MARCH 2024

COMPASS

With a track record of serving over 600 firms, including Fortune 10 companies and the largest Fintech unicorns, we provide impactful solutions to address complex regulatory, licensing, and compliance challenges faced by Fintech and financial services companies globally.

CHARTWELL IS NOW ANKURA

By Daniel Lee

Golden State Guidelines – A Deep Dive into California's New Virtual Currency Regulatory Framework

Introduction

California Governor Gavin Newsom signed two bills (Assembly Bill 39 and Senate Bill 401) into law on October 13, 2023[1], that will create an imposing regulatory framework for virtual currency regulation that will rival New York's "BitLicense" regulatory framework. California is the third state to introduce a licensing regime for virtual currency activity, after New York and Louisiana.

> "Governor Gavin Newson signed two bills into law on October 13, 2023."

The first bill, the California Digital Financial Assets Law (DFAL) is a new virtual currency licensing and regulatory framework which requires entities conducting virtual currency business activity to obtain a license similar to New York's "BitLicense" and to comply with a slew of regulatory requirements such as establishing and maintaining compliance programs for AML, information security, fraud, consumer compliance, and more. The second bill, Senate Bill 401, is related to the DFAL and specifically regulates digital financial asset transaction kiosks (e.g. Bitcoin ATMs).

Exemptions

The DFAL exempts several categories of persons including, but not limited to:

- Banks, credit unions and trust companies
- Payment processors providing processing, clearing, or settlement services solely for transactions between or among persons that are exempt from licensing requirements
- A person whose digital financial asset business activity with, or on behalf of, residents is reasonably

expected to be valued, in the aggregate, on an annual basis at fifty thousand dollars ($50,000) or less

- A person registered as a securities broker-dealer under federal or state securities laws to the extent of its operation as a broker-dealer
- A merchant that accepts a digital financial asset as payment for the purchase or sale of goods or services, which does not include digital financial assets[2]

Requirements

Licensing

On or before July 1, 2025, any person engaging in digital financial asset business activity must be licensed, have submitted a license application and are awaiting approval or denial of that application, or otherwise be exempt from licensure.[1]

The DFAL states that license applications will require among other things:

- A description of the current and former business of the applicant for the five years before the application is submitted, or, if the business has operated for less than five years, for the time the business has operated, including its products and services, associated internet website addresses and social media pages, principal place of business, projected user base, and specific marketing targets
- The source of funds and credit to be used by the applicant to conduct digital financial asset business activity with, or on behalf of, a resident
- Documentation demonstrating that the applicant has sufficient capital and which must include, but is not limited to, both of the following:
  - A copy of the applicant's audited financial statements for the most recent fiscal year and for the two-year period t preceding the submission of the application, if available
  - A copy of the applicant's unconsolidated financial statements for the current fiscal year, whether audited or not, and, if available, for the two-year period preceding the submission of the application
- A copy of the certificate, or a detailed summary acceptable to the department, of coverage for any liability, casualty, business interruption, or cybersecurity insurance policy maintained by the applicant for itself, an executive officer, a responsible individual, or the applicant's users
- The plans through which the applicant will meet its obligations regarding compliance program, policies and procedures required by the DFAL[2]

Compliance Programs

The DFAL also imposes strict requirements for digital financial asset businesses to adopt and maintain compliance programs for all of the following:

- An information security program and an operational security program
- A business continuity program
- A disaster recovery program
- An anti-fraud program
- A program to prevent money laundering
- A program to prevent funding of terrorist activity
- A program designed to ensure compliance with the DFPI, other California or federal laws applicable to the digital financial asset business activity and to assist the licensee in achieving the purposes of other state laws and federal laws if violation of those laws has a remedy under this division. Such a program must specify detailed policies and procedures that the licensee undertakes to minimize the probability that

the licensee facilitates the exchange of unregistered securities [2]

Stablecoins

Additional requirements regarding stablecoins require that licensees only store a digital financial asset or engage in digital financial asset administration, whether directly or through an agreement with a digital financial asset control services vendor, if both of the following are true:

- The issuer of the stablecoin is an applicant, is licensed with the California Department of Financial Protection (DFPI), or is a bank, a trust company, or a national association authorized under federal law to engage in a trust banking business
- The issuer of the stablecoin at all times owns eligible securities having an aggregate market value computed in accordance with United States generally accepted accounting principles of not less than the aggregate amount of all of its outstanding stablecoins issued or sold[2]

In determining whether to make an approval for the issuance of a stablecoin, the DFPI will consider factors such as:

- Any legally enforceable rights provided by the issuer of the stablecoin to holders of the stablecoin, including, but not limited to, rights to redeem the stablecoin for legal tender or bank or credit union credit
- The amount, nature, and quality of assets owned or held by the issuer of the stablecoin that may be used to fund any redemption requests from residents

- Any risks related to how the assets are owned or held by the issuer that may impair the ability of the issuer of the stablecoin to meet any redemption requests from California residents
- Any representations made by the issuer of the stablecoin related to the potential uses of the stablecoin
- Any representations made by the issuer of the stablecoin related to the risks of using the stablecoin as payment for goods or services or as a store of value [2]

Coin Listing

Similar to the NYDFS's coin listing requirements, licensed exchanges under the DFAL, prior to listing or offering a digital financial asset, must certify on a form provided by the DFPI that the covered exchange has done the following:

- Identified the likelihood that the digital financial asset would be deemed a security by federal or California regulators
- Provided, in writing, full and fair disclosure of all material facts relating to conflicts of interest that are associated with the covered exchange and the digital financial asset
- Conducted a comprehensive risk assessment designed to ensure consumers are adequately protected from cybersecurity risks, risk of malfeasance, including theft, risks related to code or protocol defects, or market-related risks, including price manipulation, and fraud
- Established policies and procedures to reevaluate the appropriateness of the continued listing or offering of the digital financial asset, including an evaluation of whether material changes have occurred
- Established policies and procedures to cease listing or offering the digital financial asset, including notification to affected consumers and counterparties [2]

Reporting

The DFAL also includes several financial reporting requirements for digital financial asset businesses.

Licensees are required to maintain, for all digital financial asset business activity with, or on behalf of, a California resident for five years after the date of the activity, records such as:

- All transactions with, or on behalf of a California resident or for the licensee's account in California
- The aggregate number of transactions and aggregate value of transactions for the previous 12 calendar months
- Any transaction in which the licensee exchanged one form of digital financial asset for legal tender or another form of digital financial asset with, or on behalf of a California resident
- A general ledger maintained at least monthly that lists all assets, liabilities, capital, income, and expenses of the licensee
- Any business call report the licensee is required to create or provide to the DFPI
- Bank statements and bank reconciliation records for the licensee and the name, account number, and United States Postal Service mailing address of any bank the licensee uses in the conduct of its digital financial asset business activity with, or on behalf of a California resident
- A report of any dispute with a California resident [2]

Consumer Protections and Disclosures

The DFAL also includes multiple consumer protection and disclosure requirements for digital financial asset businesses.

As part of its consumer protection responsibilities, covered exchanges must ensure they are using reasonable diligence to ensure that the outcome to a California resident is as favorable as possible under prevailing market conditions, with compliance determined by factors such as:

- The character of the market for the digital financial asset, including price and volatility
- The size and type of transaction
- The number of markets checked.
- Accessibility of appropriate pricing.

> "Covered exchanges must review aggregated trading records of California residents."

Covered exchanges must, at least once every six months, review aggregated trading records of California residents against benchmarks to determine execution quality, shall investigate the causes of any variance, and shall promptly take action to remedy issues identified in that review. If a covered exchange cannot execute directly with a market and employs other means in order to ensure an execution advantageous to a California resident, the burden of showing the acceptable circumstances for doing so is on the covered exchange. [2]

Licensed entities in California must also ensure that they provide a number of consumer protection related disclosures. Examples of some of the disclosures required by the DFAL are:

- A schedule of fees and charges the covered person may assess, the manner by which fees and charges will be calculated if they are not set in advance and disclosed, and the timing of the fees and charges.
- Whether a covered entity's product or service is covered by either of the following:

- A form of insurance or other guarantee against loss by an agency of the United States as follows:
    - Up to the full United States dollar equivalent of digital financial assets placed under the control of, or purchased from, the covered person as of the date of the placement or purchase, including the maximum amount provided by insurance under the Federal Deposit Insurance Corporation, National Credit Union Share Insurance Fund, or

otherwise available from the Securities Investor Protection Corporation.

- If not provided at the full United States dollar equivalent of the digital financial asset placed under the control of or purchased from the covered person, the maximum amount of coverage for each California resident expressed in the United States dollar equivalent of the digital financial asset.

- Private insurance against theft or loss, including cybertheft or theft by other means. Upon request of a resident with whom a covered person engages in digital financial asset business activity, a covered person shall disclose the terms of the insurance policy to the resident in a manner that allows the resident to understand the specific insured risks that may result in partial coverage of the resident's assets.

- The irrevocability of a transfer or exchange and any exception to irrevocability.

- A description of all of the following:

  - The covered person's liability for an unauthorized, mistaken, or accidental transfer or exchange.

  - A California resident's responsibility to provide notice to the covered person of an unauthorized, mistaken, or accidental transfer or exchange

  - The basis for any recovery by a California resident from the covered person in case of an unauthorized, mistaken, or accidental transfer or exchange

  - General error resolution rights are applicable to an unauthorized, mistaken, or accidental transfer or exchange

  - The method for a California resident is to update the resident's contact information with the covered person

- The date or time when the transfer or exchange is made and the resident's account is debited may differ from the date or time when the resident initiates the instruction to make the transfer or exchange

- Whether the resident has a right to stop a preauthorized payment or revoke authorization for a transfer and the procedure to initiate a stop-payment order or revoke authorization for a subsequent transfer.

- The resident's right to receive a receipt, trade ticket, or other evidence of the transfer or exchange.

- The resident's right to at least 14 days prior notice of a change in the covered person's fee schedule, other terms and conditions that have a material impact on digital financial asset business activity with the resident, or the policies applicable to the resident's account.

- A list of instances in the past 12 months when the covered person's service was unavailable to 10,000 or more customers seeking to engage in digital financial asset business activity due to a service outage on the part of the covered person and the causes of each identified service outage.

- The conclusion of a digital financial asset transaction must provide a California resident with a confirmation in a record which contains all of the following:

  - The name and contact information of the covered person, including the toll-free telephone number required by the DFAL

  - The type, value, date, precise time, and amount of the transaction

  - The fee charged for the transaction, including any charge for conversion of a digital financial asset to legal tender, bank credit, or other digital financial asset, as well as any indirect charges[2]

Digital Financial Asset Transaction Kiosks

The second bill signed includes provisions for digital financial asset transaction kiosks, which are defined as electronic information processing devices that are capable of accepting or dispensing cash in exchange for a digital financial asset.

Daily limits of one thousand dollars ($1,000) for accepting or dispensing cash will be required as well as limits on the amount of fees that can be charged. Fees must be limited to the greater of the following, five dollars ($5), or fifteen percent of the United States dollar equivalent of digital financial assets involved in the transaction according. The bill also includes customer disclosure requirements and regulatory reporting requirements.[3]

Penalties

The DFPI can assess a civil penalty of up to $20,000 per day to licensees or covered persons who materially violate the DFAL. Additionally, unlicensed entities engaging in digital financial business activity can be charged a civil penalty of up to $100,000 per day.[2] These civil monetary penalties are significantly higher than those in most states.

Ramifications

This new development in virtual currency regulation will create sweeping new requirements for virtual currency businesses in the state of California. The good news is that many of the requirements such as the establishment and maintenance of an AML Program and InfoSec Program are compliance requirements that many virtual currency companies already have in place. However, new requirements such as financial reporting, the assessment of whether a digital financial asset would be deemed a security by federal or California regulators, comprehensive risk assessment of cybersecurity, malfeasance, or market related risks, and the myriad consumer protection disclosures needed to be provided to customers, will require many companies to implement significant new policies, pr cedures and processes to ensure compliance. Additionally, the DFAL prohibits a covered person from engaging in digital financial business activity with an issuer of a stablecoin, if it is not a bank, trust company, or national association authorized under federal law to engage in a trust banking business or is licensed under the DFAL, which could potentially restrict the nu ber of stablecoin issuers a licensed entity could work with once the DFAL comes into effect.

Conclusion

For any digital financial asset service providers that want to get a head-start on beginning their digital financial asset license applications and building their compliance programs for the state of California, Ankura's team of licensing, maintenance and compliance professionals has extensive experience in assisting companies with licensing and regulatory compliance for all U.S. states and territories, including New York and California. Ankura has successfully assisted numerous cryptocurrency startups obtain licenses in the state of New York whose "BitLicense" licensing and regulatory framework bears many similarities to the one proposed by California's DFAL.

The DFAL provides the California Department of Financial Protection and Innovation (DFPI) with rule making authority and an operative date of July 1, 2025. The DFPI will be charged with creating the regulatory framework to balance the needs of consumer protection with the needs of the crypto asset industry. This gives the industry some time to interpret the statute and any subsequent regulations that are written to ensure that they have implemented the required provisions of the DFAL in a timely manner.

SOURCE

[1] *Digital Financial Assets Law.* Official website of the State of California. dfpi.ca.gov/dfal/#:~:text=Beginning%20July%201%2C%202025%2C%20companies,a%20license%20from%20the%20DF

[2] *AB-39 Digital financial asset businesses: regulatory oversight.* California Legislative Information. leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=20

[3] *SB-401 Digital financial asset transaction kiosks.* California Legislative Information. leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB401

FOR MORE INFORMATION CONTACT

Daniel Lee
Director at Ankura
dan.lee@ankura.com

Daniel Lee, Director at Ankura, has over 15 years of regulatory compliance and consulting experience in the Banking and Money Service Business industry.

As a former examiner and Fintech subject matter expert at the Colorado Division of Banking, Daniel led examinations of Fintechs and virtual currency companies for compliance with state and federal regulations and has assisted mid to large size financial institutions with their model validation, model tuning, and model risk governance activities.

By Jake Hines

International Day of Family Remittances – A Global Push for Financial Inclusion and Resilience

Each year, June 16 is globally recognized as International Day of Family Remittances (IDFR), as established by the United Nations. The core goal of IDFR is to recognize the transformative impact of remittances, specifically those from over 200 million migrants (half of them women) to their 800 million family members worldwide. An estimated half of these annual flows end up in rural areas where remittances are vital to aiding those afflicted by poverty and hunger. IDFR also promotes the UN's Sustainable Development Goals (SDGs), specifically SDG 10, which includes the goal of lowering the costs of migrant remittances to below 3% by 2030 as part of an overall effort to reduce inequality within and among countries. Each of the 17 SDGs established is part of a global plan that aims to sustainably protect the environment and improve human lives worldwide.[1]

The IDFR theme for 2023-2024, "digital remittances towards financial inclusion and cost reduction", focused on digital remittances, their impact on reducing costs, and how they're enabling more inclusion amongst senders and recipients of the most vulnerable groups. According to World Bank, 2022 remittances to low- or middle-income countries (LMICs) grew to $626 billion, an estimated 5% increase from 2021. As of recent data, although mobile remittances were the cheapest way to send remittances of $200 to LMICs, costing only approximately 3.73% as compared to the much higher average of 6.3%, digital transfers continue to

make up only a small percentage of the total of all global flows.[34]

The difference between these cost percentages is extremely significant in practical terms for the communities most in need. According to the UN, 75% of remittances to LMICs pay for immediate needs such as food, housing, healthcare, or sanitation. Every cent matters when remittances are going directly to the bare necessities needed to survive, and digital developments in the remittance industry are helping to significantly lower the cost. The hope of these lower costs is to build greater long-term financial resilience for vulnerable populations who rely on remittances for a significant portion of their needs.

With the cooperation of international participants, both public and private, the push to better the lives of those relying on remittances and to promote financial inclusion through technological advancement is picking up steam. Please visit the website for the International Fund for Agricultural Development, an agency of the UN focused on addressing hunger and poverty in rural areas of developing countries, for further information at familyremittances.org. Housed here are several resources, ranging from brochures to links to study results, that can be used by remittance providers to understand their place in fostering the financial inclusion of migrants and creating innovations that allow for remittances that are faster, safer, and cheaper.

Consider participating in IDFR this June to help improve lives worldwide.

> "Every cent matters when remittances go to basic needs. Digital innovation offers significant cost reduction, building long-term financial resilience for vulnerable populations."

SOURCES

[1] sdgs.un.org/goals
[2] worldbank.org/en/news/press-release/2022/11/30/remittances-grow-5-percent-2022
[3] familyremittances.org/idfr-2023-24
[4] gsma.com/mobilefordevelopment/mobile-money
[5] documents-dds-ny.un.org/doc/UNDOC/GEN/N18/182/46/PDF/N1818246.pdf?OpenElement

FOR MORE INFORMATION CONTACT

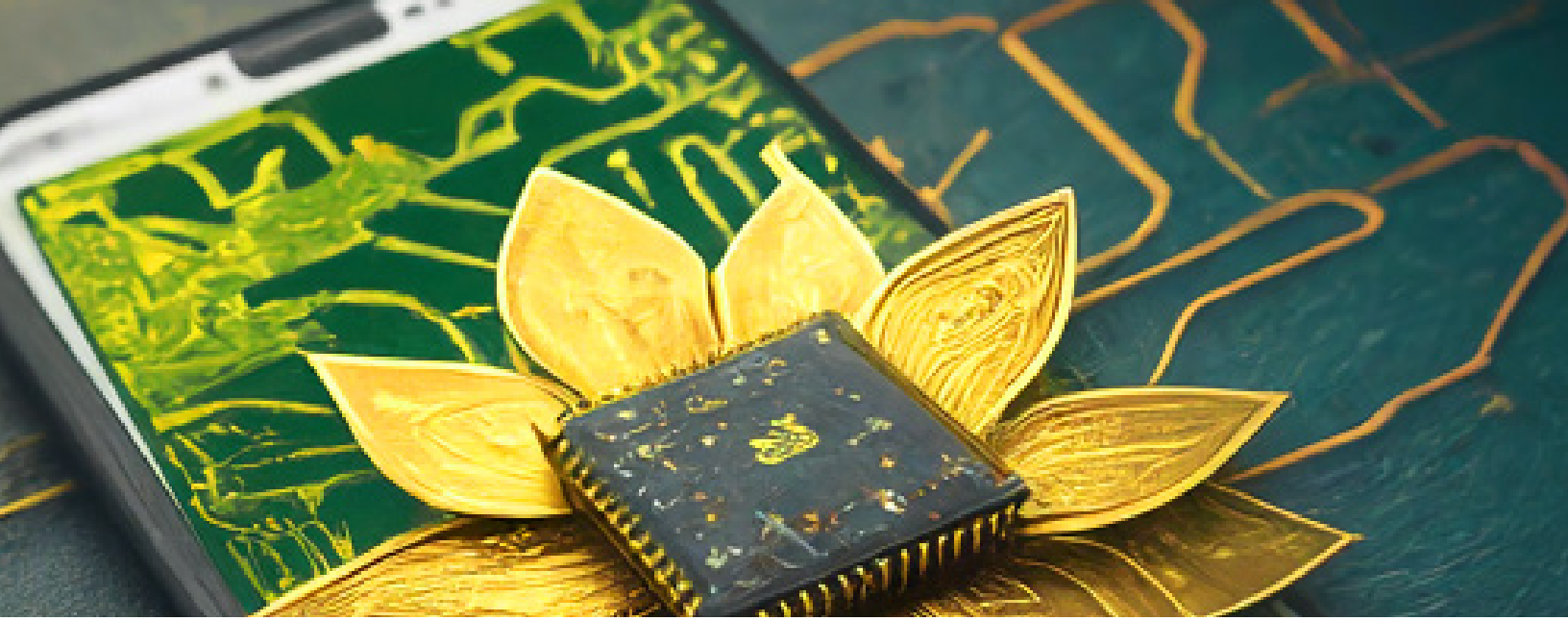
Jacob (Jake) Hines

Director at Ankura

jake.hines@ankura.com

Jacob (Jake) Hines, Director at Ankura, brings years of experience in state money transmitter acquisition, statutory license maintenance, and regulatory as well as consumer compliance.

Prior to joining Ankura, Jacob worked at a rapidly growing cryptocurrency firm, Voyager Digital, where he assisted in licensing acquisition, refining policies and procedures for compliance with applicable regulations, as well as with aiding in various other regulatory compliance functions.



By Patricia Lewis

No, We're Not Just Blowing Smoke. You CAN **Bank Marijuana-Related Businesses**

Since California first passed legislation legalizing medical marijuana in 1996, the legal landscape involving medicinal and recreational marijuana has grown significantly. According to the American Bankers Association, "thirty-seven states, the District of Columbia, Guam, and Puerto Rico" have all enacted some sort of marijuana legalization regulation as of the end of 2023 [i]. However, despite this, the federal government still classifies the sale or distribution of marijuana as illegal, making it very difficult for financial institutions to provide services to entities engaging in legal (at the state level) marijuana operations.

Those engaged in marijuana operations are not just those with direct connections to the industry (such as growers and retailers) but includes those with indirect connections, such as employees of dispensaries, the landlords of the brick and mortar operations, and vendors providing supplies to the companies (among others). Because marijuana is still considered illegal at the federal level, financial institutions are often hesitant to accept customers with direct or indirect connections to the industry. This causes many marijuana related businesses (MRBs) to rely heavily on cash, as Fintech (financial technology) companies that provide payment services such as credit/debit card processing and digital payment options are often backed by financial institutions supervised by a federal banking regulator. Any business, but especially MRBs, operating on an all-cash basis are very attractive to criminals and money launderers and susceptible to theft, tax evasion, and organized crime. In addition, the use of cash makes it very difficult to track incoming and outgoing funds in these businesses as those transactions fall outside of the traditional financial system.

The Senate Banking Committee passed the Secure and Fair Enforcement Regulation Banking Act (SAFER Banking Act) in September 2023, but it did not make it to the Senate floor, was delayed, and was not passed by the conclusion of the legislative session. However, the Democratic led Senate has indicated that passing marijuana banking reform will be a top priority in 2024. If the SAFER Banking Act were to pass in 2024, this would assist in the effort to curb some of these

issues and make it easier for financial institutions to provide services to MRBs. The bill prevents a federal banking regulator from penalizing a depository institution for banking such entities, as well as prohibits them from requesting that they terminate the relationship without specific parameters (such as if the institution is "engaging in an unsafe or unsound practice or is violating a law or regulation"). Most importantly, the regulation declares that proceeds from transactions involving MRBs are no longer considered "proceeds from unlawful activity"[II]. The SAFER Banking Act is setting a path to allow more financial institutions and Fintech companies to open the door to MRBs and onboard them without the threat of repercussions from federal regulators.

> "Without banking access, MRBs fuel the shadow economy. The SAFER Banking Act offers a solution for a safer future."

If 2024 is the year that the SAFER Banking Act is passed, it would behoove financial institutions and Fintech to be proactive and update their compliance programs to onboard MRBs so that when the bill is passed, they are ready to operate in this space with the proper controls in place to do so compliantly. With that being said, in order to begin this process, there are many aspects a financial institution or Fintech must consider and actions that will need to be taken to ensure the appropriate level of compliance.

These include:

- **Establishing and conducting enhanced diligence on the MRB.** Make sure that all beneficial owners are known, identified, and verified. Review all licenses and paperwork submitted to the state for red flags or items that may have been overlooked.
- **Including adverse media research into the enhanced due diligence (for owners AND employees).** MRBs are a controversial industry in many states, with strong arguments on both sides of legalization. The reputation of these businesses must stay above reproach, so any negative news or criminal history related to those involved in the business, as well as the business itself, should be thoroughly investigated and documented.
- **Enacting an effective transaction monitoring program.** MRBs will still likely continue to be a cash intensive business, and as referenced above, still very attractive to those with criminal intentions (as with any cash-based business). Financial institutions should be prepared to thoroughly examine all transactions related to the business and identify any red flags and implement rules and alerts to specifically identify activity related to MRBs. Be sure to look for larger than normal revenues (in cash or other forms of payment), especially if they have grown significantly since joining the financial institution.
- **Making sure that proper controls are in place within the company.** Is the MRB also taking steps to ensure compliance with AML regulations as a customer of the financial institution? Do they share the bank's commitment to compliance? Are they able to provide and maintain adequate policies and procedures?
- **And most importantly: Preparing to vehemently defend your decision to provide services to an MRB.** Even with the provisions provided under the SAFER Banking Act, at the end of the day,

marijuana will still be illegal on the federal level. Financial institutions providing services to MRBs are often federally insured. If they want to continue to receive that insurance, and provide financial services to an MRB, they must be able to effectively justify their decision to bank an MRB. This includes the actions they are taking to ensure this business is not engaged in illegal activities, is adopting and actively engaging in a compliance program, and adhering to any stipulations outlined in their agreement with the financial institution.

The actions detailed above are not all-inclusive. It is vital that any financial institution or Fintech considering engaging with an MRB take the decision very seriously to avoid significant consequences. However, it can be done, as the SAFER Banking Act states that "all depository institutions should take a risk-based approach in assessing individual customer relationships rather than decline to provide banking services to categories of customers without regard to the risks presented by an individual customer or the ability of the depository institution to manage the risk"[III]. This provides hope for the future for the financial industry, as well as MRBs in general, as companies (including MRBs) that "prioritize AML compliance demonstrate their commitment to ethical and responsible business practices, which can enhance their reputation and credibility in the marketplace".[IV] This will be essential in paving the future of relationships between financial institutions and MRBs. MRBs, like any business, need access to financial systems to help pay employees, taxes, access loans, and process electronic payments.

> "The SAFER Banking Act is setting a path to allow more financial institutions and FinTech companies to open the door to MRBs and onboard them without the threat of repercussions from federal regulators."

Without access to these opportunities, MRBs' exponential growth will continue to be outside of the financial system which will only increase its potential use for illicit activities, illicit actors, and organizations that benefit from this industry operating outside of the financial system. Financial institutions have the chance to make a difference in this evolving industry in preparation for a future that is not far off.

It's time that those in the financial industry take a hard look at what the future holds and consider this rising field of banking MRBs. If you find that you're ready to take the leap, let Ankura help you. We have many experts that can help guide you down the right path and get you prepared for this exciting journey.

SOURCES

[1] Cannabis Banking: Bridging the Gap between State and Federal Law. (2023). Retrieved January 23, 2024, from American Bankers Association: aba.com/advocacy/our-issues/cannabis

[2] H.R.2891 - SAFE Banking Act of 2023. (2023, April 26). Retrieved January 31, 2024, from Congress.Gov: congress.gov/bill/118th-congress/house-bill/2891#:~:text=This%20bill%20provides%20protections%20for,a%20Schedule%20I%20controlled%20substance

[3] Merkley, M. (2023). S. 2860 Introduced in Senate. U.S. Government Publishing Office. Retrieved January 20, 2024, from govinfo.gov/content/pkg/BILLS-118s2860is/html/BILLS-118s2860is.htm

[4] AML Compliance for Legal Cannabis. (2023). Retrieved January 26, 2024, from Sanction Scanner: sanctionscanner.com/blog/aml-compliance-for-legal-cannabis-632

FOR MORE INFORMATION CONTACT

Patricia Lewis

Senior Associate at Ankura

✉ patricia.lewis@ankura.com

Patricia Lewis, Senior Associate at Ankura, has over 10 years of investigative and data analysis experience related to financial crimes.

Prior to joining Ankura, Patricia spent eight years working in the gaming industry in BSA/AML and auditing roles, as well as four years working with consultants AML RightSource LLC, where she focused on data analysis for cryptocurrency platforms, money service businesses, Fintech companies, and financial institutions. In addition, she also performed due diligence on high-risk client customers in these industries.

By Jake Hines

Owning Up: What You Need to Know About FinCEN's Ultimate Beneficial Ownership Reporting Rule

On September 30, 2022, FinCEN published the Ultimate Beneficial Ownership (UBO) Reporting Rule[1] (the Rule), which implements reporting requirements regarding Beneficial Ownership Information (BOI) under the Corporate Transparency Act (CTA). The Rule became effective on January 1, 2024, leaving covered entities only a few more months to ensure that they are prepared to comply with the new requirements.

As with any new requirements imposed by FinCEN, there are bound to be questions about who is covered, what companies need to do to comply, and why this level of granular detail on BOI is even necessary.

Why is The Rule Necessary?

Before getting into the specific requirements of the Rule itself, it's important to understand the goals behind its inclusion in the Anti-Money Laundering Act of 2020 (AMLA), what it hopes to fix, and how it can be of use in regulatory enforcement in the future.

The AMLA was enacted into law as part of the National Defense Authorization Act for Fiscal Year 2021 as a means to disrupt corruption and the use of U.S. financial systems to facilitate illicit activities that could present opportunities for individuals and entities which threaten U.S. national security to participate in the U.S. economy. As it stood prior to the Rule, the lack of standard requirements resulted in the quality and depth of BOI collected being inconsistent at best, leaving potentially dangerous blind spots.

According to the U.S. Department of the Treasury's National Strategy for Combating Terrorist and Other Illicit Financing[2] (the Strategy), published in 2022, "A lack of uniform requirements to report BOI at the time of entity formation (and changes in ownership) hinders the ability of (1) law enforcement to swiftly investigate those entities created and used to hide ownership for illicit purposes and (2) regulated sectors to mitigate risks." The first priority detailed in the Strategy is to increase transparency and close regulatory and legal

gaps in the U.S. framework for AML/CTF, thus making it more difficult for illicit actors to anonymously utilize U.S. financial systems to move funds and purchase U.S. assets. Collection of BOI is the first supporting action detailed, and if the Rule works as intended, will further restrict the ability of illicit actors to use front or shell companies to hide their identities, move illicit funds through U.S. financial systems, and launder money. The Rule's requirements, which are explained in more detail below, will give unprecedented insight into the BOI of both existing and newly registered entities.

2024 Benchmarks for Progress are also detailed in the Strategy. Among these are the desire to create "an operational beneficial ownership registry" and to "engage and work with foreign jurisdictions that have weak or non-existent BOI collection requirements to revise corporate secrecy laws and take other necessary steps to facilitate timely access to BOI information by law enforcement and regulatory authorities; strengthen and adequately resource investigatory programs; and significantly improve international cooperation relating to BOI."

> "The AMLA was enacted into law as part of the National Defense Authorization Act for Fiscal Year 2021 as a means to disrupt corruption and the use of U.S. financial systems to facilitate illicit activities that could present opportunities for individuals and entities which threaten U.S. national security to participate in the U.S. economy."

Who is Covered Under the Rule?

Covered entities, referred to in the Rule as Reporting Companies, are essentially any non-exempt company which registers to do business with a secretary of state, Indian Tribe, or other similar offices. They are delineated into two classifications: Domestic Reporting Companies and Foreign Reporting Companies, both of which have fairly broad definitions and coverage.

Domestic Reporting Companies include entities "created by the filing of a document with a secretary of state or a similar office under the law of a State or Indian Tribe." This means that a range of entity types are covered, e.g., corporations, limited liability companies (LLCs), limited partnerships (LPs), and business trusts.

Foreign Reporting Companies include entities "formed under the law of a foreign country and registered to do business in the United States by the filing of a document with a secretary of state or a similar office under the laws of a State or Indian Tribe."

FinCEN carves out 23 specific exemptions which are not considered Reporting Companies under the CTA. By and large, these exempted entities are either already required to report BOI or are very closely regulated. Some examples of these exemptions are many entities under specific sections of the Exchange Act (12 USC 78), entities registered with the Securities Exchange Commission, banks, federal credit unions, money services businesses registered with FinCEN under either 31 U.S.C. § 5330 or 31 CFR § 1022.380, and others.

(For full details on who is or isn't covered, refer to 31 CFR § 5336a(11), or review the BOI Small Compliance Guide[3].)

What Information is Required?

All beneficial owners of a Reporting Company must provide:

1. Full legal name;
2. Date of birth;
3. Current residential street address; and
4. The unique identifier and issuing jurisdiction for, and an image of, an accepted government-issued ID (e.g., a non-expired passport, driver's license, etc.)

A unique identifying number issued by FinCEN to an individual, called a FinCEN Identifier, can be provided in lieu of the above requirements.

Can UBO Information be Shared?

Generally, no.

Unless it's for a reason specifically carved out in the final rule, FinCEN and any officers/employees of the U.S. government, state, tribe, or local agencies, or even of any financial institution or regulatory agency who have access to this information cannot share it. In fact, as the next section will point out, there are fairly steep penalties for unauthorized sharing of this information.

The reasons specifically included in the final rule to allow sharing of information are:

1. An official request from a federal agency – specifically one "engaged in national security, intelligence, or law enforcement activity" – and the information must be used to further that activity

2. State, tribal, or local enforcement agencies which have been granted authorization by "a court of competent jurisdiction" to seek the information in furtherance of a criminal or civil investigation

3. Requests from foreign federal agencies on behalf of an appropriate party (such as enforcement agencies, judges, or prosecutors) in line with international treaties or agreements which will be used to assist in a prosecution or investigation. These requests must comply with the specific disclosure and use provisions of the applicable treaty or limit the use of any information received to only the authorized investigation or agency

> "Persons who commit reporting violations can face civil penalties of up to $500 per day that the violation continues or has not been remedied (up to $10,000 total) and/or up to two years imprisonment."

4. Requests from financial institutions who have the consent of the Reporting Company to facilitate compliance with customer due diligence requirements set forth under applicable law

5. Requests from federal function regulators or another appropriate regulatory agency, as described in the Final Rule

FinCEN will maintain this information securely for at least five years after the date of termination of the Reporting Company.

Is there a Timeline for Submission?

Yes, but the timeline is different depending on when the Reporting Company was created or registered to do business. That being said, the timelines are explicitly clear on when a Reporting Company is expected to comply.

- If a Reporting Company was created or registered to do business before the start of 2024, it will have until January 01, 2025 to ensure it's in compliance
- If a Reporting Company is created or registers to do business in 2024, it will only have 90 days to ensure it's in compliance
- If a Reporting Company is created or registers to do business after January 01, 2025, it will have 30 days to ensure it's in compliance

What are the Penalties for Noncompliance?

Reporting Violations:

- Reporting violations occur when any person (1) willfully provides or attempts to provide false or fraudulent UBO information or (2) fails to report to FinCEN complete or updated UBO information
- Persons who commit reporting violations can face civil penalties of up to $500 per day that the violation continues or has not been remedied (up to $10,000 total) and/or up to two years imprisonment

Unauthorized Use or Disclosure Violations:

- An Unauthorized Use or Disclosure Violation occurs when a person knowingly discloses or uses beneficial ownership information obtained through a report or disclosure submitted to FinCEN under the Rule except as specifically authorized thereunder
- Persons who commit an unauthorized use or disclosure violation can face civil penalties of up to $500 per day that the violation continues or has not been remedied (up to $250,000 total) and/or up to five years imprisonment
- If an unauthorized use or disclosure violation occurs while violating another U.S. law or is part of a pattern of illegal activity that involves over $100,000 over a 12-month period, the persons who committed the violation can face penalties up to $500,000 and/or up to 10 years imprisonment

There is safe harbor from both civil and criminal penalties if the person has no actual knowledge that the reported information is inaccurate, isn't attempting to evade the requirement, or submits a correction within 90 days of the original report's filing.

SOURCES

[1] federalregister.gov/documents/2022/09/30/2022-21020/beneficial-ownership-information-reporting-requirements#citation-12-p59499;
[2] govinfo.gov/content/pkg/FR-2022-09-30/pdf/2022-21020.pdf

The first step is to thoroughly review the requirements and implement a written policy for compliance. Your Compliance Officer may wish to do so by adding details on this requirement in an existing document or by creating a wholly new document. This will ensure that the expectations for compliance are clearly laid out on a company level for those involved in the reporting process.

From there, you'll need to assess which individuals will need to be reported and whether they already have a FinCEN Identifier. If the UBOs do not have a FinCEN Identifier, or if their information is outdated, you will need to begin the process of ensuring all information is collected and up to date.

Reports are filed via the FinCEN BOI E-Filing System[4], and may be completed via the fillable PDF document (The Beneficial Ownership Information Report, or "BOIR") available for download[5] or by completing and filing the report online. Once this is fully and accurately completed, you will want to ensure you maintain a copy of the final version for your records and then submit via the preferred method.

As with any new requirement, there will likely be some hiccups over the coming months following implementation, on both the industry and regulatory sides. FinCEN has made many resources available to aide companies that are or may be covered under the new requirement but given the importance of ensuring everything is being reported within the applicable timeframe, even well-oiled compliance teams have needed some additional help up front. If your company needs assistance with these requirements, it's recommended that you reach out to an independent compliance professional who will be able to guide you through the process to ensure your company is meeting its requirements.

[3] home.treasury.gov/system/files/136/2022-National-Strategy-for-Combating-Terrorist-and-Other-Illicit-Financing.pdf
[4] fincen.gov/sites/default/files/shared/BOI_Small_Compliance_Guide.v1.1-FINAL.pdf
[5] boiefiling.fincen.gov
[6] boiefiling.fincen.gov/b299dba56ae2428cdc4c.pdf

FOR MORE INFORMATION CONTACT

Jacob (Jake) Hines
Director at Ankura
jake.hines@ankura.com

Jacob (Jake) Hines, Director at Ankura, brings years of experience in state money transmitter acquisition, statutory license maintenance, and regulatory as well as consumer compliance.

Prior to joining Ankura, Jacob worked at a rapidly growing cryptocurrency firm, Voyager Digital, where he assisted in licensing acquisition, refining policies and procedures for compliance with applicable regulations, as well as with aiding in various other regulatory compliance functions.

By Jake Hines

10 Tips for More Effective **Change Reporting**

Congratulations! Your money service business (MSB) has gone through the grueling process of building out all business functions, writing and implementing policies and procedures, and acquiring licenses for your covered activities; the hard part is over!

Well, not quite.

While most companies anticipate the heavy lift of standard periodic reporting, many underestimate how cumbersome making a change can be. In some states, making changes is nearly as much work as a new application – and for some changes your company may actually be required to file a whole new application. Whether it is a new officer, owner, or product, you need to be sure you are following the reporting requirements for your company's proposed change.

1. Assess the change and whether it needs to be reported to the states.

Identify the change, the scope of its impact, and then review requirements in each licensed jurisdiction. Not every change needs to be reported, so do not make things more difficult for yourself by not taking the time to review them. Be thorough - and when in doubt, just reach out.

2. Look at the timelines for notification and/or requesting prior approval from all licensed jurisdictions.

Each jurisdiction has its own requirements, starting with whether a licensee needs to simply notify the regulator of the change or request prior approval. Ensure your company is meeting the requirements not only on the type of communication needed but also the time in which it must be provided to regulators. For example, a licensed money transmitter may have some changes that require notice within 15 days of the change and others that require them to request approval at least 120 days prior to the change's effective date. Keep in mind that some changes, such as a complicated change in ownership, may take even longer than this. In these such cases, flexibility is going to be your friend.

3. Look at the submission requirements associated with the change for each state.

There are some general requirements for changes that are congruent across most jurisdictions, but just like the application process itself, many states have additional state-specific requirements, too. States present on the NMLS provide amendment checklists that include the minimum requirements you will need to submit for your change. Ensure you know what is needed for each state in which your company is licensed, paying special attention to those requirements that may take more time or resources to complete.

4. Prepare the filing requirements, starting with general requirements needed by multiple states, then work on state-specific requirements.

The best way to begin here is to ensure you begin preparing general requirements as soon as you know a change is coming. You will also want to add the more cumbersome items to the top of the list. If you rely on a vendor, need to gather complex information, or have to prepare detailed documentation, make sure you build in enough time to do all the necessary prep work.

5. There is a time for everything, so plan accordingly.

You do not always have the luxury of delaying a change, but you should still be cognizant of when you are submitting a change request. If you are submitting a change that requires a state's prior approval, keep in mind that factors such as renewals and holidays can affect the change process. If you submit during a time of year when regulators are especially busy – such as during renewals or near the holidays – you may want to plan for the process to take some additional time.

6. Communicate, communicate, communicate!

Of course, this is not exclusive to change reporting, but it is absolutely crucial for a smooth process! Always be sure to keep an open line of communication with your regulators, whether you need clarity on a request, have questions about the state's requirements, or just want to check in on the status as your effective date draws near. As long as you are not calling their cellphones weekly, your regulators will probably be glad that you checked in – and sometimes you will even save them the effort of making another follow-up request.

7. Be pleasant with your regulators and your change team.

Juggling tight deadlines, responding to state requests, and gathering all the requisite documentation needed for a change can be stressful. Oftentimes, the same team handling the change is also still performing their full-time day-to-day duties. The process will go so much smoother if you maintain a positive attitude. You might think this goes without saying, but the fast pace of a tough change can wear down even the most optimistic teammates. Remember that you are on the same side, and that your regulators are not your adversaries.

> "While most companies anticipate the heavy lift of standard periodic reporting, many underestimate how cumbersome making a change can be."

8. Verify all approvals before the change becomes effective.

Once you have given notice and provided all required documentation, you still need to get the requisite approvals. For states that do not have a presence on the NMLS or states that communicate approvals via letter or email, you will want to keep a copy of the approval for your records. I also recommend keeping a PDF copy of the approvals in the Advance Change Notice section of the NMLS.

9. Confirm with your regulators that the change has become effective or if there has been a change of plan.

In line with tip number three, you will want to follow up with your regulators once the change becomes effective. This not only ensures that they are aware the change has been consummated but also gives them the opportunity to start in motion any post-change requirements (e.g., signed documents, change fees, etc.). On the other hand, if you have a change in plan that either delays or altogether cancels the change, communicate that to your regulators.

10. Do not be afraid to phone a friend!

Changes in the money services industry can be tricky and time consuming, so there is no shame in asking for help. In fact, often it is a major factor in getting the approvals you need in a timely manner. In addition to effective counsel with experience in the industry, you may want to consider bringing in outside help in the form of an independent compliance professional when facing big changes. Having someone on your side who has worked through this process with regulators in the past can smooth out the process significantly.

I hope these tips help you navigate the change process. It can be a daunting task, but with patience, thoroughness, and sometimes a bit of help, you can find success.

If your company needs help navigating a change, in your company, Ankura has many qualified – and pleasant – experts who have successfully guided companies large and small through the process, and we would be happy to assess how we can best help you!

FOR MORE INFORMATION CONTACT

Jacob (Jake) Hines

Director at Ankura

✉ jake.hines@ankura.com

Jacob (Jake) Hines, Director at Ankura, brings years of experience in state money transmitter acquisition, statutory license maintenance, and regulatory as well as consumer compliance.

Prior to joining Ankura, Jacob worked at a rapidly growing cryptocurrency firm, Voyager Digital, where he assisted in licensing acquisition, refining policies and procedures for compliance with applicable regulations, as well as with aiding in various other regulatory compliance functions.

By Omar Magana and Daniel Lee

Navigating OFAC **Sanctions Risks in the Digital Realm**: IP Addresses and Effective Controls

In today's digital landscape, sanctions enforcement has become a critical concern for Financial Institutions (FIs). The borderless nature of cyberspace can make it difficult to monitor and regulate activities that may breach sanctions imposed by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC). FIs are becoming increasingly aware of how important it is to examine and assess the complex risks arising from sanctions and internet protocol (IP) addresses. This overview aims to illuminate the intersection of OFAC sanctions and IP addresses, and to shed light on the complex challenges that organizations face while maintaining compliance and mitigating OFAC risks in the digital space.

Understanding OFAC Sanctions and IP Address Risks

OFAC administers economic and trade sanctions against foreign nations, individuals, and entities, aiming to safeguard national security and foreign policy objectives. Recognizing the intricate relationship between OFAC sanctions and IP addresses is crucial for organizations seeking to ensure compliance in the digital age.

IP addresses serve as critical data points in the identification and tracking of individuals, entities, and geographic locations subject to OFAC sanctions. A comprehensive compliance strategy involves monitoring IP addresses associated with sanctioned entities and countries to prevent inadvertent engagement in prohibited transactions. Unraveling the complexities of IP-based risks in the context of OFAC sanctions demands a proactive approach. Organizations must employ advanced technologies and analytics to scrutinize network traffic, detect anomalies, and promptly address potential violations. By incorporating IP address intelligence into risk management frameworks, businesses can fortify compliance efforts, safeguard against inadvertent entanglements with OFAC-sanctioned countries, and uphold ethical and legal standards.

Risks of Concealed Identities in Violation of Sanctions

The risks associated with concealed identities in violation of sanctions underscore the critical intersection between cybersecurity and OFAC regulatory compliance. In financial transactions and global trade, concealing one's identity through digital means poses a serious threat to the effectiveness of sanctions imposed by OFAC. Bad actors can exploit concealed identities to circumvent sanctions, engage in illicit activities such as money laundering and terrorist financing, or conduct business with sanctioned entities.

> "IP addresses serve as critical data points in the identification and tracking of individuals, entities, and geographic locations subject to OFAC sanctions."

From anonymizing technologies like virtual private networks (VPNs) to the manipulation of IP addresses and the deployment of encrypted communication channels, concealed identities create a veil that hampers traditional monitoring and detection mechanisms. Addressing these risks requires a holistic approach that combines technological advancements in identity verification and the continual adaptation of regulatory frameworks.

Geolocation Spoofing

Geolocation spoofing (i.e., the manipulation and misrepresentation of digital location information) has emerged as a real threat to FIs. It involves the use of specialized tools or applications that alter GPS coordinates, Wi-Fi network information, or IP addresses to create a false trail that can be challenging to trace. This tactic is particularly concerning in an era where location-based services are integral to electronic transactions. By falsifying geolocation data, threat actors can deceive systems with the aim of evading restrictions or accessing region-specific content.

Impact on Sanctions Compliance

The impact of geolocation spoofing on sanctions compliance is particularly pronounced in the financial sector, where transactions are closely scrutinized for potential ties to sanctioned entities or regions. By falsifying their geographic coordinates, bad actors can disguise the true nature of their financial activities, which undermines the efficacy of sanctions regimes. Addressing this challenge requires financial institutions and technology providers to develop advanced detection mechanisms capable of identifying and mitigating the risks associated with geolocation spoofing.

Mitigating Sanctions Risks: Effective Controls

Advanced IP Address Verification Technologies

Mitigating risks associated with OFAC sanctions and IP addresses demands a proactive risk management strategy. Organizations must implement advanced IP address monitoring tools capable of detecting and flagging any suspicious activities or deviations from established patterns. These tools should scrutinize incoming and outgoing traffic, conduct thorough analyses

of historical data, and identify potential anomalies indicating sanctions-related risks.

Additionally, organizations need to integrate stringent identity verification protocols within their systems to ensure that transactions and communications are legitimate. This may involve employing advanced authentication methods, such as biometric verification or two-factor authentication, to enhance the accuracy of user identification. Collaborating with threat intelligence providers and staying abreast of emerging risks is crucial for maintaining an effective defense against evolving tactics used by malicious actors seeking to exploit IP addresses for sanctions evasion.

Furthermore, a robust compliance program that includes regular audits, employee training initiatives, and clear communication channels with regulatory bodies must be established. Regularly updating and enhancing these controls ensures that organizations can adapt to the dynamic nature of OFAC sanctions, and the evolving methods employed by those attempting to circumvent them through IP address manipulation. By integrating these mitigating controls, FIs can bolster their defenses, foster a culture of compliance, and contribute to the overall integrity of international sanctions enforcement in the digital age.

How Can Your Organization Implement IP Address Detection?

IP address detection can be leveraged to enhance sanctions compliance, particularly in the context of financial transactions or online services. Here are some

> "Organizations must employ advanced technologies and analytics to scrutinize network traffic, detect anomalies, and promptly address potential violations."

ways in which IP address detection can be employed for sanctions compliance:

1. **Geolocation Analysis:** IP addresses can be used to determine the geographical location of users. Geolocation analysis can help to identify whether a user is accessing a service from a sanctioned country. Financial institutions and online platforms can also use geolocation data to flag transactions or activities originating from sanctioned jurisdictions.
2. **Proxy Detection:** Proxy detection is a process where businesses attempt to understand how online users connect to their websites. It is beneficial for catching harmful agents who spoof their connection details in order to commit fraudulent activities.
3. **Collaboration with IP Intelligence Services:** Third party vendors offer IP address screening to fulfill sanctions requirements by helping customers geolocate users of their products and services. These solutions can be deployed in different IT and data environments allowing organizations to strike a balance between compliance efficiency, automated processing, and effectiveness of controls.

It is important to note that while IP address detection can be a valuable tool, it is not a panacea. Instead, it should be part of a broader sanctions compliance program. Through past actions taken, OFAC has made it clear that it expects companies to utilize geolocation information screened from IP address data as part of its larger sanctions compliance program.

However, OFAC has also stated in its FAQs that international distribution authorities can reassign IP blocks, making the geographic location of an IP potentially dynamic. Therefore, any FI that facilitates internet-based transactions should ensure that its automated technological tools are part of a comprehensive sanctions compliance program that includes traditional due diligence methods such as gathering authentic identification information on customers before opening a new account or initiating new transactions.

> "In the last two years, OFAC has imposed penalties totaling over $35 million on companies that allegedly neglected to implement effective controls to mitigate risks associated with IP addresses."

In the last two years, OFAC has imposed penalties totaling over $35 million on companies that allegedly neglected to implement effective controls to mitigate risks associated with IP addresses. These substantial fines underscore the increasing scrutiny and emphasis on cybersecurity within the global business landscape. OFAC's enforcement actions reflect a growing recognition of the critical role that robust risk management and compliance measures play in safeguarding against illi it activities associated with sanctions evasion. As technology continues to advance, FIs must remain vigilant in fortifying their cybersecurity frameworks to ensure both regulatory adherence and the protection of sensitive information, thereby avoiding the financial repercussions that come with non-compliance.

Organizations should stay informed about regulatory changes, update their systems accordingly, and ensure that they are compliant with applicable laws and regulations in the jurisdictions where they operate. Consulting with legal and compliance experts is advisable to develop a robust and effective sanctions compliance strategy.

FOR MORE INFORMATION CONTACT

Omar Magana, CAMS

Managing Director at Ankura

✉ omar.magana@ankura.com

Omar Magana, CAMS, Managing Director at Ankura, has over 20 years of experience developing and leading domestic and international compliance programs and business practices aligned with state and federal regulatory laws, regulations, and industry best practices. Omar is a subject matter expert in anti-money laundering/combating the financing of terrorism (AML/CFT) and sanctions screening, as well as other regulatory requirements specific to financial services.

Prior to joining Ankura, Omar worked in the Money Services Business industry and in private banking with a proven track record in developing programs, building international and domestic AML programs; as well as leading anti-bribery and corruption programs.

FOR MORE INFORMATION CONTACT

Daniel Lee

Director at Ankura

✉ dan.lee@ankura.com

Daniel Lee, Director at Ankura, has over 15 years of regulatory compliance and consulting experience in the Banking and Money Service Business industry.

As a former examiner and Fintech subject matter expert at the Colorado Division of Banking, Daniel led examinations of Fintech and virtual currency companies for compliance with state and federal regulations and has assisted mid to large size financial institutions with their model validation, model tuning, and model risk governance activities.

By Robert Reed

The Importance of **KYC/CDD Review in Preparing for a BSA/AML** Program Examination

The Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) regulations are fundamental components of the financial industry's efforts to combat financial crimes. As a BSA/AML Officer, it is crucial to ensure that your institution's BSA/AML Program is robust, effective, and compliant with regulatory requirements. A critical aspect of this program is the Know Your Customer (KYC) and Customer Due Diligence (CDD) processes. Preparing for a BSA/AML Program examination by conducting a thorough review of KYC/CDD practices is vital for several reasons.

As KYC and CDD are essential elements of a financial institution's BSA/AML compliance framework, regulators expect institutions to have a comprehensive understanding of their customers' identities, the nature of their business, and the risks they may pose. A rigorous KYC/CDD review ensures that the institution has accurate and up-to-date information on its customers, which is crucial for detecting and reporting suspicious activities. When Regulators identify missing data, it leads to the obvious conclusion that the customer risk scoring program may be hampered by the missing data.

> "Regulators will scrutinize the institutions adherence to BSA/AML requirements."

A well-conducted KYC/CDD review allows the institution to identify and assess the risks associated with its customer base. By understanding these risks, the institution can implement appropriate controls to mitigate them. This proactive approach not only aids in the prevention of illicit activities but also demonstrates to examiners that the institution is actively managing its risk exposure.

As we all know, during an examination, regulators will scrutinize the institution's adherence to BSA/AML requirements. A list of all current clients is expected in the initial pull list of the exam. Your proactive comprehensive KYC/CDD review ensures that all customer profiles are complete and conform to regulatory standards. It also verifies that Enhanced Due Diligence (EDD) is performed on higher-risk customers because you know your customer risk scoring program has the necessary information to do its job. Non-compliance can result in significant penalties and reputational damage, making the KYC/CDD review an indispensable part of the preparation process.

The KYC/CDD review process can reveal gaps in policies, procedures, and training programs. This discovery presents an opportunity to update and strengthen these areas before an examination. It also ensures that employees are well-trained and equipped to carry out their BSA/AML responsibilities effectively.

A thorough KYC/CDD review sends a strong message to regulators and stakeholders about the institution's commitment to BSA/AML compliance. It showcases the institution's dedication to maintaining a strong control environment and its willingness to invest resources in compliance efforts.

In preparation for a BSA/AML Program examination, conducting a comprehensive KYC/CDD review is of paramount importance. It not only ensures compliance with regulatory standards but also enhances the institution's ability to manage risks effectively. By identifying any deficiencies and taking corrective actions, the institution can demonstrate its commitment to upholding the integrity of the financial system. As BSA/AML Officers, we must prioritize this review to safeguard our institutions against the threats of money laundering and terrorist financing while maintaining public trust in our financial systems.

A recent trend has been identified with regulators focusing on KYC/CDD becoming a data collection exercise instead of truly knowing one's customer. With massive amounts of data to review, the challenge of how to accomplish such tasks with any reasonable certainty or efficiency deters most from the important quality control process. Obtaining assistance from a third party such as Ankura allows you to maintain business as usual but prepare for the exam. Ankura has several approaches that could work for your institution. Let us start the conversation.

FOR MORE INFORMATION CONTACT

Robert Reed

Managing Director at Ankura

robert.reed@ankura.com

Robert Reed, Managing Director at Ankura, has over 20 years of experience in the financial services industry as a senior C-suite executive, BSA/AML officer, and operations, compliance, MIS risk, and trading professional. Robert has established regulatory effectiveness groups at global and regional banks and led over 100 anti-money laundering (AML) regulatory examinations with U.S. federal, state, and global regulators, including a challenging written agreement in one instance and a consent order in another.

Further, he has overseen multiple remediation projects pertaining to compliance findings and directed global technology projects to enhance automated reporting, AI, and process monitoring. Robert brings a broad perspective and diverse skillset to enhance operations through scalable processes and technology, develop strong programs and concise executive reporting, and solve serious regulatory issues across a wide spectrum of compliance matters.

By Malessa Babineaux

AML Risk Assessment Revisited

The Bank Secrecy Act (BSA) does not explicitly state that money services businesses (MSBs) must conduct an anti-money laundering (AML) risk assessment. However, it does say that an MSB "shall develop, implement, and maintain an effective AML program" and that the program "shall be commensurate with the ***risks*** posed by the location and size of, and the nature and volume of the financial services provided" (31 CFR § 1022.210). By that logic, how can an MSB build a program that is commensurate with its risks if it hasn't evaluated its risks by conducting a risk assessment? How else can an MSB assess its money laundering and terrorist financing risks? Thus, while not a requirement, an AML risk assessment (AML RA) is necessary for an MSB to ensure its AML program is effectively identifying and mitigating its risks.

With that being said, the AML RA has become an expectation of regulators and an industry standard, even if not a regulatory requirement. However, it's not enough to conduct an AML RA once or to consider it as a stand-alone document. It should be utilized to inform the rest of your AML program and tied to the MSB's AML policy. When an MSB's risk changes, not only should the risk assessment be updated but also the MSB's AML policy to ensure processes and controls to mitigate the risks identified are implemented. As stated previously, the risk assessment process should not be viewed as a one-time thing. An AML RA should be updated at least annually or whenever there are significant changes to the MSB's operation. The AML RA is an ever evolving, living document, that should accurately reflect and consider the MSB's operation to take into account changes that occur as the operation evolves.

> "What better time to update your AML RA than at the beginning of the year."

And what better time to update your AML RA than at the beginning of the year. That is the best time to assess your AML program, review the previous year's operation, and take into account future plans for expansion or changes. While updating the risk assessment annually is an industry best practice, always remember that updates should be made whenever significant changes to an MSB's operation

occur that would alter a company's risks. Whenever the MSB is updating its AML RA, it should consider asking some of the following questions:

Customers

- Has the target customer changed over time?
- Did the MSB's main customer base change within the past year?
- Did the MSB identify changes in customer activity patterns?
- Does the MSB plan to expand its services to business customers?

Geography

- Does the MSB only offer its services domestically?
- Does the MSB plan to expand its geographic footprint internationally?
- Does the MSB have plans to offer its services in high-risk jurisdictions?

Products/Services

- Did the MSB add products/services to its portfolio?
- Did the MSB change any of the products/services it offers?
- Does the MSB plan to add or remove products/services in the future?

People/Processes/Technology

- Did the MSB make changes to the systems that it uses to collect and store customer data?
- Did the MSB change or update its transaction monitoring or sanctions screening systems?
- Were changes made to key personnel such as Board members, senior management, the AML Officer or other compliance or operational staff?
- Did the MSB implement new or updated processes for compliance?

The MSB should identify the answers to these questions and others, as this list is not all inclusive, and update its AML RA accordingly. The MSB should also have a methodology documented to support its scoring model so that the AML RA does not appear subjective. The MSB should also focus on using both quantitative and qualitative data, as it should have a nice balance of both to provide real insights into the MSB's risks.

While we are on the subject, now is the perfect time to also ensure that your AML Risk assessment addresses the eight National Priorities ("Priorities") issued pursuant to the AML Act of 2020 (AMLA) on June 30, 2021. At that time, FinCEN issued its first ever government wide priorities for anti-money laundering and countering the financing of terrorism (AML/CFT) in accordance with § 6101(b)(2)(c) of the AMLA. These Priorities are as follows: corruption; cybercrime; terrorist financing; fraud; transnational criminal organizations; drug trafficking organizations; human trafficking and human smuggling; and proliferation financing.

While not technically a requirement until FinCEN issues regulations to specify how MSBs should incorporate these priorities into their risk-based AML programs, as a best practice, MSBs should incorporate these Priorities now, if they haven't already done so. These Priorities are not unfamiliar to MSBs. Long before FinCEN identified these as Priorities, this type of activity has been prevalently seen in the MSB industry. Thus, MSBs should not wait for FinCEN to issue regulations to address these Priorities as this industry is at the forefront of detecting, investigating, and reporting

> "MSBs should be proactive and review their current risk assessment program's processes, controls, and governance to prepare for the forth-coming require-ments."

this type of activity in its day to day AML compliance operation. To properly address the risks associated with these Priorities, MSBs should review each one to identify which ones are relevant to the MSB's operation and incorporate them accordingly into their AML RA. Once these regulations are issued in connection with the Priorities established by FinCEN, MSBs will be required to evaluate and integrate these Priorities based on their own operation and AML program. In the meantime, MSBs should be proactive and review their current risk assessment program's processes, controls, and governance to prepare for the forthcoming requirements.

Lastly, at a recent conference, a representative of FinCEN indicated that it would soon, as in some time in 2024, issue guidance making AML risk assessments a statutory requirement for all financial institutions going forward. It was also commented that FinCEN would issue standard guidelines on how to create an AML risk assessment.

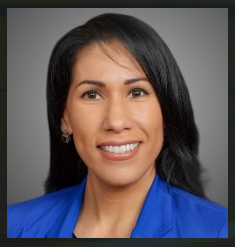
Thus, now is the time to get ahead and update your risk assessments to include the National Priorities identified in the AMLA and to make any updates necessary to properly address the changes to your operation and accompanying AML risks. The beginning of the year is always the perfect time to reflect on the previous year and look toward the future. While there is yet no standard way or official guidelines on how to create an AML RA, Ankura has experienced consultants that can assist you with conducting, creating, updating, and implementing an effective and reasonably designed AML RA that is tailored to your Company's operation and that will satisfy industry best practices and future regulatory requirements.

SOURCES

[1] ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1022/subpart-B/section-1022.210

[2] fincen.gov/news/news-releases/fincen-issues-first-national-amlcft-priorities-and-accompanying-statements

[3] fincen.gov/sites/default/files/shared/Statement%20for%20Non-Bank%20Financial%20Institutions%20(June%2030%2C%202021).pdf



FOR MORE INFORMATION CONTACT

Malessa Arias-Babineaux, CAMS, CITRMS,

Managing Director at Ankura

malessa.babineaux@ankura.com

20 years of experience in BSA/AML compliance at Transnetwork, Noventis, FTGlobalPay, and Bancomer Transfer Services. Expert in AML, sanctions, and consumer compliance in the U.S., Canada, and Latin America. Fluent in English and Spanish.

During her career, Malessa has gained experience in building and maintaining effective BSA/AML compliance programs at several companies in the Money Services Business (MSB) industry. In addition to BSA/AML, her expertise includes developing and implementing programs for OFAC, consumer privacy (GLBA), CFPB remittance transfer rule (Reg E), consumer fraud, anti-bribery (FCPA), elder abuse, sanctions screening including PEPs, and transaction monitoring and reporting. She also has extensive knowledge in building agent oversight and foreign correspondent programs, training programs, customer due diligence processes, risk assessments and writing regulatory policies and procedures. She has also created, established, and managed MSB compliance programs in Latin America.

Nationwide Multistate Licensing System

NMLS CORNER

2024 NMLS Annual Conference and Training

The annual 2024 NMLS Annual Conference and Training was held on February 13 – 16, 2024 in San Antonio, Texas.

The 2024 NMLS Conference and Training connects users to the NMLS ecosystem and gives users an opportunity to meet peers, network with regulators and industry partners and hear about the latest trends and updates from the world of supervision. Attendees participated in concurrent breakout sessions, listened to roundtable discussions with experts, networked with peers, and met their regulators.

The NMLS conference, held annually, includes representation from the following industries:

- Mortgage
- State Licensing
- Money Services Business
- Consumer Finance
- Debt
- Federal Registry
- Surety
- State Examinations

Ankura participated in the NMLS Conference

The Conference included the NMLS Ombudsman Meeting – an opportunity for industry users to raise issues concerning the use and policies of NMLS and collaboratively discuss these issues in-person with state regulators in an open environment. Ankura discussed the timely topics of obtaining a trust/primary bank account for money transmission and financial requirements for start-up companies as issues that impede the licensing process for our clients.

In the session, **How to Reach a Win-Win: NMLS Best Practices – Learn What it Takes to Keep Agency Licensing Staff and the Company Users They License Happy,** a panel comprised of guest speakers from all sides of the licensing process shared their perspectives and recommendations for creating a strong agency and company relationship. The panel included:

- Trish Lagodzinski, Senior Director at Ankura
- Amy Greenwood Field, Partner at McGlinchey Stafford PLLC.
- Jennifer Pic, Director, Learning and Development, Conference Of State Bank Supervisors.
- Bradley Fletcher, Consumer Services Manager, Illinois Department of Financial & Professional Regulation.
- Maureen Camp, Chief of Licensing & Administration, Washington Department of Financial Institutions.
- Ulaya Parson, NMLS Regulatory User Group, Conference of State Bank Supervisors.

Additional NMLS Conference and Training Sessions included:

Forces Transforming Financial Services – looking at financial services (and financial service providers) 5-10 years from now and how public cloud wars, AI-as-a-Service, 5G, internet from space, AI chips on-device, and Software 2.0 will impact the evolution, distribution, and consumption of financial services.

Nationwide Multistate Licensing System

NMLS CORNER

Manage Your NMLS Account with Confidence: A Closer Look at NMLS Modernization in 2024 – coming enhancements to make managing your NMLS account a better experience.

Digital Currency: The View from DC – Despite high profile events in the crypto world over the last 18 months, Congress and federal regulators have moved slowly in addressing these new products. This session evaluated the current status of federal action in the digital currency world, barriers to progress, and what state regulators and industry participants can expect in 2024.

Mortgage One Company One Exam & Exam Standards with SES – a new mortgage One Company One Exam (OCOE) Protocol was established in 2023. State regulators are preparing for the next phase of this initiative and discussed the new supervisory process, and the work state regulators are doing to standardize exams and exam information requests.

Cybersecurity Threat Briefing and Proactive Resilience: Strategies for Addressing Evolving Threats – Jennifer Gold, President and Board Chair of NY Metro InfraGard addressed the dynamic threat landscape facing the financial services industry including valuable insights on navigating the FTC Safeguards Rule.

Empowering Mortgage Professionals: A Closer Look at NMLS Modernization in 2025 – the Mortgage Loan Originator (MLO) experience will be the focus of major NMLS enhancements in 2025.

SES Basics Training for Companies – the end-to-end process for a company user with tips and tricks to make your first exam an easy one.

Working Session on Money Transmission Modernization Act Implementation – a discussion and update on the Money Transmission Modernization Act (MTMA) legislative efforts and implementation issues and challenges.

Consumer Finance Trends in Lending Products – regulator, consumer advocate, lender discussion on the growth of "lending" products such as earned wage access programs and buy now pay later.

Cybersecurity Challenges Faced by Licensees – the session covered the IT and cybersecurity challenges faced by licensees, including the threat landscape, explored the impact and applications of Artificial Intelligence (AI), and shared best practices for cyber and IT exams.

Mortgage Call Report Form Version 6 Training – this session focused on the new changes in the Mortgage Call Report Form Version 6 and helping companies manage those changes.

Work Smarter with SES QuickIR: Basics and Best Practices for Companies – this session took a closer look at QuickIR, the information request response management tool available to companies in SES.

Aligning the MSB Call Report and Money Transmission Modernization Act – MSB regulators discussed how they are using the MSB Call Report to assess compliance based on the Money Transmission Modernization Act.

Financial Services State Legislative Update – State legislatures dealt with an array of financial services-related issues that arose during 2023 in compliance.

From Data to Decisions: Leveraging Feedback to Improve NMLS – In this session, the NMLS team shared how they are engaging NMLS users and other stakeholders to improve the NMLS ecosystem now and in the future.

MSB One Company One Exam Working Session – Three years ago, the state system launched the One

Company One Exam (OCOE) supervisory process for MSBs, creating the roadmap for state exam coordination. Leaders from both state agencies and industry discussed how the landscape has evolved and how the process has matured since the launch of this initiative.

Testing and Education Update – During this annual update of the Mortgage Testing and Education program, the session addressed changes that are being considered regarding how education is delivered which could have an impact on course providers and future MLOs including the SAFE MLO test.

You've Asked, We've Listened and Our Doors are Still Open (with IDWG) – The Industry Development Working Group members discussed the work they do for the industry including successes and an opportunity to provide feedback and ask questions.

Communications-Focused Cyber Incident Preparedness & Response Discussion, Part 1 and Part 2 – In this two-part fictional cyber incident scenario, participants learned about the communication roles of non-technical personnel in the overall incident response process.

Crypto Across the States – Despite gridlock in Washington, state agencies and state legislators across the country continue to move forward bringing the digital currency activities inside the regulatory perimeter. This session explored various state responses to addressing regulatory and consumer protection issues created by cryptocurrencies.

The NMLS Basics Series:

The NMLS Basics series is centered on the NMLS features that state-licensed company users need to apply for and maintain their licenses. Each training session can be done as a standalone course or for the best experience users can complete the full series.

NMLS Basics Part 1: MU1 – focused on successfully completing the MU1 and addressing common completeness checks.

NMLS Basics Part 2: MU2 – NMLS Basics Part 2: MU2 focused on successfully completing the MU2, who is required to complete the MU2, and addressed common completeness checks.

NMLS Basics Part 3: ESB & Financial Statements – NMLS Basics Part 3: ESB and Financial Statements focused on successfully submitting initial ESB and Financial Statements as well as completing annual Financial Statement requirements.

NMLS Basics Part 4: License Management – NMLS Basics Part 4: License Management addressed those who have one or more active licenses and want to learn more about amending or updating licenses.

NMLS Policy Guidebook Updates Available – An updated version of the NMLS Policy Guidebook was posted to the NMLS Resource Center and the Regulator Resource Center. Click here to view a summary of the updates.

State News from NMLS:

Louisiana Adds New Private Education Lender to NMLS January 1, 2024

As of January 1, 2024, NMLS began receiving new application filings for the Louisiana Office of Financial Institutions Private Education Lender License. Click here for more information.

Nevada FID Adds Student Loan Servicer License to NMLS December 1, 2023

As of December 1, 2023, NMLS began receiving new application filings for the Nevada Financial Institutions Division Student Loan Servicer License. Click here for more information.

Nationwide Multistate Licensing System

NMLS CORNER

Maine Adds Full and Limited Service Payroll Processor License and Restricted Service Payroll Processor License to NMLS December 1, 2023

As of December 1, 2023, NMLS began receiving new application and transition filings for the Maine Bureau of Consumer Credit Protection Full and Limited Service Payroll Processor License and Restricted Service Payroll Processor License.

Note: Companies holding these license types were required to submit a license transition request through NMLS by filing a Company Form (MU1) and an Individual Form (MU2) for each of their control persons by January 31, 2024. Click here for more information.

Maine Office of Consumer Credit (Bureau of Consumer Protection) Adds New License Types to NMLS on October 1, 2023

NMLS began receiving new applications for the Maine Office of Consumer Credit (Bureau of Consumer Protection) on October 1, 2023. New applicants can submit these records through NMLS for the following license types:

- Debt Collector
- Debt Collector Branch

New applicants can view the license requirements and submit these records through NMLS. Click here for more information.

Connecticut Department of Banking Adds Private Education Lender Registration to NMLS on October 1, 2023

NMLS began receiving new applications for the Connecticut Department of Banking Private Education Lender Registration on October 1, 2023. New applicants can submit these records through NMLS.

Applicants can view the license requirements on the State Agency Licensing page. Click here for more information.

Maryland Office of Financial Regulation Adds Student Financing Company to NMLS on October 1, 2023

NMLS began receiving new applications for the Maryland Office of Financial Regulation Adds Student Financing Company on October 1, 2023. New applicants can submit these records through NMLS.

Applicants can view the license requirements on the State Agency Licensing page. Click here for more information.

Minnesota Money Transmission Modernization Act

On May 24, 2023, Governor Tim Walz signed Minnesota Session Law 2023, Chapter 57, Senate File 2744 into law, which included the Minnesota version of the Money Transmission Modernization Act (MTMA). For a copy of the communication from the Minnesota Department of Commerce regarding the MTMA, click here.

Licensing Port of Call

Resources for the Regulatory Voyage

To learn more, or if you want to see how Ankura can help you navigate the regulatory waters and add value to your team, contact Eric Gagnon at eric.gagnon@ankura.com

PENDING LEGISLATION UPDATES:

- Arizona introduced SB1128, which will allow State Agencies to enter agreements with Cryptocurrency Service Providers to provide a method to accept cryptocurrency for payment of fines, civil penalties, taxes etc. in Arizona.
- Rhode Island introduced H7266, which would provide guidelines for virtual currency kiosks, including a maximum daily transaction amount. This bill does not include a provision requiring a license for the operation of the virtual currency kiosk.
- California Introduced AB1934, which could require additional monthly reporting to show compliance with specific conditions for companies exchanging, transferring, or storing digital financial assets.

IMPORTANT UPDATES | "CHANGES IN THE REGULATORY TIDE"

Money Transmission Modernization Act (MTMA)

States have been adopting the Money Transmission Modernization Act (MTMA), either in full or by adopting significant portions of the Act. The effective dates of these adoptions began in 2023, with a number of additional states still in the process of enacting the MTMA. Ankura strongly encourages that money service businesses review the regulatory changes and update relevant procedures to ensure continued compliance.

The following States have adopted in full or significant aspects of the MTMA:

Arkansas, California, Connecticut, Georgia, Hawaii, Indiana, Iowa, Maryland, Minnesota, Nevada, New Hampshire, North Dakota, South Dakota, Tennessee, Texas, Utah, and West Virginia.

The following States have pending legislation to process for MTMA in 2024:

Alaska, Idaho, Illinois, Iowa, Kansas, Maine, Massachusetts, Missouri, New Hampshire, Rhode Island, South Carolina, Vermont, Virginia, and Wisconsin.

How does continued MTMA adoption affect your company?

During the 2023 Money Transmitter License renewal season, your company may have seen changes to required surety bond amounts, the need to submit additional net worth calculations, and possibly changes to the permissible investment types. For many companies, permissible investment and surety bond changes may have been negligible. But for many companies that operate in states where the MTMA has been adopted, the change from using a Net Worth calculation to Tangible Net Worth calculation brings great consternation. This marks a shift in focus from dependence on surety bonds to the financial sustainability of a money service business.

Until recently, most states reviewed the company's Audited Financial Statements and noted the bottom-line net worth. With the adoption of MTMA, the shift to a Tangible Net Worth calculation changes how companies are evaluated by State Regulators.

Net Worth is normally calculated as the value of the company's Assets minus its Liabilities. Once we specify that assets must be 'Tangible' the net worth calculations can change substantially. Tangible Net Worth [TNW] requires intangible assets be excluded from the Assets. Intangible assets will include line items such as Goodwill, along with the value assigned to copyrights, patents, and intellectual property.

In high-growth innovation-driven sectors like the fintech space, it's common for investment into intangibles (innovation, brand capital, data, and analytics) to exceed those of other sectors. With that in mind, excluding potentially large investments into areas like *Innovation and Brand Capital* from a fintech's balance sheet could flip a company's Net Worth from a strong positive position into a negative TNW.

In states where MTMA has been signed into law, being required to show a positive TNW may inhibit a company from submitting a new application or could force current licensees into a capital restoration plan. It's imperative before filing applications to connect with industry consultants to make sure all regulatory guidelines are being met before submitting applications.

We Can Show You The Way

We deliver powerful solutions to complex regulatory, licensing, and compliance challenges experienced by Fintech and financial services companies. We have served nearly 600 firms ranging from Fortune 50 to Fintech's biggest unicorns throughout the world. The acquisition of Chartwell by Ankura further enhances the entire organization's global anti-financial crime offering to help banking and Fintech clients navigate the full spectrum of BSA/AML challenges, licensing acquisition, maintenance, and administration as well as outsourcing services.

VALUE PROPOSITION

ONE-STOP SOLUTION

Complete outsourcing of worldwide license acquisition and maintenance and many day-to-day compliance and AML staff functions. Flex talent and variable fee structure that are superior to direct hiring or other service provider options.

SATISFIED CLIENTS

Over 600 satisfied clients, including some of the most prominent multinationals in their respective industries and many firms within the Fortune 1000.

STABLE, HIGHLY QUALIFIED WORKFORCE

Our team is staffed by employees, the majority of whom have over 20 years of experience as practitioners or regulators. We are proud of its low turnover rate and the many awards it has received for a unique and revolutionary corporate culture and approach to staff development.

EXCEPTIONAL PROJECT MANAGEMENT

Our staff members practice a Kaizen methodology and use proprietary project management techniques that sustain a high level of quality.

2024 PROMOTIONS

Ankura is pleased to congratulate the following individuals on their promotions.

Claudia Raskey
Senior Associate

Erik Kemme
Director

Eric Gagnon
Senior Director

Gregory Scheffler
Senior Associate

Heather Chester
Director

Hilda Mussi
Senior Director

Juan Saa
Senior Associate

Jake Hines
Director

Richard Davis
Senior Director

Olivia Turner
Senior Associate

Karen Greene
Director

Russell Morin
Senior Director

Risk, Forensic & Compliance – Anti-Financial Crime Team

Our team members are cross-certified in regulatory compliance, anti-money laundering, testing, information technology and security, and fraud. The diversified experience of our consultants provides our clients with access to seasoned examiners, operators, and regulatory policy makers in the banking, non-banking, and emerging payments compliance segments of the financial services industry.

CONSULTANTS AVERAGE 22 YEARS OF EXPERIENCE

We use this vast experience to design and implement executive compliance and risk management programs properly calibrated to address both the current and prospective regulatory environment.

EXTENSIVE EXPERIENCE AT THE INDUSTRY'S BEST ORGANIZATIONS

Staff members have served in:

- The Regulatory Divisions of CA DPFI, CO DOB, FL OFR, TX DOB, & VT
- The Regulatory Divisions of the California Department of Business Oversight and the Florida Office of Financial Regulations
- MSBs such as Western Union, First Data, and Sigue
- State and nationally chartered banks
- The Federal Bureau of Investigation's Financial Crimes and Terrorist Financing Section
- Assistant Director of the Enforcement and Compliance Division at the Office of the Comptroller of the Currency (OCC)

CROSS-CERTIFIED STAFF MEMBERS

- Certified AML (CAMS)
- Regulatory manager certifications CRCM and PMP

Our Services

Fintech Licensing

With its large team of long-time licensing officers and former regulators, We have centuries of collective experience obtaining and maintaining thousands of regulatory licenses for Fintech companies in areas like money transmission, cryptocurrency, prepaid access, currency exchange, lending, and gaming. The firm provides a fully outsourced solution in all key component parts of getting and staying licensed. Our emphasis on excellent project management and Kaizen methodology helps ensure timely results. Our sta have serviced, worked at, or supervised a statistically significant portion of all licensed U.S. money transmitters.

Banking Compliance

Our team has well-credentialed former bank compliance officers and regulators who serve all types of banks as well as challenger/neo/digital banks in most areas of bank regulatory compliance. Numerous clients come from the Fintech industry and several of the Fintech banking market leaders have worked with us. Our team brings a unique, first-hand experience to its work.

Federal Compliance

Our team is one of the world's preeminent providers of AML/CFT, fraud prevention, and regulatory compliance services to the Fintech industry. Comprised of an incredibly deep bench of long-time practitioners from all corners of the Fintech industry, the firm builds, localizes, enhances, and audits compliance programs. It has served many of the industry's leading Fintechs, hundreds of companies overall throughout the world.

Global Outsourced Compliance

Our team of veteran compliance officers, regulators and analysts are positioned as an outsourced resource for compliance program execution with many financial services businesses. The firm handles many of the day-to-day functions required to maintain an effective compliance program, including transaction monitoring and reporting; sanctions screening; KYC and customer due diligence; onboarding and enhanced due diligence; fraud prevention; consumer compliance; and taking overall leadership of the program. Providing flex talent at variable cost, with excellent bench depth and quality assurance, we are a strong alternative to hiring directly in many cases.

Strategic Alliances

Hawk AI helps banks, payment companies and fintechs fight financial crime with AML and fraud surveillance. Powered by explainable AI and Cloud technology with a focus on information sharing, our technology improves the efficiency and effectiveness of anti-financial crime teams.

Thomson Reuters is a leading provider of business information services. Our products include highly specialized information-enabled software and tools for legal, tax, accounting and compliance professionals combined with the world's most global news service – Reuters.

Fiserv, a global leader in payments and financial technology, helps clients achieve best-in-class results in account processing and digital banking solutions; card-issuer processing and network services; payments; e-commerce; merchant acquiring and processing; and the Clover® cloud-based point-of-sale solution.

Through its subsidiary, MVB Bank, Inc., and the Bank's subsidiaries, MVB provides financial services to individuals and corporate clients in the Mid-Atlantic region and beyond.

Acuant Compliance's Trusted Identity Platform provides identity verification, regulatory compliance (AML/KYC) and digital identity solutions leveraging AI and human-assisted machine learning to deliver unparalleled accuracy and efficiency.

NICE Actimize uses innovative technology to protect institutions and safeguard consumers and investors by identifying financial crimes, preventing fraud and providing regulatory compliance.

Middesk's Identity product provides accurate, complete information that financial services companies need to make efficient onboarding decisions. Our Agent product makes it easy for employers to file with the state and federal agencies needed to establish their business across the country. Our customers include Affirm, Brex, Plaid, Mercury, Divvy, Rippling, Gusto, and others.

Coinfirm is a global leader in AML & RegTech for blockchain & cryptocurrencies. Offering the industry's largest blockchain coverage - over 98% of cryptocurrencies supported - Coinfirm's solutions are used by market leaders, ranging from VASPs such as Binance, and protocols like WAVES, to major financial institutions and governments.

Accuity offers a suite of innovative solutions for payments and compliance professionals, from comprehensive data and software that manage risk and compliance, to flexible tools that optimize payments pathways.

Compass

Stay up to date on the latest in financial regulatory compliance, financial crime prevention, and risk management.

SUBSCRIBE TODAY

EDITORIAL STAFF

Jonathan Abratt | Senior Managing Director | jonathan.abratt@ankura.com
Sherry Tomac | Senior Managing Director | sherry.tomac@ankura.com
Richard Davis | Senior Director | richard.davis@ankura.com

WE ARE HONORED TO BE RECOGNIZED BY THE FOLLOWING ORGANIZATIONS

RECOGNITION HELIOS HR APOLLO AWARDS WINNER

FinTech EXCELLENCE Awards WINNER

2022 moxieaward CELEBRATING BOLDNESS IN BUSINESS FINALIST

SmartCEO's FUTURE 50 awards WINNER

SmartCEO's CORPORATE CULTURE AWARDS WINNER

SmartCEO's HEALTHIEST COMPANY awards celebrating workplace wellness