulations, including, but not limited to, the Bank Secrecy Act (BSA) as amended, and the USA PATRIOT Act of 2001, in addition to applicable state laws relative to the business that the Company engages in. Though the Company may not be defined as an "MSB" under certain conditions, it has opted to follow all the rules and regulations governing MSB activity that may apply to its business operations.

Money is "laundered" to conceal illegal activity, including crimes that generate the money itself, such as drug trafficking, and human smuggling. Money laundering conceals the source of illegal proceeds so that the money can be used without revealing where it original came from (source of funds.).

Money laundering causes harm to the public as a whole and weakens the confidence in the financial services industry. The war against money laundering and financial crime is a never- ending, evolving process that requires the commitment of all financial institutions.

The Company is committed to the highest of standards of BSA/AML compliance as so required based on its service offerings and requires that all applicable personnel adhere to these standards in preventing our services and products from being used in any way to facilitate money laundering, terrorist financing and other financial crimes. All staff having to do with the operation, management or creating systems for the company's products or services are required to understand and adhere to these policies and procedures.

Any questions about these policies and procedures may be directed either to the Company BSA/AML Compliance Officer as defined within this AML program.

It is the responsibility of all Company employees and Agents to follow these policies and procedures. At the discretion of Management, violation of these policies and procedures by any employee may serve as grounds for immediate termination or suspension of services if an Agent is found to not be following these policies and procedures.

PROGRAM REQUIREMENTS

The Company's Anti-Money Laundering Policies and Procedures shall be commensurate with the risks posed by the location and size of the business, and the nature and volume of the financial services provided by The Company. Additionally, the Company will provide for policies and procedures preventing money laundering when dealing with transactions it conducts and all other activity that may be defined under Title 31 of the U.S. Patriot Act inclusive should it apply to the scope of operation as conducted by the Company.

As per regulation, these Anti-Money Laundering policies and procedures are to be available for inspection by the Department of the Treasury upon their duly authorized request or any Federal or State jurisdiction that may have over site of the Company.

The program shall include:

- ✓ The designation of a Compliance Officer to be responsible for the day to day adherence to the policies and regulations.
- ✓ Policies, procedures, and internal controls appropriately designed to ensure compliance with prevailing regulations and laws.
- ✓ Internal monitoring of the program to ensure that all policies and procedures are maintained.
- ✓ An independent review of the Anti-Money Laundering Program with the scope and frequency being commensurate with the risk of the financial services provided.
- ✓ Ongoing training relative to implementation of these policies and procedures as well as how to spot suspicious activity and other record keeping requirements.

BSA/AML RISK ASSESSMENT

In accordance with guidance from FinCEN, it is the Company's policy to ensure that a risk assessment is conducted at the inception of the BSA/AML program, and periodically thereafter based on the Company's adoption of any new financial services or products, or substantial changes to the operations, systems or areas served.

Management will then consider the staffing and the level of training necessary to promote adherence with the Company's policies, procedures and processes. To the extent that heightened risks are revealed, Management will also update this in the risk assessment and respond by providing a stronger program that specifically monitors and controls the higher risks identified.

Date of Company Establishment:

MAR, 2016

Principal Representative:

Chau Nguyen

Services Offered:

Our platform incorporates our proprietary payment solution, with prepaid cards including Visa, prepaid MasterCard, Loyalty Rewards card and Union Pay International Card. Our technology simplifies domestic and international payment transactions in multiple global currencies while ensuring fully compliant transactions. Our security systems include digital facial recognition software, Anti-Money Laundering (AML) date compiling software and an efficient Know-Your-Customer (KYC) process that meets and exceeds banking and government agency requirements.

RISK ASSESSMENT:

1 = Low	2 = Medium	3 = High	Score
Rural or Small Metro-Area (<100,000) and Non-HIFCA Non-HIDTA	Medium to Large Metro-Area (>100,000) Non-HIFCA Non-HIDTA	Located in HIFCA* or HIDTA*	3
Single Location	2 – 5 Locations	More than 5 Locations or Agents	3

1 = Low	2 = Medium	3 = High	Score
Single State operation	Mixture of Individuals and Sole Proprietorship Business Entities	Individuals & all types of Business Entities	3
Avg trans. Less than $500	Avg trans. $500 to $2,000	Avg. trans. Greater than $2,000	3

0 = None/1= Low	2 = Medium	3 = High	Score
1 Single Service/ Product	2 to 3 Services/ Products	3 + Services/ Products	3
Check cashing	Wire transfer	Wire transfer and/ or digital currencies	3

0 = None/1= Low	2 = Medium	3 = High	Score
None/To & From non-Foreign OFAC countries & Average Daily # of Transactions is less than 50 per day	To & From non-Foreign OFAC countries & Average Daily # of Transactions is between 50 to 100 per day	To Foreign OFAC countries and/or Average Daily # of Transactions is greater than 100 per day	0
None/Average Daily # of Transactions is less than 25 per day	Average Daily # of Transactions is between 25 to 50 per day	Average Daily # of Transactions is greater than 50 per day	2
No wire transfer/ $ (less than $1,000 per day) and Average Daily # of transactions less than 5 per day	Wire transfer (greater than $1,000 per day) and/or Average Daily # of transactions: 5 to 25 per day	Higher Volume (greater than $1,000 per day) and/or Average Daily # of transactions is greater than 25 per day	2

0 = None/1= Low	2 = Medium	3 = High	Score
More than 5 Years in business	2 – 5 Years in business	1 Year or Less in business	2

1 = Low	2 = Medium	3 = High	Score
MSB Incidental to the Business:	MSB Significant to the Business: 10% to 50% of gross	Primary Source of Business Revenue:	3
ACAMS Certified and/or more than 3 Years of compliance experience in the MSB Industry	1 Year to 3 Years of compliance experience in the MSB Industry	Less than 1 Year of compliance experience in the MSB Industry	1
Whenever changes to BSA/AML regulations changes occur/ At least annually	Only when recommendations or findings are identified by Bank or outside Independent Audit service/agency	Never	1

1 = Low	2 = Medium	3 = High	Score
Training as documented within AML policies and Procedures within guidance of BSA as well as revisions to the Business BSA/ AML Policy & Procedures, and new BSA Federal, State Regulation documented. Testing.	Review of BSA/ AML Policy & Procedures for all new employees required. (testing optional) No supporting training materials or evidence of training is very limited	Review of BSA/ AML Policy & Procedures for all new employees is not documented and no evidence of continual BSA/AML training documented.	1
POS System with Integration of All Services/Products	POS System with Partial Integration of Services/ Products	No POS System (All Manual Processes)	1
Written procedure ID requirement(s) set by amount thresholds that are always followed for Product/Services. Cashier and/or transaction records reviewed weekly by Compliance Officer for Integrated POS Systems.	A written procedure has ID requirement(s) set by cash thresholds for all Financial Product/Services. Cashier tape and/or transaction records are not reviewed by Compliance Officer or are reviewed longer than weekly for Integrated POS Systems.	No written procedures for ID requirement(s) and/ or no formal written process where daily Cashier transactions are reviewed	1

All copies of customer Identifying documents & BSA/ AML required documents kept in secure location only accessible to authorized employees and destroyed in secure manner, after 5 years.	Copies of customer Identifying documents & BSA/ AML required documents kept in secure location only accessible to authorized employees. Records are either kept, or destroyed by owner (no formal process)	Copies of customer Identifying documents & BSA/ AML required documents not kept in secure location accessible only to authorized employees and/or expired documents are thrown in the trash, or not properly shredded.	1
Unexpired, photo identification required for all new customers and/or Identification program in place to ensure that all customers have been identified as so required	Photo identification required for all new customers and alternative Identification program in place for only customers who have conducted transactions requiring Identification based on policy & procedures	No photo or documented identification obtained on all new and repeat customers and/or no photo ID is being obtained on the individual person who conducts or receives the cash payment.	1

1 = Low	2 = Medium	3 = High	Score
At least weekly transactions monitoring for CTR filing, and there was no evidence of CTRs filed with incorrect information	At least monthly monitoring, and/or errors identified in CTRs that have been filed are pertaining to information not mandatory by FinCen	Monitoring occurs more than semi-monthly, and/or internal monitoring has not been administered regularly	1
Periodic transaction monitoring integrating all Product/Services, reviewed at least weekly by Compliance Officer. Documentation available explaining why SARs were not filed, or all filed timely.	Periodic transaction monitoring not integrated with all Financial Product/ Services, reviewed at least monthly by Compliance Officer or documentation not available explaining why SARs were not filed.	No written process in place or written process is not being followed, and/or SARs that were filed were not filed timely or narratives were lacking sufficient information	1
Daily OFAC screening integrated into POS system of All Financial Services/ Products and procedure in place clearly identifying OFAC process or completed manually on each transaction as required	Customer individuals and transactions are not for the benefit of entities outside of the United States. OFAC screening integrated only into Agent POS system. Business determination for not completing OFAC screening on every transaction not documented.	No OFAC process implemented or not documented in BSA/AML Policy & Procedures	1

Risk Rating Level	
>/= 28	Low Risk
29 to 44	Medium
45>	High Risk
Final Risk Rating:	**36**

RISK ANALYSES:

Consumers engage with the company as follows: Consumers contact the company via:

- Website: www.olegroupinc.com
- Phone: 626-295-2620

The following daily thresholds apply:

$25,000 per month or $5,000 per transaction for cash in transactions.

Cash out transactions are subject to vendor policies and procedures.

The Company's typical transactions are with regular customers with usual transaction of $5,000 or less.

The Company does serve customers living abroad.

Any customer conducting more than $100,000 per month will not be permitted.

Any apparent structuring or any other events that may be deemed suspicious by the Company will require a case file to be opened which will include the customer information, transactions, nature of activity and any enhanced due diligence required.

If EDD is warranted, the customer is checked for negative news, social media pages, attempt job verification etc. and as required, a confirmation of source of funds.

The Company will only conduct business where it is lawfully allowed to do so. The Company does not maintain Agent relationships beyond doing business with third party vendors.

All transactional history will be reviewed to confirm if any thresholds were met which would require a currency transaction log (CTR), which should be referred to the Compliance Officer to confirm if a CTR is required to be filed.

The Company has policies and procedures in place that limit its risk of conducting transactions that may promote money laundering such as maintaining customer verifications, enhanced due diligence, as well as its high percentage of repeat customers, its mitigation of risks as outlined in its AML program, its risk matrix and analyses. The Company maintains a "MEDIUM" risk rating.

HIFCA (High Intensity Financial Crime Area)

Regions	Area Jurisdiction by Counties
California Northern District	Monterey, Humboldt, Mendocino, Lake, Sonoma, Napa, Marin, Contra Costa, San Francisco, San Mateo, Alameda, Santa Cruz, San Benito, Monterey, Del Norte
California Southern District	Los Angeles, Orange, Riverside, San Bernardino, San Luis Obispo, Santa Barbara, Ventura
Southwest Border	Arizona–All Counties; Texas–Counties Bordering, and adjacent to those bordering, the U.S. and Mexico Boundary
Chicago	Cook, McHenry, DuPage, Lake, Will, Kane
New York	New York–All Counties; New Jersey–All Counties
Puerto Rico	Puerto Rico–All Areas; U.S. Virgin Islands–All Areas
South Florida	Broward, Miami-Dade, Indian River, Martin, Monroe, Okeechobee, Palm Beach and St. Lucie

HIDTA (High Intensity Drug Traffic Area)

There are currently 28 HIDTAs, which include approximately 16 percent of all counties in the United States and 60 percent of the U.S. population. HIDTA-designated counties are located in 46 states, as well as in Puerto Rico, the U.S. Virgin Islands, and the District of Columbia

For more information on HIFCA/HIDTA jurisdictions:

www.whitehousedrugpolicy.gov

**International High-Risk Jurisdictions Some foreign jurisdictions are described as posing a higher risk for potential money laundering, financial crime or terrorist-financing activity. International high-risk geographic locations generally include:

- ✓ Countries subject to OFAC sanctions, including state sponsors of terrorism http://www.treas.gov/offices/enforcement/ofac/
- ✓ Countries identified as supporting international terrorism under section 6(j) of the Export Administration Act of 1979, as determined by the Secretary of State. http://www.state.gov/s/ct/rls/crt/
- ✓ Jurisdictions determined to be "of primary money laundering concern" by the Secretary of the Treasury, and jurisdictions subject to special measures imposed by the Secretary of the Treasury, through FinCEN, pursuant to section 311 of the PATRIOT Act. http://www.fincen.gov/reg_section311.html
- ✓ Jurisdictions or countries identified as non-cooperative by the Financial Action Task Force on Money Laundering (FATF). http://www.fatf-gafi.org/
- ✓ Major money laundering countries and jurisdictions identified in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR), in particular, countries that are identified as jurisdictions of primary concern. http://www.state.gov/p/inl/rls/nrcrpt/
- ✓ Offshore financial centers (OFCs) as identified by the U.S. Department of State: http://www.imf.org/external/ns/cs.aspx?id=55 The Company will maintain outside Vendors as required and will ensure that those vendors have policies and procedures in place as required. The Company retains customer information and reviews transactions that may be suspicious.

THE APPOINTMENT OF BSA/AML COMPLIANCE OFFICER

BSA/AML Compliance Officer Qualifications and Experience

The Owners/Senior Management shall ensure that the individual appointed to serve as the Company's BSA/AML Compliance Officer has sufficient training and experience to effectively serve in this capacity and oversee the operations of the Anti-Money Laundering (AML) Program.

The Company will convene annually to reaffirm their commitment to this compliance program and to demonstrate their support of the Compliance Officer in a company resolution.

- ✓ On the anniversary date of this compliance program the Compliance Officer will call a meeting of Stockholders at which an annual report prepared by an independent reviewer as to the adequacy and performance of this compliance program will be provided.
- ✓ The Directors or Officers at the conclusion of their annual compliance meeting, will draft and sign a new Company Resolution memorializing their commitment
  - A Compliance Program
  - The Compliance Officer
  - An Independent Reviewer

Designated BSA/AML Compliance Officer Information

The Company has appointed the following individual to serve as the BSA/AML Compliance Officer on a daily basis, until otherwise removed or terminated:

Shea Writer

(Print Full Name)

CUSTOMER IDENTIFICATION PROGRAM (CIP)

Prior to conducting a transaction with the Customer, the Company will make a diligent effort to know, with reasonable certainty, the identity of the Client and shall adhere to this policy as so applicable. This shall not apply to repeat customers who have already been identified or customers not otherwise required to meet certain KYC or CIP requirements as defined within this program or otherwise not required by law. Additionally, the Company will adhere to all identification processes relative to State, County or City regulations for which it operates in as applicable.

Examples of acceptable forms of identification include, but are not limited to, an unexpired, Government issued identification document bearing a photograph (or similar safeguard) or a valid permanent alien ID. All identification documents must be of a format familiar to The Company or otherwise verifiable.

All identification documents must be unmolested, current, valid, and signed or notarized if so required by the document. Additionally, all Identification received should comply with all State, County, and City regulations where the company conducts business. If the customer does not have an acceptable form of identification or refuses to provide one as required, the Company will refuse to do business with them.

In an attempt to know their customer, The Company will make a diligent effort to become familiar with the types, amounts, and frequency of transactions of any repeat customer. If a transaction is deemed unusual in that it differs from, or is conducted differently from the previous practices of a Client, or deviates from a Client's normal business protocol, the Compliance Officer will be notified so they may conduct the appropriate investigation to determine what, if any, action should be taken. The Company will also make use of Ocular•KYC in an effort to validate the consumer information in addition to other required CIP information as otherwise applicable.

CURRENCY TRANSACTION REPORTING (CTR'S) & CMIR'S

The Company does not conduct transactions in excess of $5,000 per day per customer or related customer. The Company will be required to file a CTR anytime there is a transaction or group of transactions greater than $10,000 in currency in any business day by, or on behalf of the same person. A CTR is required when a transaction meets the following requirements:

- ✓ In currency;
- ✓ Cash in or cash out transactions
- ✓ Greater than $10,000 in sum;
- ✓ By, or on behalf of, the same person or entity;
- ✓ Occurs within a business day.

The form will be reviewed for accuracy and completeness by the Compliance Officer who will then sign it as the Approving Officer, and file it using the BSA E-File system at http://bsaefiling.fincen.treas.gov/main.html

All Forms filed will be retained electronically within the Company's database for a period of not less than 5 years.

CMIR 105's will be filed on all foreign currency transactions of $10,000 or more on all foreign transactions outside of the U.S. This document will be filed manually within 15 days of the date of the transaction

The form will be mailed to:

- ◉ **Commissioner of Customs, Attention:**
- ◉ **Currency Transportation Reports, Washington DC 20229.**

SUSPICIOUS ACTIVITY REPORT (SAR-MSB)

The Company shall at all times comply with all applicable anti- money laundering laws and regulations, pertaining to Suspicious Activity Reporting (SAR) requirements under the BSA. Transactions will be monitored carefully to determine if any suspicious transactions may take place.

The Company must be aware and be able to track all transactions that may be suspicious. This should be conducted by screening the transactions as well as the Company.

- ✓ A SAR should be filed in any instances where it is suspected that the funds involved in the transaction are derived from illegal activity, are being used for a criminal purpose, or where the transaction has no legitimate business purpose or is designed to evade a reporting requirement (e.g., a CTR filing)

- ✓ It is the responsibility of the BSA/AML Compliance Officer or its designee to ensure the following:

    - That employees are trained to report all suspicious transactions to the Compliance Officer and provide all necessary information, including consumer ID information, on any suspicious transactions.;

    - That employees are trained to know that it is illegal for any Company employee to inform any person involved in a suspicious transaction that a SAR will be or has been filed. Any employee violating this law may be prosecuted by the authorities, and will be subject to termination by the Company;

    - That employees are trained to know that it is illegal for an employee to engage in “willful blindness,” i.e., to turn a “blind eye” to consumer activity that the employee knows, or reasonably should know, involves money laundering or other illegal conduct;

    - The Compliance Officer will investigate transactions reported by all employees as well as identified during periodic reviews and report to the Compliance Officer all findings within 30 days. A decision whether or not to file the SAR will be made;

- Where the Company becomes aware (as opposed to suspicious) of a violation of law that requires immediate attention, such as terrorist activity or an ongoing money laundering scheme, appropriate law enforcement authorities will be notified by either the Compliance Officer in addition to filing an SAR if required;

  Note: FinCEN has established a Financial Institutions Hotline, 866-556- 3974, for all types of financial institutions to voluntarily report transactions that may relate to terrorist financing or other terrorist activity.

✓ Should it be determined that a SAR will not be filed, the reason(s) will be notated in writing and kept with all previous filed SAR records;

✓ Should it be determined that a SAR is to be filed then it must be filed within 30 days after the date detection;

✓ All SARs are to be completed through the BSA E-Filing system of FinCEN, refer to the following link: http://bsaefiling.fincen.treas.gov/main.html for instructions;

✓ All authorized personnel (including Management) has access to the BSA E-Filing system of FinCEN;

✓ SAR narrative sections of each SAR filed must contain a detailed description of the transaction, including the nature of the suspicious activity (e.g., structuring), the identity and addresses of all parties involved, physical descriptions, types of instruments involved, types and numbers of all ID presented, amounts involved, and an explanation as to why the Company believes the activity is suspicious.

✓ Refer to the FinCEN website and SAR instructions for more detailed directions on completion of the SAR narrative section;

- All supporting documentation is being maintained for a period of five years from the date of detection of the suspicious activity.

- The MSB should be responsible based on the transactions for determining if a SAR is required at which time a SAR would be filed.

In the case of a SAR filing, the Company or employees will not give the client involved in the suspicious transaction any notification that the report is being filed. The SAR record must be kept for no less than five (5) years.

EXAMPLES OF SUSPICIOUS CONSUMER ACTIVITY:

- ✓ Consumer uses false ID
- ✓ Consumer alters transaction upon learning that he/she must show ID
- ✓ Consumer alters the spelling or order of his/her full name
- ✓ Two or more persons working together to break one transaction into two or more transactions in order to avoid AML/BSA reporting requirements
- ✓ A consumer who presents different identification each time a transaction is conducted
- ✓ A legitimate ID that appears to have been altered;
- ✓ A transaction in which it appears the customer is attempting to cause the CTR form not to be filed, or is trying to cause the filing of a false or incomplete form, or a transaction that appears to be "Illegal";
- ✓ The activity being conducted by the customer appears to be suspicious in that the transaction does not meet with the usual business practice of the customer or, the activity being conducted is not usual for the business;
- ✓ The Company knows, suspects or has reason to know or suspect, that the transaction involves funds derived from illegal activity or is conducted in order to hide or disguise funds from their illegal origin or;
- ✓ The transaction is designed, whether through structuring or other means, to evade any regulations promulgated under the Bank Secrecy Act or;
- ✓ The transaction appears to have no reasonable business purpose after examining the available facts.
- ✓ The Customer sends excessive amounts determined by their history

- ✓ There are multiple purchases or sales from the same address by various customers.

Situations like the ones described in the previous sections may often be found upon closer examination to be completely legitimate. Reasonable judgment must be made to determine if the activity is suspicious or not.

Three Stages of Money Laundering

- ✓ Placement: Putting illegal money/proceeds into the financial system. Examples of Placement are opening accounts and depositing cash, or buying many money orders, purchasing phone cards or prepaid debit cards, and sending more than one money remittance to different people.

- ✓ Layering: Changing the money/proceeds of crime into another form and creating complex layers of financial transactions to disguise the audit trail, source and ownership of funds. Example of Layering is a person has multiple money orders purchased with illegal money and then goes to another location to use the money orders to send money to a person in a different country.

- ✓ Integration: Placing the laundered money/proceeds back into the economy to make it look like the money is for legitimate purposes. Example of Integration is taking illegal money and purchasing a house, jewelry, or a new car.

SERVICE POLICIES AND PROCEDURES

No transaction may exceed $5,000 per day or $25,000 per month.

ENHANCED DUE DILIGENCE

All transactions in excess of $25,000 monthly will be placed into a separate log for monitoring. The customer logs are then verified for potential suspicious activity based on frequency and amounts of transactions which will include:

- ✓ the customer information
- ✓ transactions, nature of activity
- ✓ enhanced due diligence required.
- ✓ EDD conducted

Based on the findings of the Enhanced Due Diligence, the Company may take any or all of the following action

- ✓ A confirmation with the customer as to the source of funds.
- ✓ A confirmation with customer confirming reason for purchase.
- ✓ 3rd party database validation to help confirm the consumer.
- ✓ Suspension of customer account
- ✓ Revocation of customer account
- ✓ Filing of a SAR
- ✓ Referral to law enforcement.

RECORED KEEPING REQUIREMENTS

Accurate and thorough record keeping is critical to the Company's Compliance Program. In order to comply, it must adhere to the following:

- ✓ Business records are to be maintained in an orderly fashion in a secure area. Records are to be readily accessible for production to federal and state examiners as well as the Company's financial institution;
- ✓ Copies of CTRs must be maintained for a period of five years from the date of transaction;
- ✓ A copy of all transactions including all order information.
- ✓ Copies of Suspicious Activity Reports (SARs), and any related documents (decisions not to file), must be maintained for a period of five years from the date of detection of the suspicious activity;
- ✓ Tax and supporting accounting records are to be maintained for a period of at least seven (7) years as required by Internal Revenue Code regulations;
- ✓ The Company must adhere to any Geographic Targeting Orders (GTOs) issued by the Treasury Department. GTOs may require financial institutions in an area to keep additional records beyond the time specified by the Bank Secrecy Act. The targeting order may specify the form in which MSBs are to keep the specified records, and the length of time they are to keep them;
- ✓ All consumer records and records bearing confidential financial information shall be maintained in a secure area, and protected from disclosure.

BSA/AML EMPLOYEE TRAINING

The Company, through the Compliance Officer will train all employees to guard against money laundering, terrorist financing, and fraud. Training must be provided for all new hires for anyone who works on the systems implementing KYC, CIP or Enhanced Due Diligence, operational staff, or management within 30 days of hire.

Additional training must be provided for effected persons as described herein at least annually to update and maintain existing knowledge as well as provide new information pertaining to BSA regulations as needed.

Initial Training and Newly Hired Employees

- ✓ It will be required that every employee will be screened prior to their being hired. The screening may include but is not limited to:
  - Criminal background checks including OFAC;
  - Credit/Judgment checks;
  - References with past employers ;
- ✓ It is required that every new employee will be instructed on his appropriate responsibilities under this compliance program prior to commencing his official duties.
- ✓ The following PATRIOT Act and Anti-Money Laundering issues will be covered:
  - What is money laundering
  - How to properly maintain foreign currency logs
  - Filing of CTR's
  - Record keeping
  - Suspicious Activity Reporting (SAR)
  - Money laundering penalties

Existing Employees

- ✓ Continuing ongoing training is essential to this compliance program. Existing employees are required to remain knowledgeable of all BSA and AML regulations.

- ✓ The Compliance Officer is responsible for the creation of a Compliance Library that will be accessible to all employees. These training materials will be provided by the Compliance Officer and may include written material, videos, examinations and articles. There will be a training log that indicates the employee name, type of training received and date of training. The Employee will sign this log upon completion of such training. The Compliance Officer will require each employee to receive training no less than semi-annually.

- ✓ Annually the Compliance Officer will administer an internally designed Anti-Money Laundering Examination. This test shall consist of both true/false and multiple-choice questions.

    - Every employee will take an examination within 30 days of hire and annually thereafter with a passing score of no less than 70%.

    - If a compliance deficiency is observed or discovered the Compliance Officer will determine which employee was negligent and review the specific policy, procedure or situation that was overlooked.

    - The Compliance Officer will document the negligence in the form of a written reprimand and include a copy of in the employee's personnel file. Repeated violation of this compliance program will be cause for termination.

    - If the employee fails the examination, they will be retested within 30 days. Additional failure may be cause for termination.

Record-keeping (Training)

- ✓ The BSA/AML Compliance Officer will ensure that all new employees complete acknowledgements of receipt of the company's AML Compliance Policies and Procedures, and will obtain updated acknowledgements when changes to the Policies and Procedures are made;

- ✓ The BSA/AML Compliance Officer will retain copies of all refresher training material used, including results of any testing, certificate of completion, and training logs as applicable;

- ✓ The BSA/AML Compliance Officer will maintain all of the above records for a period of 5 years from the date performed.

The Compliance Officer shall be subject to additional training from time to time to ensure that he or she is up to date on all applicable state and federal requirements and shall receive enhanced training in the recognition of suspicious activity and enhanced due diligence. This training may be received from outside sources including but not limited to seminars, webinars or conventions.

RISK ASSESSMENT

Regardless of where risks arise, money services businesses must take reasonable steps to manage them. 31 C.F.R. § 103.125 requires money services businesses to establish anti-money laundering programs tailored to their operations and the money laundering risks posed by those operations. Additionally, to assist in developing its AML program, the Company will conduct a risk assessment on not less than annual basis.

The Reviewer's risk assessment will be based on objective criteria and should identify and assess the money laundering risks that may be associated with its unique products, services, consumers, and geographic locations.

INDEPENDENT REVIEW

The Company shall conduct an AML independent examination in accordance with guidelines set forth in the FinCEN MSB Examination Manual (available at www.fincen.gov), and in accordance with any further guidance materials as set forth by FinCEN, IRS and other applicable regulatory authorities.

The scope and frequency of the exam must be appropriate with the risk of the financial services provided by the Company and the geographic area served.

Risk Rating Level	Recommended Time Periods
Low Risk	Within the first year of offering MSB related services
Medium Risk	Within 6 months of initial offering of MSB related services and then no less than annually
High Risk	Every 6 months.

The independent exam function may be performed by a properly qualified BSA/ AML professional not responsible for regular administration or maintenance of the Company and who is not the Company's designated Compliance Officer.

PROCEDURE

Annually, the Compliance Officer will cause for an independent review to be conducted. This expert may be a Certified Anti-Money Laundering Specialist (CAMS). Additional specialized training (i.e. law enforcement or auditing) will be a consideration in the selection of this reviewing party.

The primary purpose of the independent review is to monitor the adequacy of this AML Compliance Program. The review should determine whether the business is operating in compliance with the requirements of the Bank Secrecy Act and the unique policies and procedures of the Company.

- ✓ The review also should cover all of the anti-money laundering program actions taken or defined as part of the responsibility of the Compliance Officer. These actions include, for example, the determination of the level of money laundering risks faced by the business, the frequency of Bank Secrecy Act anti- money laundering training for employees, and the adoption of procedures for implementation and oversight of program-related controls and transactional systems.

- ✓ The review at minimum will ascertain whether:

    - Reports (CTRs, SAR's) are timely and accurate
    - Records (wire, logs, supporting SAR records) are being maintained
    - FinCEN Registration is current
    - State Licensing is current as required
    - Policies and Procedures cover all applicable Products & Service
    - Policies & Procedures are adequate for the level of risk involved
    - Prior recommendations have been incorporated into the Compliance Program, including recommendations from:
        - Independent Reviewers
        - IRS Examiners
        - State Auditors
    - The Review will include transactional testing to determine if the Compliance Program has been reasonably designed and implemented to protect the Company from becoming involved in a financial crime which will consist of no less than 5% of the Company's monthly transactions.

- ✓ The review will also cover the actions and the responsibilities of the Compliance Officer. Including:
  - Internal Monitoring
  - Records & Reports Maintenances
  - Overall attitude & knowledge of BSA issues
- ✓ The Independent Reviewer will determine if the design and implementation of the Employee Training Policies & Procedures of this Compliance Program are sufficient to protect the Company from becoming involved in a financial crime. Included in this evaluation:
  - The initial training & testing of new employees
  - The ongoing training &testing of existing employees
  - Documented in training logs
  - Timeliness of training material
  - Overall Employee attitude & knowledge of BSA issues

Annual Compliance Report

- ✓ The BSA/AML Compliance Officer will ensure any findings, including any BSA violations, deficiencies or recommendations concerning the Compliance Program is reported in a timely manner to Senior Management.

- ✓ Any BSA violations or deficiencies indicated by the independent examiner are to be remedied within thirty (30) days by the BSA/AML Compliance Officer. All further recommendations will require to be completed in designated period determined or an explanation detailing the reasons why recommendations will not be completed by the next independent exam are to made by the BSA/AML Compliance Officer. The results of the report and explanation of all corrective actions are to be part of the Compliance record of the Company and shall be maintained for a period of not less than five (5) years by the Compliance Officer.

Procedure

- ✓ After the report is issued, the Reviewer & the Compliance Officer will converse regarding any deficiencies and weaknesses discovered during the review.

- ✓ The Compliance Officer will resolve any issues that resulted in a missing or incorrectly filed BSA reports or records;

- ✓ The Compliance Officer will draft and send to the Reviewer an action plan to address any deficiencies and weaknesses discovered during the review.

- ✓ The Compliance Report and the Compliance Officer's action plan should be retained for five years;

- ✓ If requested, the Annual Compliance Report(s) will be provided to government examiners and law enforcement personnel who have authority to examine such documents;

- ✓ If requested by other interested parties, such as State Regulators, Vendors or bank personnel, the Compliance Officer will determine if the request is appropriate;

- ✓ If the request is appropriate the Compliance Officer will forward a copy of the Annual Compliance Report to the other interested parties;
- ✓ If the Compliance Officer determines that the request is inappropriate he will draft a letter stating the reasons for the conclusion.

MONEY SERVICE BUSINESS (MSB) REGISTRATION REQUIREMENTS

The Company will comply with all applicable MSB registration requirements as required. A business is required to be registered with the U.S. Treasury Department if it falls in one or more of the following types of Money Service Business categories. (1) check cashers, (2) issuers, sellers or redeemers of money orders, traveler's checks, or stored value cards, (3) money transmitters principal (but not individual agents), and/or (4) dealers in foreign currency exchange. However, a business that does not conduct transactions over $1,000 for one person during a single business day is not an MSB and need not register. Additionally, if the Company is acting as an Agent of other MSB's, it need not register.

- ✓ It is the responsibility of the Compliance Officer and Senior Management to ensure that should the Company be required to register as an MSB that it adheres with the following:
  - Registration of Money Service Business forms are to be completed and filed electronically through the FinCEN E-Filing system (www.fincen.gov/forms/e- filing). Failure to register may result in a civil penalty of up to $5,000 per day for each day an MSB fails to comply;
  - Copies of all filed MSB registration forms and supporting documents must be maintained for period of not less than five (5) years;
  - Registration is completed only on the Company's main office; each branch office of the Company is not required to file a separate registration form;
  - The initial registration period is two years. Registration must be renewed after expiration of the initial two-year period, and no later than December 31, every two years thereafter, by completing and re-filing the FinCEN Registration of Money Service Business form electronically,;

- The Company must re-register in the event of any of the following: (1) a transfer of more than 10 percent of ownership or control of the business; (2) a change in ownership or control that requires re-registration under state law; or (3) a more than 50-percent increase in the number of the MSB's (i.e., money transmitters) agents.

NOTE: Correcting a previous registration does not constitute a re-registration and current registration status may be confirmed by ensuring that the Company is listed on FinCEN's

INTERNAL MONITORING PROCESS

It is the policy of the Company to engage in appropriate transaction monitoring to ensure compliance with applicable BSA requirements, including most importantly identification and reporting of suspicious activities, as applicable. Based on risk and industry standards, this will occur no less than monthly.

- ✓ Monitoring shall include regular review of transaction records to ensure compliance with suspicious activity reporting, currency transaction reporting requirements, SAR's and CTR's and wire records s as applicable
- ✓ Overall transaction monitoring functions shall be overseen by the BSA/AML Compliance Officer who shall report to Management. Specific monitoring functions may be delegated to other personnel who report directly to the Compliance Officer.
- ✓ Monitoring shall include both employee monitoring of consumer activity at point of sale, as well as compliance personnel review of transaction reports/ records, including reports generated by the Company's systems and reports available through its provider and vendors, where applicable.
- ✓ The Company may utilize available systems based filtering and exception reporting mechanisms as well as spreadsheets or other tools to facilitate this process.
- ✓ Management shall periodically review monitoring procedures to ensure their appropriateness.
- ✓ The Compliance Officer shall be responsible for completion of a regularly scheduled review of activity to ensure appropriate record-keeping, CTR compliance and identification of suspicious activities.
- ✓ Monitoring will include review of available daily records and weekly/ monthly transaction reports. The Company may rely on available systems generated reports for this purpose.
- ✓ Monitoring will include identification of potential structuring patterns, such as consumers attempting to conduct multiple transactions to avoid the $10,000 threshold, or other suspicious activities.

✓ A Sampling of the following will be included:

- sample of SAR's filed during the review period to ensure completeness and timely filing;
- A sample of 10% of the Monthly transactions during the month in review;
- A sample of training logs for employees hired during the review period and
  follow up training.
- A review of records to ensure that CTR's, SAR's and wire records are being filed

RESPONDING TO LAW ENFORCEMENT / IRS REQUESTS & GTO'S

The Company shall maintain appropriate records under the BSA and to respond quickly and accurately to all legitimate requests from law enforcement for reports and records maintained by the Company in connection with its AML program.

It is the responsibility of the BSA/AML Compliance Officer and Senior Management to ensure the following:

- ✓ All employees are aware to immediately notify and provide any and all notices for Title 31 examinations, notices of state regulatory examinations, and any other notices from the IRS, FBI, or other federal or state agency or authority to the Compliance Officer or Senior Management.

- ✓ All subpoenas and other written requests for records from law enforcement shall likewise be immediately provided to the Compliance Officer and/or Management.

GEOGRAPHIC TARGETING ORDERS

If the US Treasury issues a Geographic Targeting Order it is the policy of the company to completely and earnestly adhere to the new directives and to disseminate this information to all appropriate company personal.

- ✓ The existence of a Geographic Targeting Order will not be revealed to the general public for any reason or at any time

- ✓ When Geographical Targeting Order is received, the Compliance Officer will notify all store personnel including management as to the change in reporting and recording thresholds or any other portion of this compliance that is affected. But will not disclose information contained in the Order that is not pertinent to the employee's job:

    - Notification shall be done in a written memo. This memo will explain how the Geographic Targeting Order impacts the day-to-day operation.

- Each member of the organization will be required to read, sign and date a copy of the memo. The signed memo will be retained in the employee's personnel files.

✓ If the Compliance Officer deems the Targeting Order to be permanent in nature (longer than 3 months) then the Compliance will adjust this compliance program to reflect the changes.

TITLE 31 BSA EXAMINATIONS

The Compliance Officer serves as the primary contact for the Company with regards to Title 31 BSA Examinations.

The IRS Appointment Letter & Form 4564 (Information Document Request) will be immediately forwarded to the Compliance Officer.

The Compliance Officer will notify upper management & staff members of the examinations start date, end date and exam scope.

The Compliance Officer will gather all requested records noted on IRS Information Document Request Form. Typically the documents requested are:

- ✓ Written AML Compliance Program
- ✓ FinCEN Registration Confirmation
- ✓ Independent Compliance Report
- ✓ Internal Monitoring Compliance Reports
- ✓ Findings & Responses to State Audits
- ✓ Copies of BSA Reports
- ✓ Monthly Bank Statements
- ✓ Daily & Monthly work records

The Compliance Officer will coordinate the examination on behalf of the company. Office space will be made available if needed in order for an investigation to be conducted.

The Compliance Officer will be on site with the examiners and will promptly respond to all requests.

If requested by the examiners, employees will be made available for interviews.

If the IRS examiners issue a Violation Notification Letter 1112 the Compliance Officer will notify upper management of the findings and draft a response letter detailing the necessary corrective actions. The notification letter and the corrective actions response letter will be retained for five years and copies will be provided to any appropriate entity.

If the IRS examiners issue a No Change Letter 4029 will notify upper management and retain the finding for five years and copies will be provided to any appropriate entity.

OFFICE OF FOREIGN ASSETS CONTROL (OFAC)

The Company shall not conduct or assist in any transaction with any person or entity appearing on the OFAC SDN List and to comply with other OFAC requirements pertaining to sanctioned countries.

- ✓ The Office of Foreign Assets Control (OFAC) is an office of the Department of the Treasury that enforces the U.S. government's economic sanctions against certain countries, such as Iran and North Korea, as well as sanctions placed on individuals and organizations involved in terrorism and criminal activity. The names of these individuals and organizations are maintained on OFAC's Specially Designated Nationals (aka SDN) and Blocked Entities List (SDN List) and are changed on a continuous basis.

- ✓ It is illegal for a financial services Company to complete or assist in any transaction for any amount involving an individual or organization appearing on the SDN List or which violate the economic sanctions against certain countries. Federal law requires all financial institutions to immediately report and if possible, block any such attempted transactions. It is the responsibility of the BSA/AML Compliance Officer and Senior Management to take the following steps as applicable:

OFAC and Funds Transfers

The Company will ensure that it utilizes software to automatically screen consumer's funds transfers against the SDN List, as well as comply with any other specific OFAC policies and procedures. It may manually do so at www.treas.gov.ofac

Transactions That Must Be Checked Against the SDN List

- ✓ It is illegal to process <u>any</u> transaction involving an SDN, regardless of the amount. As stated above, should the Company choose to offer certain services to consumers, then the Company's will check against the SDN list. The following types of transactions should also be screened against the SDN list:

- ✓ Every transaction involving Foreign Individuals and Foreign Corporate Entities

- ✓ Every International or Cross-Border transactions
- ✓ Any transaction that may involve any person or organization appearing on the SDN list (possible terrorist or international criminal organization)

Gathering Consumer Information

All information pertaining to a transaction (especially sender and beneficiary information) is to be obtained prior to conducting the transaction. Otherwise, if the consumer's name appears on the SDN List, it may not be possible to gather additional information on that individual.

Determining whether an individual or entity is an SDN requires the collection as much information as possible on the consumer to compare it closely with the SDN List and prevent any delay in completing the transaction.

Company Responsibilities

When the Company receives notification or believes that a consumer that is scanned against the SDN list is a potential SDN list match (i.e., the consumer's name appears to match a name on the SDN list). In such event, the following procedures should be followed:

- ✓ Place the transaction into a pending status without completing
- ✓ Alert the Compliance Officer before processing the transaction
- ✓ Do not return the funds (if collected) or process the transaction without the approval of the Compliance Officer

Compliance Officer/Management Responsibilities

The Compliance Officer will check the correct spelling of the consumer's name, the date of birth, place of birth, and other identifying information.

If it is clear that the consumer's information does not match the information on the SDN list the Compliance Officer will approve the transaction as applicable and then the allow continuance with the transaction.

However if, after checking the correct spelling of the consumer's name, the date of birth, place of birth, and other identifying information the Compliance is unable to confirm whether or not the consumer's information matches the information on the SDN list. The Compliance Officer will make the decision to either ask the consumer to return with additional documentation to permit a more complete investigation and comparison against the SDN List before the transaction may be authorized or refuse to complete the transaction.

In a situation where, after checking the correct spelling of the consumer's name, date of birth, place of birth, and other identifying information the Compliance Officer is certain that the consumer's information matches the SDN list. The Compliance Officer shall immediately contact the OFAC Hotline at 1-800-540-6322 and follow the instructions provided by the OFAC representative.

All consumer questions regarding OFAC compliance should be directed either to the Compliance Officer or directly to the OFAC website: www.treas.gov/ofac.

CONSUMER PRIVACY

The Federal Safeguards Rule of the Gramm-Leach-Bliley Act requires all companies that offer consumers financial products or services to their consumers to explain their information-sharing practices to their consumers and to safeguard sensitive private information about their consumers. The Company shall comply with these requirements to avoid potential consumer identity theft and related criminal activity.

It is the responsibility of the BSA/AML Compliance Officer and Senior Management to ensure the following:

- ✓ Maintain privacy of all consumer files, consumer Social Security numbers, consumer personal information, and all other consumer records. All consumer records shall be maintained in a secure area.

- ✓ Never give out to any person or company any consumer information, unless (i) expressly authorized by the consumer and as necessary to complete a transaction, (ii) pursuant to a lawful request (e.g., subpoena or summons) by law enforcement or other government agency, or (iii) to the Company's Financial Institution based on contractual agreement signed permitting the sharing of consumer information. Any requests for consumer information from law enforcement or other agency must be referred immediately to the Compliance Officer.

- ✓ Immediately report to the Compliance officer and/or Management any attempt to get confidential consumer information or records. This includes any unauthorized use of consumer information by Company employees. The Company will then report the incident to law enforcement and file the appropriate Suspicious Activity Report where applicable.

- ✓ The consumer is to be immediately contacted by Management in the event of unauthorized access or disclosure of such information, or in the event of theft or loss of such information. Early notification can help the consumer prevent improper use of his/her confidential financial information.

MAINTAINING COMPUTER SYSTEMS

These policies and procedures shall apply to the Company's computer information systems, including network and storage systems.

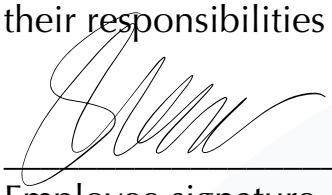
- ✓ Electronic consumer information must be stored on a secure server, which is not accessible by unauthorized personnel.
- ✓ Servers are to be maintained at all times within the secure confines of the office, or other secure area, accessible only by the Company and its employees, or other authorized personnel.
- ✓ Consumer information should not be stored on a server with an Internet connection without appropriate security and/or firewalls to protect the integrity of such information.
- ✓ Backup media and archived data shall be maintained off-line, within the secure confines of the office, or other off-site secure location, and accessible only by the Company and its employees.
- ✓ The Company shall obtain and install all necessary patches and program updates to resolve software and systems vulnerabilities.

Security Breaches

- ✓ In the event of a security systems breach, the Company should take immediate measures to report and correct the problem. Quick action on the part of the Company allows consumers to take steps to lessen misuse of their information, and may protect the consumer from potential identity theft and credit-rating damage.
- ✓ Both law enforcement and the consumer shall immediately be notified by Management in the event of unauthorized access or disclosure of private information, or in the event of theft or loss of such information. In addition, notification to credit bureaus may be advisable.

EMPLOYEE ACKNOWLEDGEMENT OF RECEIPT

The undersigned employee hereby acknowledges that he/she has reviewed the Company's policies and procedures and further confirms that they understand their responsibilities as it pertains to the procedures.



Employee signature

Shea Writer

Employee name (print)

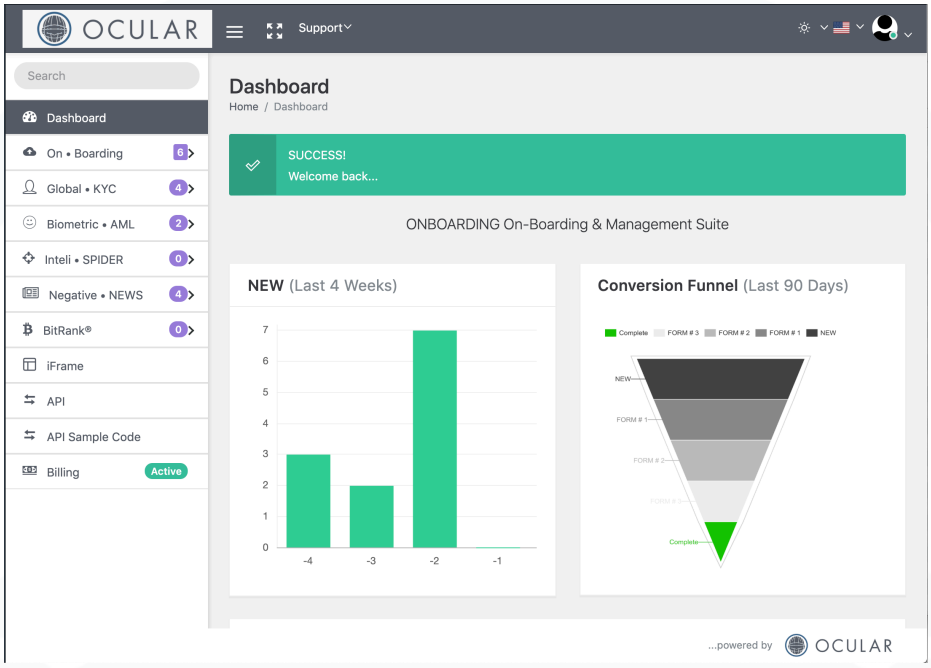
16 AUG 2019

Date

APPENDIX I: HOW TO KYC/AML VIA OCULAR•KYC

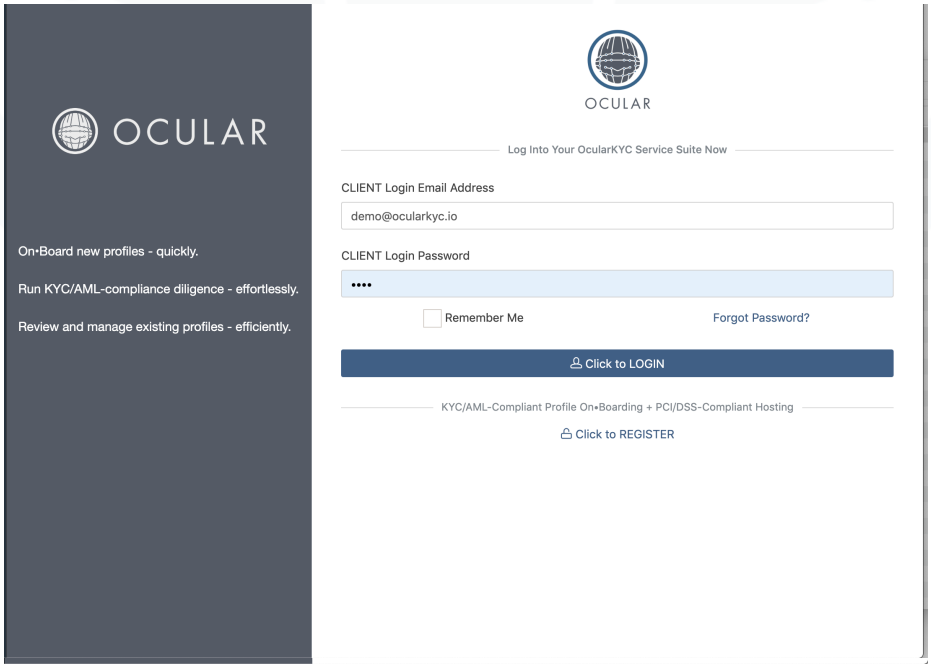
LOG-INTO YOUR OCULAR•KYC ACCOUNT

✓ Go to: https://www.OcularKYC.io



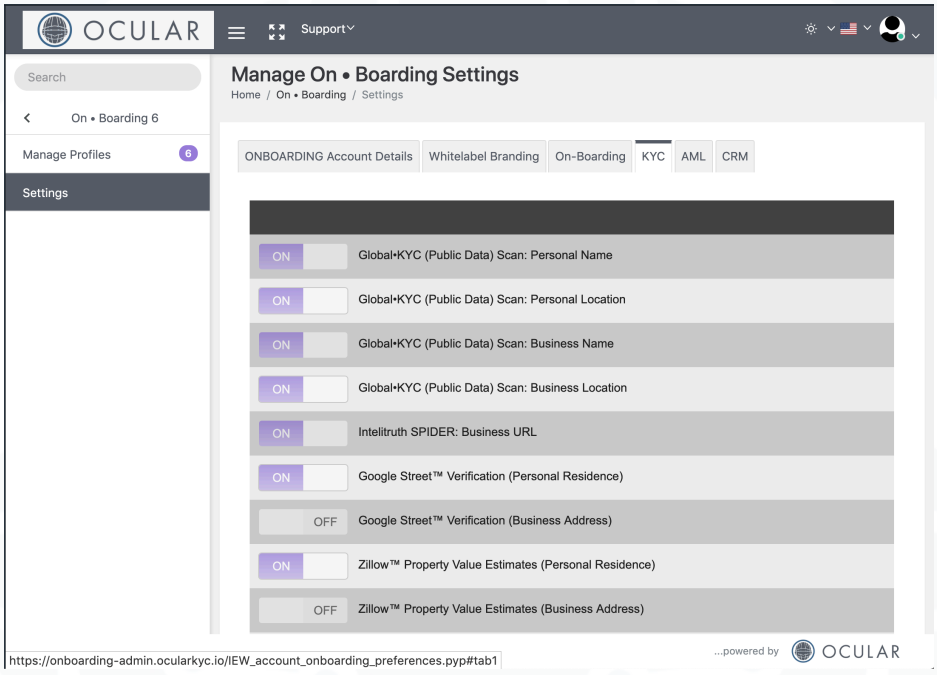
✓ Click "LOG IN"

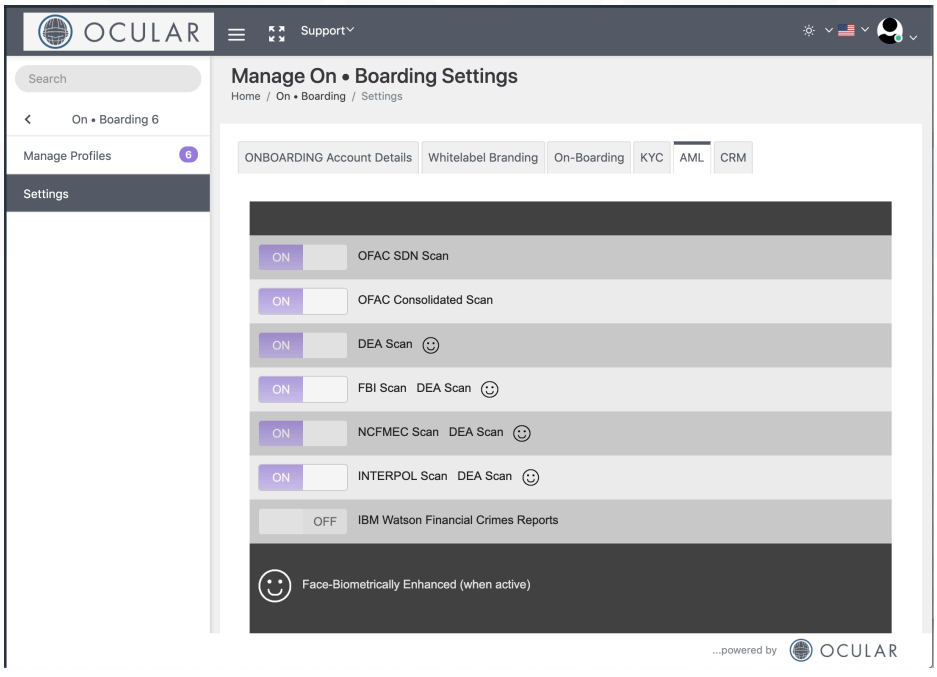
✓ Log into OculayKYC with your department credentials:



CONFIGURE YOUR KYC/AML OPTIONS & SCHEDULES

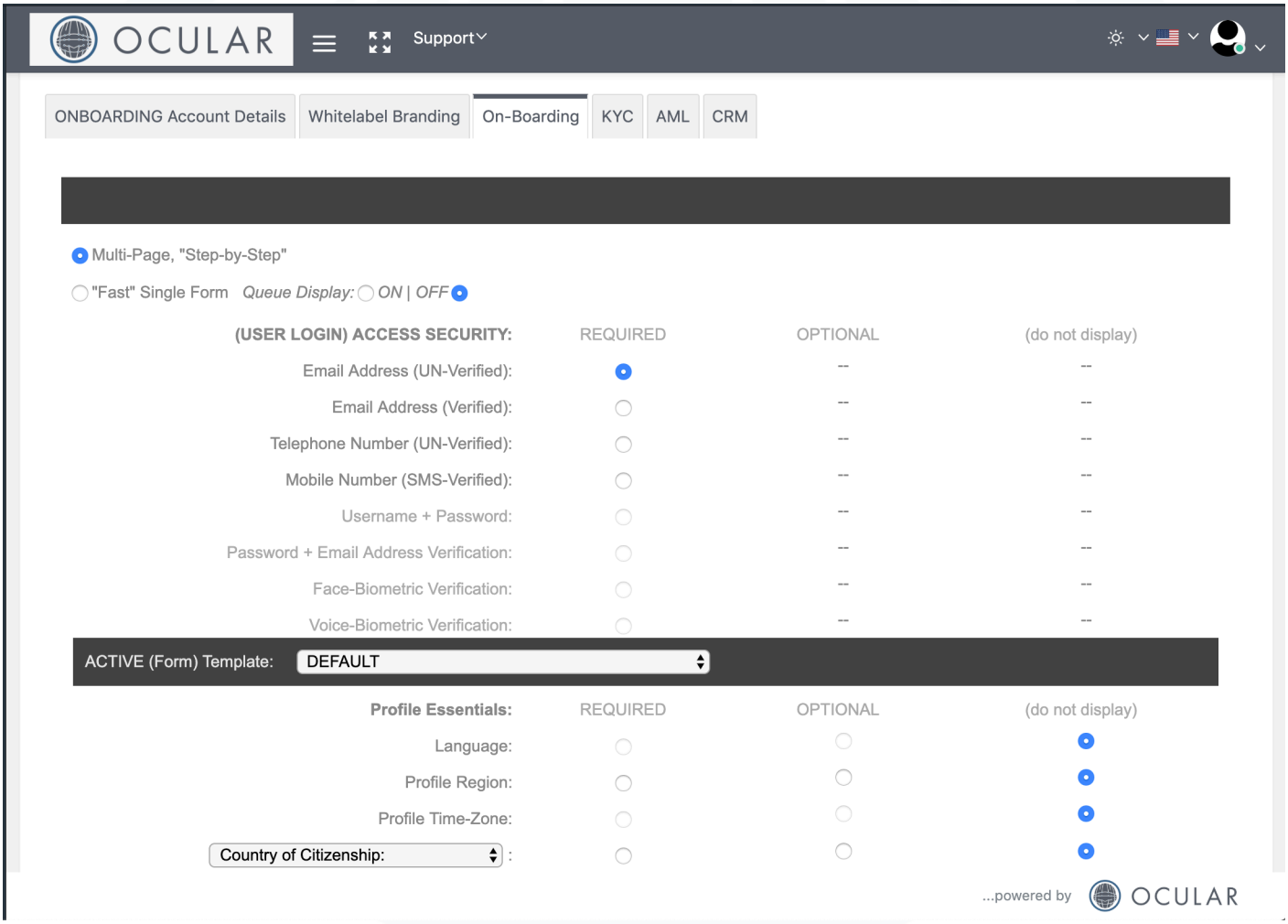
- ✓ Select "On•Boarding" from the Dashboard Nav Bar; THEN
- ✓ Select "Settings"rom the Dashboard Nav Bar; THEN
- ✓ Select KYC (tab) and/or AML (tab); THEN
- ✓ Set your default options (and schedules):





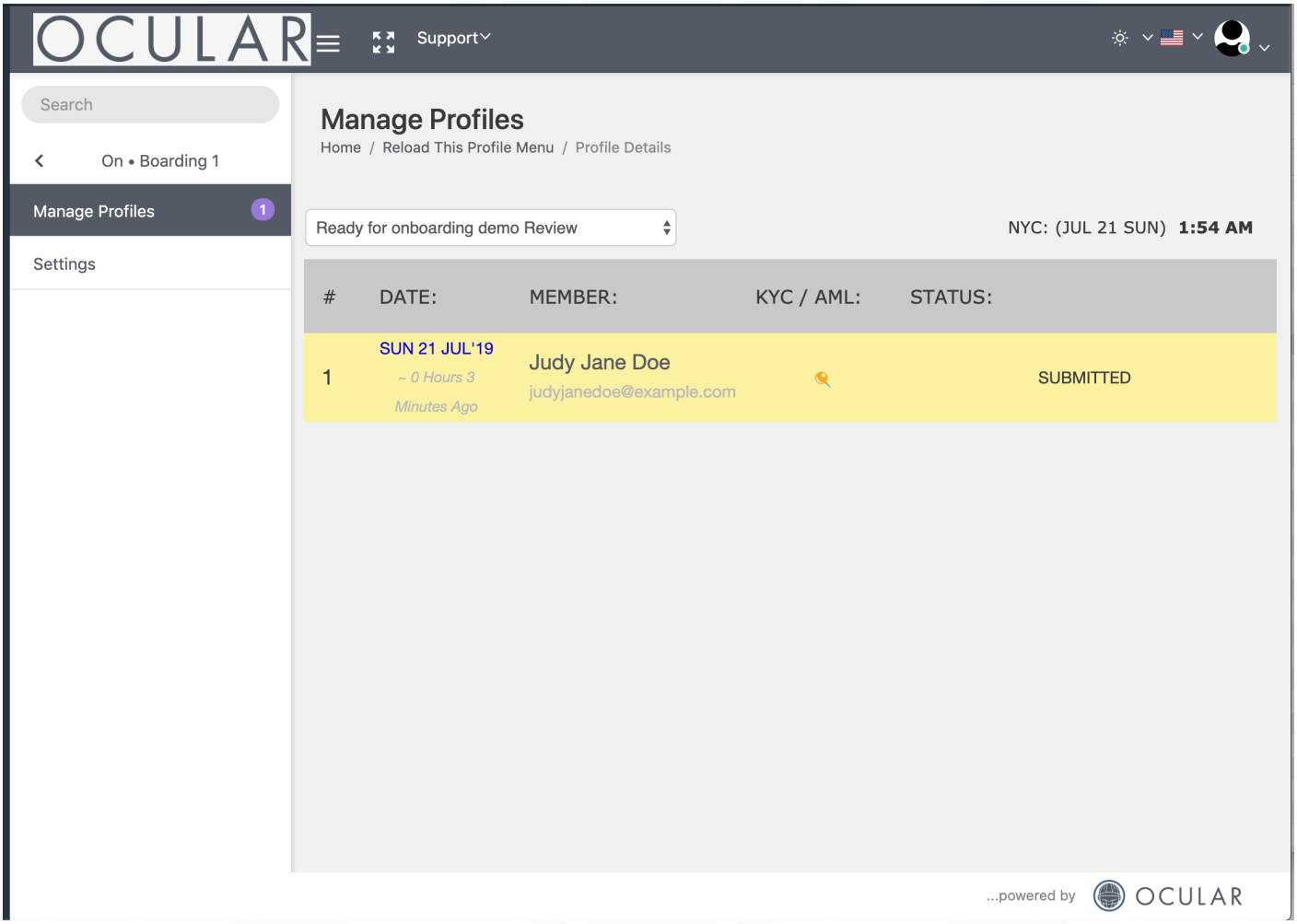
ON•BOARD PROFILE DOCUMENTS VIA OCULAR•KYC WEB/MOBILE

- ✓ Collect new profile documents by selecting "On•Boarding" from the Dashboard Nav Bar; THEN
- ✓ Select "Settings"; THEN
- ✓ Select On•Boarding (tab); THEN
- ✓ Configure your document collection options:

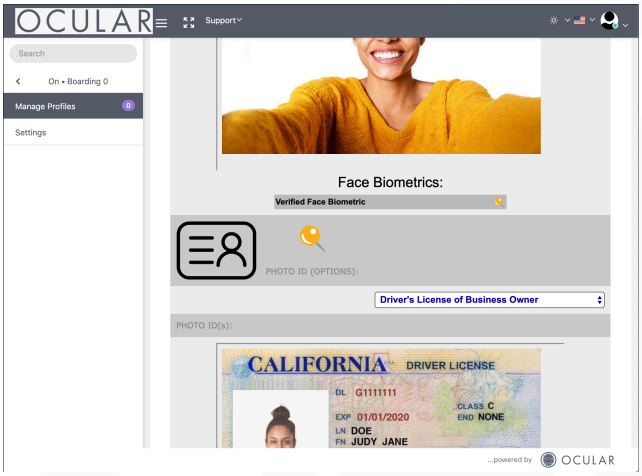


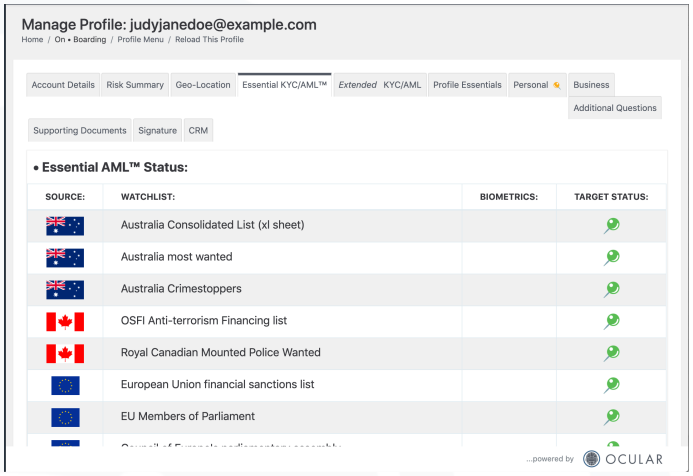
VIEW & MANAGE ON•BOARDED PROFILES

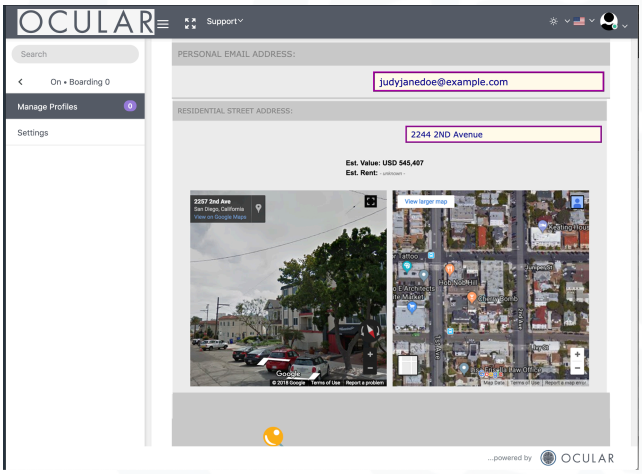
- ✓ To view and manage profiles that have been on•boarded via Omni-Channel or API, select "On•Boarding" from the Dashboard Nav Bar; THEN
- ✓ Select "Manage Profiles"; THEN
- ✓ Select the profile you want to view / manage:

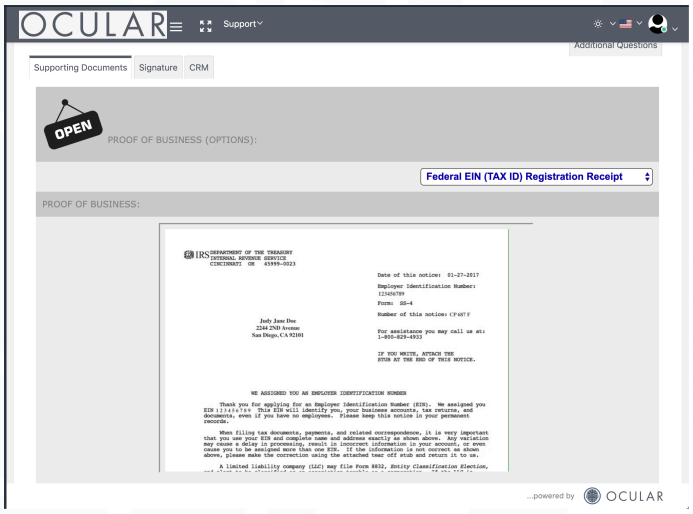


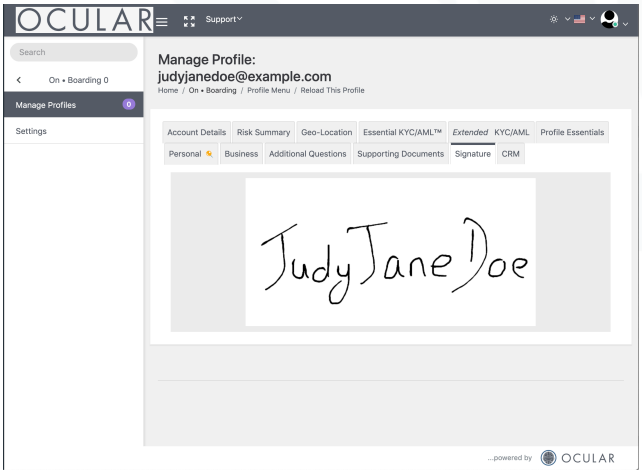
- ✓ Then finally select a profile tab (Risk Summary, KYC/AML, Personal, Supporting Documents, etc.) to review and manage the on•boarded profile.
  - NOTE: KYC/AML diligence will be automatically conducted in accordance with your KYC/AML configuration schedule.

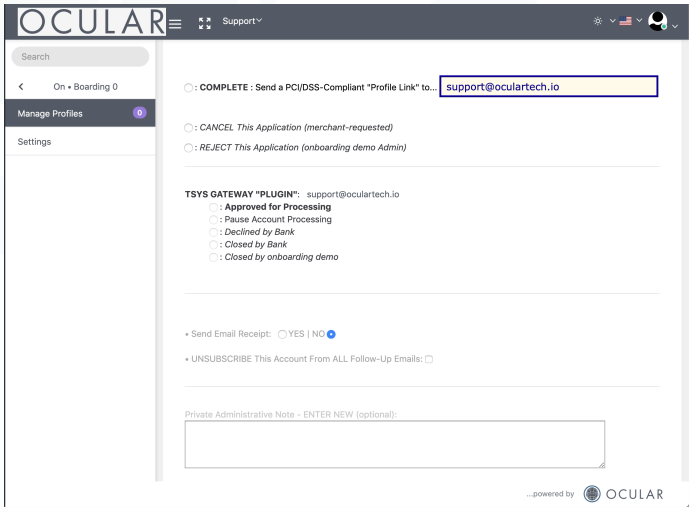






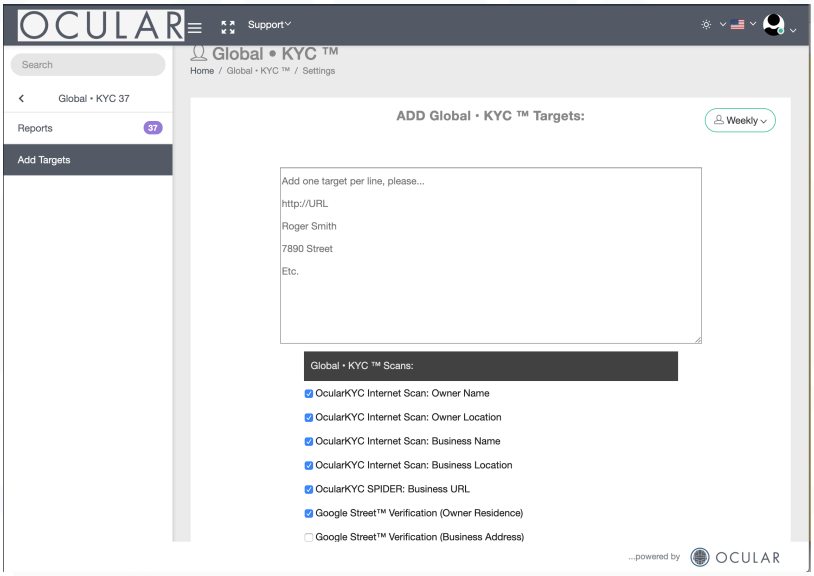




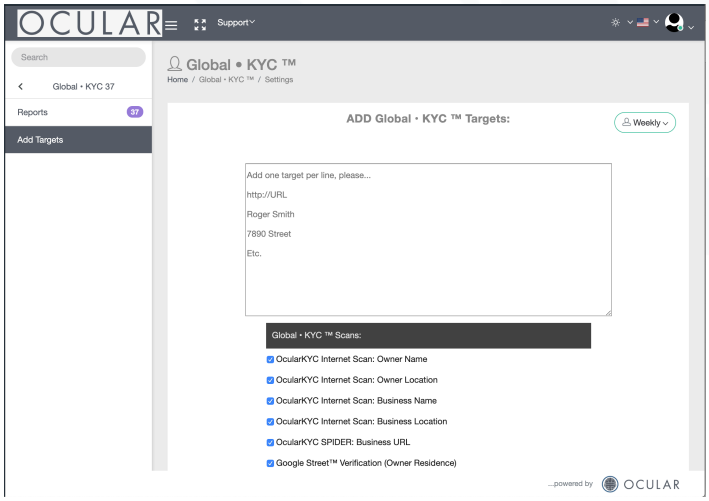


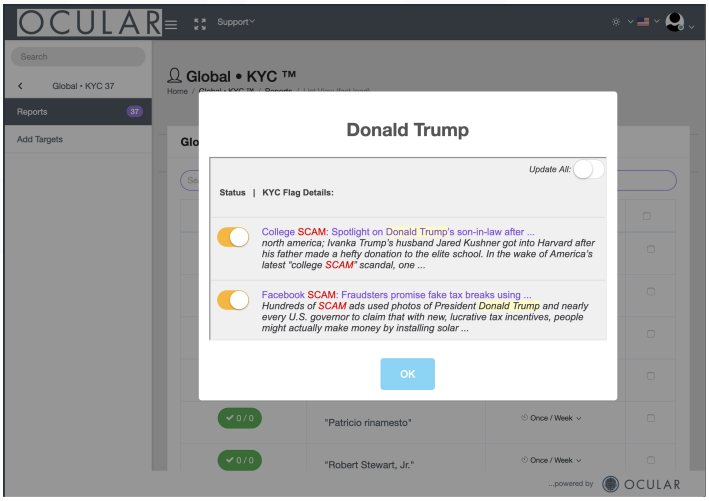
MANAGING INDIVIDUAL DETAILS: "KYC FLAGS"

- ✓ To manually run KYC-diligence against a single name or entity (i.e., w/o on•boarding a full profile), select "Global•KYC" from the Dashboard Nav Bar; THEN
- ✓ Select "Settings"; THEN
- ✓ Enter the "target" name(s) or entity(s) to KYC-monitor:



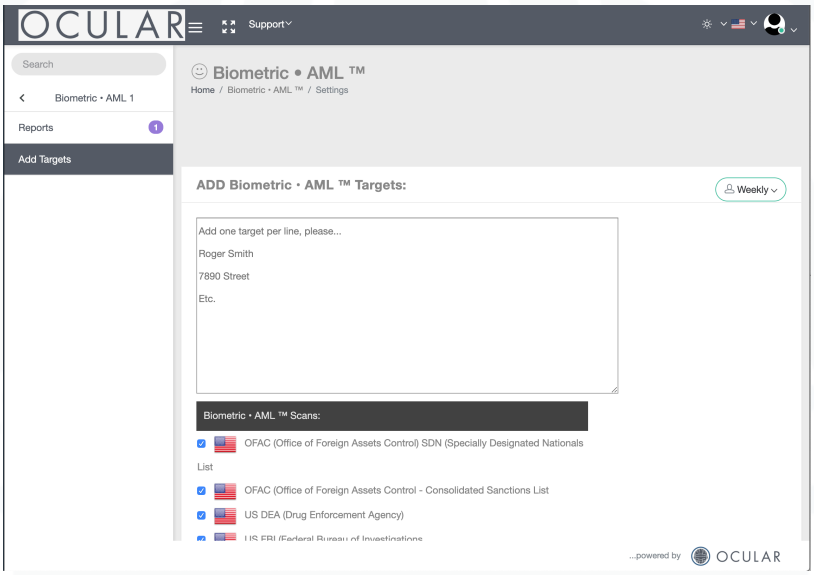
- ✓ To view the KYC-diligence results, select "Global•KYC" from the Dashboard Nav Bar; THEN
- ✓ Select "Reports"; THEN
- ✓ Click on a specific report for KYC-diligence details:



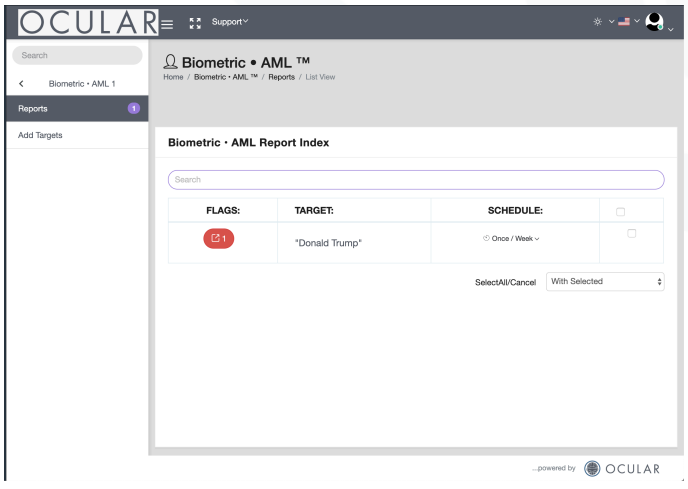


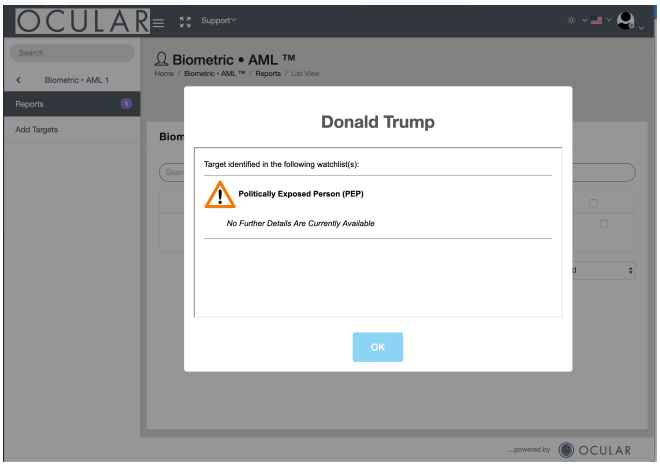
MANAGING INDIVIDUAL DETAILS: "AML FLAGS"

- ✓ To manually run AML-diligence against a single name or entity (i.e., w/o on•boarding a full profile), select "Biometric•AML" from the Dashboard Nav Bar; THEN
- ✓ Select "Settings"; THEN
- ✓ Enter the "target" name(s) or entity(s) to AML-monitor:



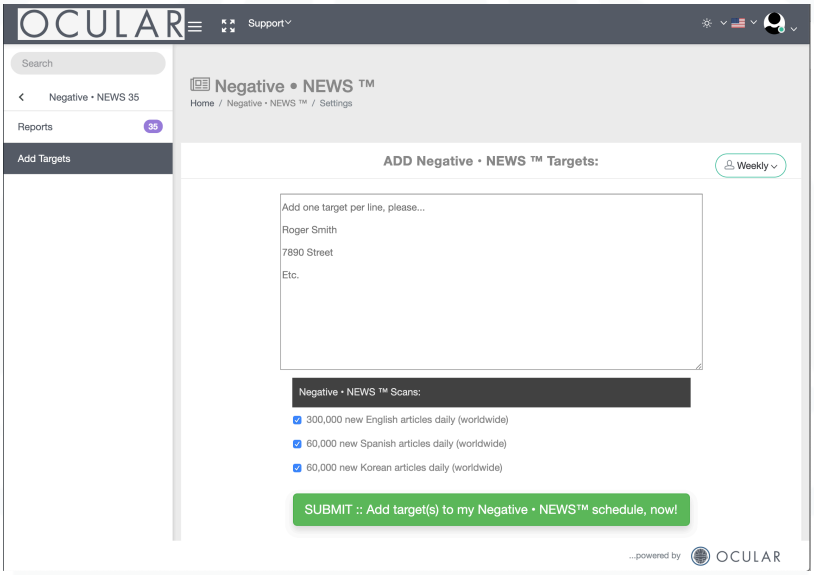
- ✓ To view the KYC-diligence results, select "Biometric•AML" from the Dashboard Nav Bar; THEN
- ✓ Select "Reports"; THEN
- ✓ Click on a specific report for AML-diligence details:





MANAGING INDIVIDUAL DETAILS: "NEGATIVE•NEWS FLAGS"

- ✓ To manually run Negative•News-diligence against a single name or entity (i.e., w/o on•boarding a full profile), select "Negative•News" from the Dashboard Nav Bar; THEN
- ✓ Select "Settings"; THEN
- ✓ Enter the "target" name(s) or entity(s) to Negative•News-monitor:



- ✓ To view the Negative•News-diligence results, select "Negative•News" from the Dashboard Nav Bar; THEN
- ✓ Select "Reports"; THEN
- ✓ Click on a specific report for Negative•News-diligence details: