CHARTWELL
IS NOW ANKURA

COMPASS

A FINANCIAL REGULATORY COMPLIANCE INDUSTRY PUBLICATION

APRIL 2023

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 biggest unicorns throughout the world.

ankura | **Chartwell Joins Ankura to Bolster Global Banking and Fintech Compliance Advisory Services**

EDITORIAL STAFF:

Jonathan Abratt, Senior Managing Director
jonathan.abratt@ankura.com;

Richard Davis, Director
richard.davis@ankura.com

Chartwell Joins Ankura to Bolster Global Banking and Fintech Compliance Advisory Services

Acquisition further enhances Ankura's Global anti-financial crime offering to help banking and Fintech clients navigate the full spectrum of BSA/AML challenges

NEW YORK – [March 1, 2023] – Ankura Consulting Group, LLC ("Ankura"), a leading global expert services and advisory firm, today announced that it has acquired Chartwell Compliance ("Chartwell"), a leading global regulatory compliance and risk management firm that is a wholly-owned subsidiary of MVB Bank, Inc. held by MVB Financial Corp. (NASDAQ: MVBF) ("MVB", "MVB Financial"). The addition of Chartwell expands Ankura's Global Anti-Financial Crime (AFC) Practice across a wide range of banking and financial technology (Fintech) businesses, addressing a crucial need for Bank Secrecy Act/Anti-Money Laundering (BSA/AML) regulatory and compliance programs among mid-market banks, cryptocurrency and blockchain platforms, venture capital firms and payment solution providers.

Founded in 2011 in Bethesda, Maryland and now headquartered in Fairmont, West Virginia, Chartwell provides integrated regulatory compliance, state licensing, financial crimes prevention, and enterprise risk management services that include consulting, outsourcing, testing, and training solutions. As one of the world's leading specialist firms in state and federal compliance and market entry facilitation for firms entering into or expanding in North America, Chartwell serves many of the most high-profile providers in the Fintech industry, including commercial bill pay solution providers, cryptocurrency and blockchain innovators, publicly-traded online marketplaces, venture capital firms, Fintech banks, third-party payments processors and financial accounting software providers. Since joining MVB Bank in 2019, Chartwell has deepened its advisory expertise and capabilities, more than tripled its revenue and headcount, and positioned itself for continued strong growth.

"Having Chartwell as a part of the MVB family over the past three years has been an extremely beneficial relationship that allowed MVB to grow and scale our Fintech business while we also strengthened our internal risk and compliance resources. Chartwell is an industry leader and has expanded in new and creative ways, and we believe Chartwell will continue to thrive as part of the Ankura team. Chartwell's services and expertise are a great fit for Ankura, and we will continue to have a trusted partnership moving forward. MVB Bank will remain a Chartwell client," said Larry F. Mazza, MVB CEO.

Chartwell's approximately 60 employees, including Jonathan Abratt and Sherry Tomac of Chartwell's Executive Management team, join Ankura's Global Risk, Forensics & Compliance Group.

"The addition of Chartwell provides Ankura with a clear market differentiator by allowing us to offer banking and Fintech compliance services that are uniquely complementary to our investigations, litigation, and oversight offerings," said Steven Richards, Senior Managing Director and Global Leader of Ankura's Risk, Forensics, & Compliance Group. "We are thrilled to have Chartwell join our Forensics practice, which complements our growth over the past two years beyond the United States into Frankfurt, London, Hong Kong, and Dubai. With Chartwell's further expertise, we'll be able to better service our global clients across borders as the premier firm helping a diverse range of Fintech clients successfully navigate and remain in compliance with existing and emerging regulations."

"My colleagues and I are incredibly excited to welcome Jonathan, Sherry, and the entire Chartwell team to Ankura," said Kevin Lavin, Chief Executive Officer of Ankura. "They have built a strong business and we are confident that they will be empowered to reach even greater heights as part of Ankura. Chartwell and Ankura share a collaborative ethos that is focused on providing the highest quality advisory services to clients, and we look forward to working with our new colleagues as we continue to help clients navigate regulatory complexity."

Davis Polk & Wardwell LLP served as legal advisor to Ankura. Squire Patton Boggs served as legal advisor to MVB Financial Corp.

ABOUT MVB FINANCIAL CORP.

MVB Financial Corp. ("MVB Financial" or "MVB"), the innovative financial holding company of MVB Bank, Inc., is publicly traded on The Nasdaq Capital Market® under the ticker "MVBF." Through its subsidiary, MVB Bank, Inc., ("MVB Bank") and the bank's subsidiaries, MVB provides services to individuals and corporate clients in the Mid-Atlantic region, as well as to Fintech, Payment and Gaming clients throughout the United States. For more information about MVB, please visit ir.mvbbanking.com.

ABOUT ANKURA

Ankura Consulting Group, LLC is an independent global expert services and advisory firm that delivers services and end-to-end solutions to help clients at critical inflection points related to conflict, crisis, performance, risk, strategy, and transformation. The Ankura team consists of more than 1,800 professionals serving 3,000+ clients across 55 countries who are leaders in their respective fields and areas of expertise. Collaborative Lateral Thinking That Delivers, hard-earned experience, expertise, and multidisciplinary capabilities drive results and Ankura is unrivalled in its ability to assist clients to Protect, Create, and Recover Value. For more information, please visit, ankura.com.

ABOUT CHARTWELL COMPLIANCE

Chartwell Compliance, which is now part of Ankura, provides integrated regulatory compliance, state licensing, financial crimes prevention, and enterprise risk management services that include consulting, outsourcing, testing, and training solutions for Fintechs and banks. For more information, please visit chartwell-compliance.com.

FORWARD-LOOKING STATEMENTS

This press release contains forward-looking statements. The statements herein statements are not guarantees of future performance and reliance should not be placed on them. Such forward-looking statements necessarily involve known and unknown risks and uncertainties, which may cause actual performance and financial results in future periods to differ materially from any projections of future performance or result expressed or implied by such forward-looking statements.

MEDIA CONTACTS

For Ankura and Chartwell:
Abigail Ruck / Jesse Rachelle
H/Advisors Abernathy
abigail.ruck@h-advisors.global / jesse.rachelle@h-advisors.global
(212) 371-5999

For MVB:
Amy Baker
abaker@mvbbanking.com
(844) 682-2265

CHARTWELL IS NOW ANKURA

The Life Cycle of a Company with the Secretary of State

By Karen Elliot

When a company determines they want to become a legal entity, the company registers with the Secretary of State in the state they choose as the domestic state. To file, the company will complete and submit Articles of Incorporation. This document is the legal document that becomes public record reflecting the company's information. Within this document a registered agent is named. The registered agent is the local physical address that is required by most states for the company to receive state/government mail and service of process. From there, the company can qualify to do business in other states as deemed necessary or where they are doing business. To file, the company will complete an Application for Certificate of Authority. This document is the legal document that reflects the company information. The company will maintain status by filing the required Secretary of State reports either annually or biannually. Once the company determines they are no longer doing business in a state, they will file documentation to properly close.

A company is required to maintain good standing/active status in the states registered to assure the legal status of the company. To stay in good standing, a company will file a report either annually or biannually. This report is used to update company information, to include business address, mailing address, business purpose, and officer and director details. While some of these updates can be made at any time, the state uses the annual report as the recurring filing used to make these updates. If the company fails to file the required reports, the company will place the company in an administrative status. These statuses include being administratively dissolved, inactive, revoked. When action is taken against a company by the Secretary of State, additional filings are required to bring the company back to good standing.

Should the company fall out of good standing for failure to file an annual report or maintain a registered agent, additional filings will need to be submitted to bring the company back to good standing. Some states will allow a reinstatement. This reinstatement will contain information that is needed for the state to bring the company back to good standing, to include information that was either presented on the legal document or on the last annual report filing. Some states will require all past due reports be submitted, along with the reinstatement. Some states do not allow for reinstatement, but instead, the company will have to re-file as if they were never registered.

When a change happens in the domestic state, typically that same change will need to be recorded in the states where the company is doing business. Some examples are changes to include name, principal address, mailing address, business purpose, officers/directors. Some states require these changes be updated within a certain timeframe; if not, the state will issue a penalty. Other changes include conversions, mergers, and dissolution.

If a company converts (changes the legal entity type), mergers or dissolves in the domestic state, the change also needs to be filed in the states where the company is doing business. For instance, if a company converts from a Corporation to a Limited Liability Company in Delaware and that company is doing business in Alaska, New York, Oklahoma and Texas, the update must also be filed in those states. This is important because the legal entity type must match in all states where the company is registered. The same applies to a merger. If the company merges, the merger updates must be filed in all states where the company is doing business. If the business is ready to wind down, another set of filings should be submitted.

When a company is closing, there are several steps to consider. If the company is closing altogether, filings should take place in all states (where possible) where the company is doing business first. The domestic state would then be closed last, to assure everything is wound down properly. This is done by filing a Certificate of Withdrawal in the states where the company is registered. Some states may also require the company obtain clearance from the Department of Revenue within the state, while other states may require the company file all applicable Secretary of State Annual Reports. Once all of the applicable filings have been approved, the company would then submit a Certificate of Dissolution to the domestic state. This document will close the company in the domestic state, removing all Secretary of State responsibilities, to include maintaining the registered agent and filing annual reports.

We are here to assist with the life cycle of your company and can file all the documents mentioned in this article. Reach out to us if you need assistance or if you have any questions – we are here for everything related to the Secretary of State, and more!

KAREN ELLIOTT, SENIOR ASSOCIATE AT ANKURA has over 17 years of experience in the Public Filings Industry working with the various Secretary of State offices. In addition, for several years Karen also sat on the Board of Directors for the National Public Records Research Association. Prior to joining, Ankura, Karen spent 15 years at Incorporating Services, Ltd as an Assistant Vice President of Client Relations where, together with her team, was responsible for delivering a variety of Secretary of State related activities and services to ensure clients remained compliant with State Department requirements. Karen also spent two years at Capitol Services, Inc. as a Customer Services Representative and Team Lead. For more information, please email Karen at karen.elliott@ankura.com.

Increased Cryptocurrency Enforcement

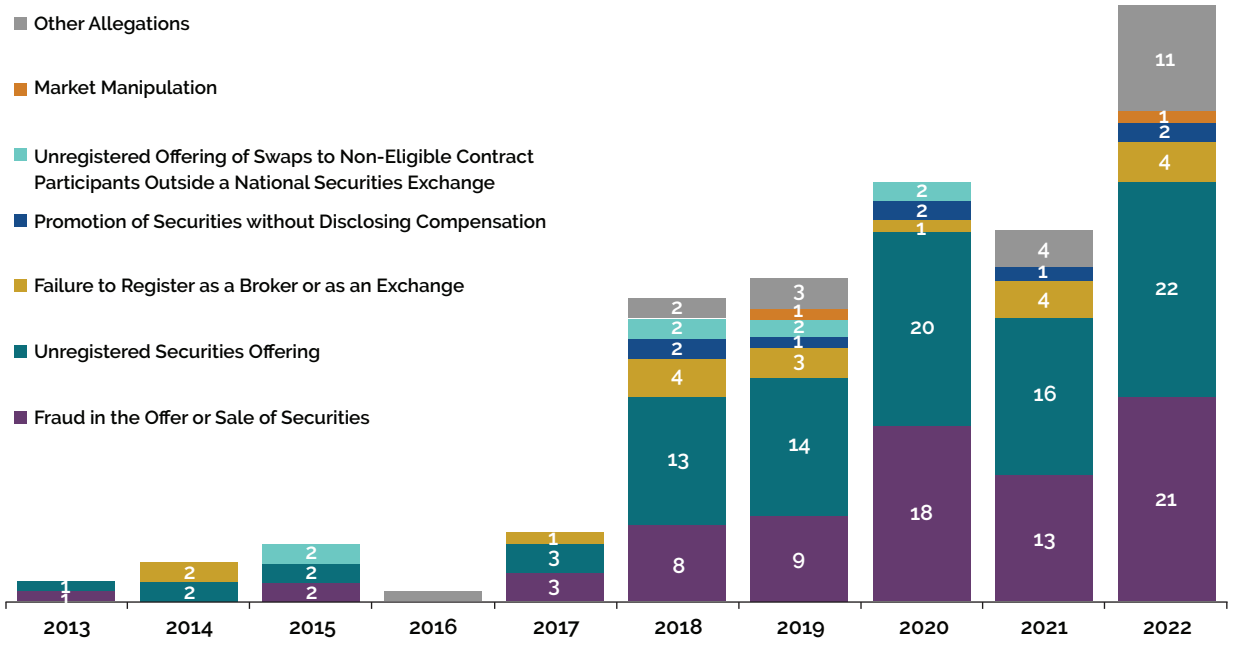
By Austin Briggs

One of the world's largest cryptocurrency exchanges, the famous, or infamous FTX Trading Ltd (FTX) filed for bankruptcy in 2022. Shortly thereafter, U.S. regulators, in particular the U.S. Securities and Exchange Commission (SEC) as well as the Commodity Futures Trading Commission (CFTC) brought to light their investigations of FTX's relationship with its sister entity Alameda Research, the FTX US platform, and its crypto-lending activities, liquidity issues, and mishandled customer funds.

A month after FTX filed for bankruptcy, the SEC released new guidance on December 8, 2022, requiring companies that issue securities to disclose to investors their exposure and risk to the cryptocurrency market. Under the new guidance, companies will have to include crypto asset holdings as well as their risk exposure to the FTX bankruptcy and other market developments in their public filings.

The Securities and Exchange Commission (SEC) charged Samuel Bankman-Fried with orchestrating a scheme to defraud equity investors in FTX Trading Ltd. (FTX), the crypto trading platform of which he was the CEO and Co-founder. Investigations as to other securities law violations and into other entities and persons relating to the alleged misconduct are ongoing. According to the SEC's complaint, since at least May 2019, FTX, based in The Bahamas, raised more than $1.8 billion from equity investors, including approximately $1.1 billion from approximately 90 U.S.-based investors.

The SEC continues to prioritize its cryptocurrency enforcement. In 2022, the SEC administration reported a total of 30 cryptocurrency-related enforcement actions, up 50% from 2021. To put this in context, there have only been 127 total cryptocurrency-related enforcement actions since 2013. The most frequent allegations in cryptocurrency-related enforcement actions remained fraud and unregistered securities offerings as seen below.

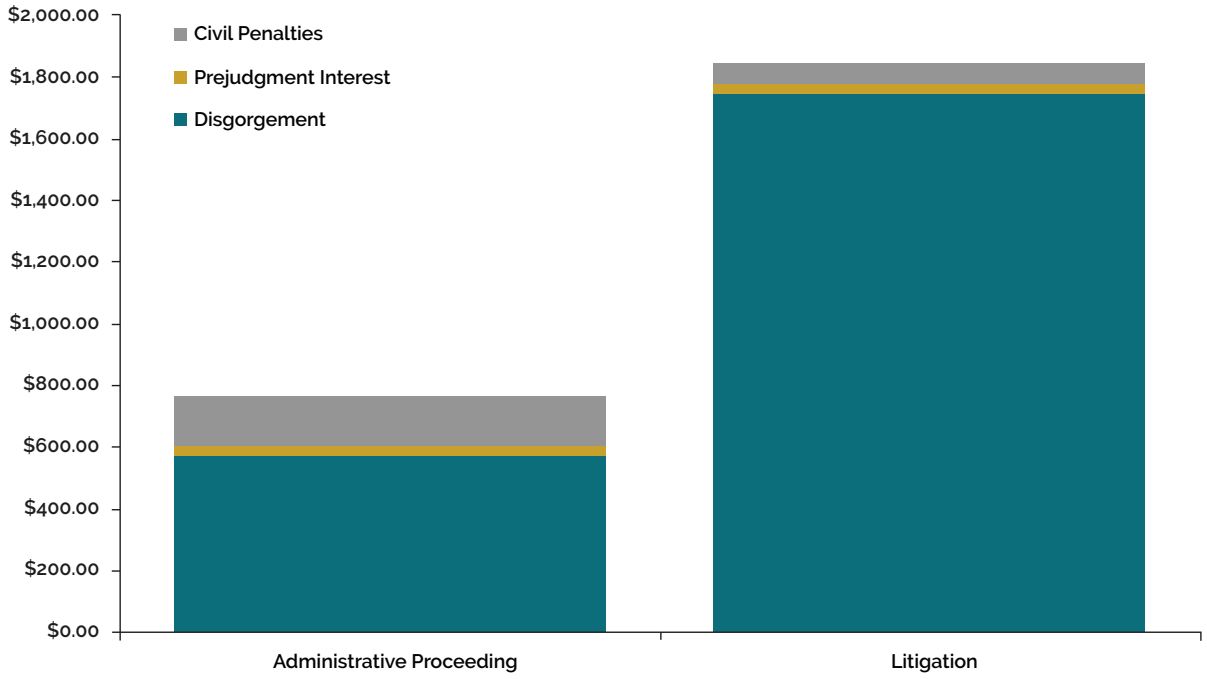


Note: The figure focuses on the total of 127 SEC cryptocurrency enforcement actions (both litigations and administrative proceedings under Section 8A of the Securities Act and/or Section 21C of the Exchange Act). An enforcement action may be associated with more than one allegation. "Other Allegations" include claims that have been alleged in only a few litigations or administrative proceedings, such as violations of restricted period, failure to register as an investment company, fraudulent transactions by investment advisers, failure to maintain internal controls, and falsification of internal controls.

The current SEC Chair, Gary Gensler provided insight into its administration's outlook stating, "There's no reason to treat the crypto market differently just because different technology is used. We should be technology-neutral. . . . We already have robust ways to protect investors trading on platforms. And we have robust ways to protect investors when entrepreneurs want to raise money from the public. We ought to apply these same protections in the crypto markets. Let's not risk undermining 90 years of securities laws and create some regulatory arbitrage or loopholes.".

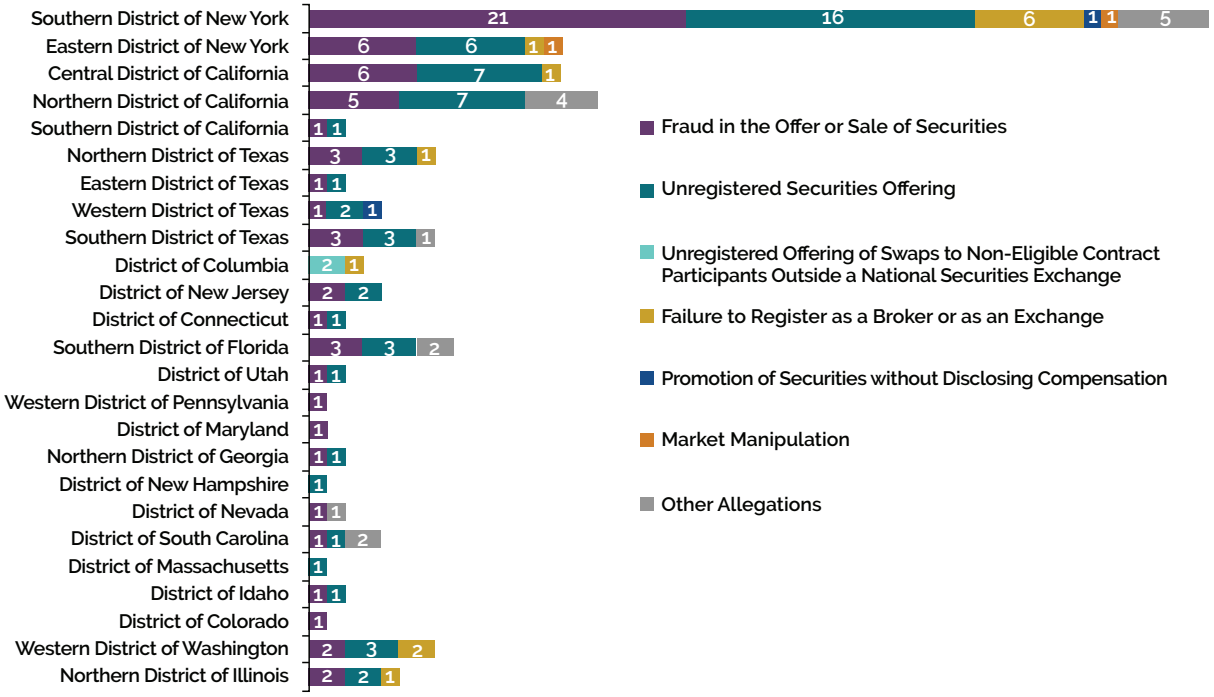
Since 2013, monetary penalties against digital-asset market participants amounted to approximately $2.61 billion. Totaling $242 million in 2022 alone. Please find the total monetary penalties in SEC cryptocurrency enforcement actions below.

2013–2022
Dollars in millions



Source: SEC. gov; PACER
Note: Total monetary penalties are determined as the sum of disgorgement, prejudgment interest, and civil penalties as of December 31, 2022, across all cryptocurrency-related administrative proceedings and litigations. Penalties other than U.S. dollar-denominated amounts (e.g., Bitcoin) are not included.

Although most litigations occur in New York, there has been increased cryptocurrency enforcement actions in other federal courts brought on by the SEC. Below you can see the types of allegations in SEC cryptocurrency litigations by court venue.



Source: SEC.gov
Note: The figure focuses on SEC cryptocurrency litigations. A litigation may be associated with more than one allegation. "Other Allegations" include claims alleged in only in a few litigations, such as a reporting violation, failure to maintain internal controls and records, and falsification of internal controls and records.

The year 2022 was a rollercoaster year for the crypto industry, from the downfall of the FTX empire to its effect on other entities in the crypto ecosystem. Many prominent institutional trading firms, venture funds, and market makers were also adversely impacted by loss of trust in the industry, centralized exchanges, and the liquidity crunch. Moving forward, Federal regulators, including the SEC, and state regulators continue to walk a fine line between maintaining regulatory compliance and controlling illegal activity and cybercrime while still encouraging the development of a growing virtual currency and potentially lucrative digital assets industry.

Our team can assist organizations with the ever-changing Federal and State regulatory environments. With its large team of long-time licensing officers and former Federal and State regulators, We have extensive experience in licensing money transmission, cryptocurrency, prepaid access, currency exchange, lending, and gaming. We also provide Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT), fraud prevention, integrated regulatory compliance, financial crimes prevention and enterprise risk management services, and regulatory compliance services to the Fintech industry.

AUSTIN BRIGGS, DIRECTOR AT ANKURA, has over 7 years of professional experience in the financial services industry with a core focus on managing, completing, and maintaining state licensing applications. Previously, Austin served as a Licensing Supervisor for Evergreen Home Loans, where he managed the company's state licenses. His responsibilities included managing and maintaining over 600 individual mortgage loan originator licenses, 200 branch licenses and 15 company licenses. In addition to supervising the Licensing Specialists, Austin assigned ongoing and daily tasks, provided guidance and facilitated relevant training. For more information, please email Austin at ✉ austin.briggs@ankura.com.

REFERENCES

SEC-Cryptocurrency-Enforcement-2022-Update
chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cornerstone.com/wp-content/uploads/2023/01/SEC-Cryptocurrency-Enforcement-2022-Update.pdf
https://www.sec.gov/litigation/litreleases/2023/lr25616.htm

2023 Money Services Business Call Report Updates

By John Laramie, CAMS

MONEY SERVICES BUSINESS CALL REPORT UPDATE OVERVIEW

In 2023 the Nationwide Multistate Licensing System (NMLS) will implement highly anticipated updates to the quarterly Money Services Business Call Report (MSBCR). MSBs must begin using the revised MSBCR (Version 2) for first quarter reports, due in May 2023. We recommend that MSBs prepare early by updating their accounting and reporting procedures as necessitated by the new format. Version 2 provides functionality improvements for all reporting institutions; however, the updates predominantly display the continued influence of virtual currency on money services regulation, most noticeably revising transaction volume reporting for virtual asset service providers (VASPs). Additionally, the new format includes small, but significant changes in reports of financial condition that may indicate regulatory conflicts in financial supervision of VASPs.

TRANSACTION ACTIVITY REPORTS: CLARIFICATION AND EXPANSION

The MSBCR transaction activity reports, company-wide and state specific, often confound both licensees and regulators. The report provides static definitions and reporting of transaction activity that many firms' products do not conform to, especially for financial

technology companies and VASPs. This creates disparate attempts from both sides to report non-traditional financial services within the provided categories. For VASPs, the absence of reporting fields for common activities, such as loads/deposits of virtual currencies into custodial platforms, often results in virtual currency activities reported as traditional money transmission, stored value, and payment instruments.

Understandably, states' regulators desire reporting of all licensable MSB activity to ensure adequate funding of supervisory programs through assessment fees, as well as accurate economic monitoring and planning. However, the lack of uniformity in MSB licensing and reporting requirements undoubtedly skews planning for financial oversight. States' examiners often cite violations for licensees' "failures" to accurately report transaction volume in MSBCRs. Licensees may attempt to amend past reports only to receive additional examination findings and contradictory reporting recommendations to satisfy other states' preferences.

MSBCR Version 2 attempts to expand and clarify transaction activity reporting for VASPs; however, it will likely require some time for firms to develop and implement new accounting and reporting procedures. We urge all MSBs to review the Version 2 form, become familiar with the transaction activity definitions and instructions, request clarifications if needed, and adapt procedures for calculating and reporting licensed activity volume.

FINANCIAL CONDITION REPORTS: SMALL CHANGES WITH LARGE IMPLICATIONS

The financial condition updates in Version 2 may appear small; however, carry large significance due to the fundamental differences that set VASPs apart from traditional money service providers. Version 1 instructed licensees to report only virtual assets belonging to the institution, often resulting in the exclusion of custodial virtual assets. Version 2 removes that statement from the instructions, implying the inclusion of all virtual assets in the possession of the institution, whether customer or company owned. In complement, the income statement section of Version 2 isolates comprehensive income from net income. Fiduciary institutions report fluctuations in custodial asset values as comprehensive income. Such institutions do not realize these fluctuations as income or losses, but rather, the customers that own the custodied assets realize these gains and losses.

The Version 2 financial condition updates may impact VASPs that operate as a fiduciary of customer assets under management. Such fiduciary relationships may conflict with the expectations of regulators for reporting financial condition through the MSBCR. Institutions that custody funds as a fiduciary commonly omit those funds from financial statements, since US generally accepted accounting principles (GAAP) may deem assets under management as inappropriate to present in their financial statements. Furthermore, financial audits may not consider and validate accounting for custodied assets. Such accounting rules for fiduciaries do not typically apply to traditional MSBs, which begs the question, if the Version 2 comprehensive income applies to a fiduciary institution, should the institution include such custodied assets in financial condition reports at all?

The omission of custodied assets in financial reports also complicates the demonstration of liquidity through permissible investments (PI) reporting. Excluding custodial assets and customer liabilities defies the logic rules of the MSBCR form, which requires reconciliation of liabilities reported in the PI section with liabilities stated in the financial condition section. Licensees can submit MSBCRs with explanatory notes to bypass this logical error; however, this deprives state regulators of visibility into licensees' customer liabilities and liquidity. We recommend that institutions consult experienced legal and accounting professionals to determine appropriate accounting policies. All MSBs should document accounting policies, procedures, and controls for examination by regulators.

States' regulators desire reporting of all licensable MSB activity to ensure adequate funding of supervisory programs ... However, the lack of uniformity in MSB licensing and reporting requirements undoubtedly skews planning for financial oversight.

PREPARATION AND IMPLEMENTATION

For most institutions, Version 2 of the MSBCR provides helpful updates and upgrades to increase efficacy and consistency in reporting. Time will tell whether Version 2 meets the expectations of regulators for the supervision of all licensed institutions. Financial technologies and innovations continue to evolve, and regulatory supervision must adapt to ensure safety and soundness in financial services. MSBs will begin submitting Version 2 for first quarter reports in May 2023, but the reporting period began January 1, 2023. This requires MSBs to align accounting and reporting procedures to the new format. Our team empowers financial institutions with guidance to navigate the complex and evolving regulatory landscape. Our team of compliance professionals provide trusted advice for licensing and registration, development and implementation of policies and procedures, and ongoing maintenance of regulatory requirements.

JOHN LARAMIE, CAMS, SENIOR DIRECTOR WITH ANKURA is the functional lead for the License Maintenance team. With deep knowledge and expertise in Money Service Business (MSB) regulatory compliance, John has over 15 years' experience in organizational development and leadership including program management, governance, policy writing, and training administration. For more information, contact John at ✉ john.laramie@ankura.com.

Licensing Port of Call

Resources for the Regulatory Voyage

Extraordinary, Significant Material Events or Changes

(Out of Cycle Reporting Requirements)

Regulators require advanced reporting and/or approval for material or exceptional events that occur within a licensed institution. Our team provides the tools and expertise to properly submit advanced change notices and approval requests to regulators. If any of the following or similar events occurred, or are planned at your company, contact us to see how we can assist:

- Change of control: such as an acquisition, merger, or other changes in ownership
- New executive officer or board director
- Change in corporate structure
- Change of primary address
- Change of company name or trade name
- Launch of new product or service

Recommended Actions:

- Update procedures to ensure adequate transaction recordkeeping
- Update procedures for calculating and reporting Florida transmission volume
- Update procedures for calculating outstanding virtual currency liabilities and same type permissible investments maintenance and reporting

Alaska Adds Virtual Currency to Money Transmitter Regulations

On August 19, 2022, the Alaska Department of Commerce, Community, and Economic Development proposed changes to money services regulation for public comment. on November 30, 2022, the Lieutenant Governor approved the proposed changes for implementation effective January 1, 2023. We strongly encourage that MSBs review the regulatory changes and update relevant procedures to ensure continued compliance with the State of Alaska.

View the revisions and updates to 3 AAC 13, effective 1/1/2023, here.

Important Updates

"Changes in the Regulatory Tide"

Florida Adds Virtual Currency to Money Services Regulations

In May 2022, the Florida legislature passed House Bill 273, which the Governor approved, revising and updating Chapter 560 pertaining to the regulation of Money Services Businesses. Our team strongly encourages that MSBs review the regulatory changes and update relevant procedures to ensure continued compliance with the State of Florida.

View the revisions and updates to Chapter 560, effective 1/1/2023, here:

Notable Changes for Money Services Businesses:

- 560.103(23) adds virtual currency to the definition of money transmission
- 560.103(36) defines "Virtual currency"
- 560.123(3) adds virtual currency transactions to record-keeping requirements for transactions valued at more than $10,000 in a day
- 560.210(2) requires "same type" permissible investmen for virtual currency obligations

Notable Changes for Money Services Businesses:

- 3 AAC 13.005 adds virtual currency to regulated money transmission activities
- 3 AAC 13.006 requires a license for virtual currency services
- 3 AAC 13.006 voids the previously required Limited Licensing Agreement for virtual currency service providers
- 3 AAC 13.810 requires permissible investments denominated in the "same" virtual currency for virtual currency obligations
- 3 AAC 13.990 defines that "monetary value" includes virtual currency

Recommended Actions:

- Update procedures to ensure adequate transaction recordkeeping
- Update procedures for calculating and reporting Alaska transmission volume
- Update procedures for calculating outstanding virtual currency liabilities and same type permissible investments maintenance and reporting
-

Louisiana Adopts Virtual Currency Businesses Act

In August 2020, Louisiana adopted the House Bill 701, the Virtual Currency Businesses Act, establishing a distinct type of licensure, separate from money transmitter licensure. The Act goes into effect on July 1, 2023, preceded with an initial licensing period from January 1, through June 30, 2023. Virtual currency businesses require state licensure and/or registration to provide services in Louisiana after the effective date.

View the text of Louisiana House Bill 701 here:

View Title 6 Louisiana Revised Statutes, Chapter 21 beginning at RS 6:1381 here:

Notable Requirements under the Louisiana Act:

Licensing and Registration:

- No licensure or registration required to conduct less than a reasonable expectation of $5,000 US dollar value in annual LA VC volume
- Registration only required to conduct less than a reasonable expectation of $35,000 US dollar value in annual LA VC volume
- Application for licensure through the NMLS
- Application fee $5,000
- Initial licensing period begins 1/1/2023
- Apply for licensure on or before 4/1/2023 ensure review before 6/30/2023
- Licensure required to conduct LA virtual currency business beginning 7/1/2023

Surety Bond Requirements:

- Minimum $100,000
- Increases by $100,000 for every $5 million in VC US dollar amount of volume in preceding calendar year
- Maximum $1 million

Equity:

- Tangible Net Worth consistent with CSBS Model Money Transmission Act
- Minimum $100,000
- 3% of total assets
- No maximum

To learn more or if you want to see how Ankura can help you navigate the regulatory waters and a value add to your team contact Richard Davis richard.davis@ankura.com.

Crypto's the future. Don't let fraudsters steal that from you!

By Patricia Lewis

"*I'm much more confident with crypto than with banks or fiat currency because I can actually control it, and the money supply is transparent, stated upfront. It makes online shopping a lot easier and a lot safer.*" This statement was made by Erik Voorhees, the creator of cryptocurrency exchange ShapeShift.[1] While he is correct in that virtual currency does make online shopping a breeze, which of course is great for ecommerce, it is not without its risks. And unfortunately, those risks are unknown to the average shopper or cryptocurrency investor. In today's world of technology, advancement often comes with nefarious individuals who want to take advantage of the unsuspecting shopper or internet user.

Cryptocurrency is often referred to as virtual currency or tokens and was introduced 14 years ago as an alternative to physical currency in the centralized banking system. It is managed on a platform called the blockchain and has an open ledger for recordkeeping, available for all to see. Like it's physical counterpart, cryptocurrency is highly susceptible to fraudsters who will attempt to find vulnerabilities in the system and obtain funds through illegitimate means from victims.

And as cryptocurrency grows in popularity, so does its rate of fraud. According the Web3 Security Report issued by CertiK, a pioneer blockchain security company, and its CEO Ronghui Gu (speaking in regards to fraud), "at $3.7 billion, 2022 is the worst year on record in terms of value lost, far surpassing 2021's $1.3 billion."[2] Therefore, we need to take an active role in fraud prevention and providing education to those wanting to invest in cryptocurrency.

TYPES OF CRYPTO SCAMS

ROMANCE SCAMS

Often seen in traditional banking relationships, romance scams have grown exponentially in the crypto world. Scammers will create fake online profiles and regularly include pictures of attractive individuals taken from the internet. They will study public information victims include in their social media and pretend to share common interests and beliefs. Often, scammers reach out to victims on dating apps or via private messaging on social media platforms. Romance scams are what are considered "long" cons. Once the scammer has developed a relationship with the victim, they will turn the conversation to cryptocurrency and attempt to convince them to send money to help the scammer after an "accident" or "family emergency." Sometimes, the scammer will try to sell the victim an investment opportunity. The scammer is banking on the established relationship that the victim will help them because they believe the relationship is real, despite the fact that the scammer and victim have never met in person. The scammer will always make up reasons why their relationship must remain online, such as they work overseas, are in the military, or travel internationally for work (among other excuses). Also, they will always refuse to meet via Zoom or other video conferencing app.

INVESTMENT SCAMS

With the state of today's economy, everyone is looking for a way to make a few extra dollars. Scammers are taking advantage of that desire by offering investment opportunities that have "guaranteed" high returns. As aforementioned, scammers will reach out to the victims via dating apps or social media platforms, sometimes impersonating love interests or investment managers. They will attempt to convince the victim that the investment has little or no risk and will always earn the victim a lot of money. Some of these situations involve "pump and dump" schemes, where the scammer will try to get the victim to purchase the crypto at what they deem a "low price," with promises that the crypto's value is going to increase and produce a massive windfall. To make the asset appear more enticing, they will often "pump" up the value and popularity of it in order to get multiple investments.

Scammers will also create fake exchanges and advertise cryptocurrency at rates below the market value and promise big returns on their investment. All that is required will often be a high introductory fee. And when the victim attempts to exit the

1 https://blockonomi.com/gleec-coin-exchanges/

2 https://www.certik.com/resources/blog/2aHoafYEoeRguK2gEgfD1s-hack3d-the-web3-security-report-2022

profits they believe they have generated, the company has disappeared or is unreachable.[3]

INITIAL COIN OFFERINGS (ICO)

Scammers often use ICOs as a chance to get money from uneducated investors new to the crypto world. The ICO is fabricated and not include any real information, such as the names of employees or whitepapers published about the coin.

PHISHING SCAMS

Phishing has been a tried-and-true method of fraud that has worked for a long time, in and out of the crypto world. Scammers will attempt to get personal or financial details from the victims through various methods. They often reach out electronically to the victims, sometimes impersonating a legitimate company (ex. Amazon or a financial institution), and entice them to click on a link, webpage, or video. There will either be embedded malware in the links and video or will redirect the victim to a page that is not associated with the legitimate business (but looks so similar to the correct page that the victim does not notice the changes). The malware will steal the victim's private keys for their crypto wallets, their sign-in credentials for exchanges, or other personal information to help the scammer access these platforms. The scammers might also trick the victim into sending money to their wallet, instead of a legitimate one they think they are using.

UPGRADE SCAMS

As technology is always expanding, software is always in the need of the latest patches and updates. This also applies to cryptocurrency exchanges. During these updates, scammers will contact victims and attempt to convince them that they (the scammers acting as the exchange or platform) needs your log-in credentials or private keys in order to complete the upgrade. Sometimes, these scams align with legitimate mergers which are well-known, so victims are often less to question the contact.

SIM-SWAP SCAMS

This is one of the most recent scams out there today involving cryptocurrency. Scammers reach out to the victim's phone carrier and pretend to be them, requesting that the phone number be transferred to a new phone. They often obtain the necessary personal information to impersonate the victim through a separate hack or method. Once they are able to convince the customer service representatives to transfer the phone number to the new SIM card (controlled by the scammer), they are able to access the phone data, such as log-in credentials and downloaded apps (such as social media and financial). In addition, since they now control the phone number, they are able to get around any two-factor authentication requests. This allows the scammer to access the crypto wallets and other accounts, often resulting the theft of the assets before the victim even knows that any changes have been made to their phone number and accounts.

HOW TO AVOID CRYPTO SCAMS

Always check the sender's email address on any communication.

Check to make sure the websites you visit are legitimate (ex. Gogle.com vs Google.com) or that there are not spelling errors in the web information provided to you (by the scammer).

Use bookmarks to visit your financial websites, especially crypto exchanges; do not click on the links in the emails to get to the webpages.

When working with individuals across social media, be sure to thoroughly review their page. Check for how long the account has been created and if they have a consistent history of posts and activity. Be very wary of brand new accounts, with little or no posts, and few followers that are attempting to sell you crypto products.

Do not believe that any investment has no risks or can generate unreasonable returns/profits.

Be cautious of messages from individuals you do not know or individuals you have been communicating with that refuse to meet or even conduct a video call.

HOW TO REPORT CRYPTO SCAMS

If you or someone you know may be a victim of fraud, you can report these scams to the following:

- the FTC at ReportFraud.ftc.gov
- the Commodity Futures Trading Commission (CFTC) at CFTC.gov/complaint
- the U.S. Securities and Exchange Commission (SEC) at sec.gov/tcr
- the Internet Crime Complaint Center (IC3) at ic3.gov/Home/FileComplaint
- the cryptocurrency exchange company you used to send the money

FINAL COMMENTS

At Ankura, we want to do everything we can to protect consumers. We work with companies in various industries, including cryptocurrency, and have experience in cases involving fraudulent actors. If you find yourself in need of advice, or services to protect your company from the ever-evolving world of fraud and security risks, we are here for you. Do not hesitate to reach out to us.

3 https://www.forbes.com/advisor/investing/cryptocurrency/top-crypto-scams/

PATRICIA LEWIS, SENIOR ASSOCIATE AT ANKURA, has over 10 years of investigative and data analysis experience related to financial crimes. Prior to 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. Patricia holds an Associates Degree in Accounting and a Bachelors Degree in Criminal Justice, with a concentration in Economic Crime Investigation. For more information, please email Patricia at ✉ patricia.lewis@ankura.com.

Learning from the Ups and Downs of Cryptocurrency

By Juan Saa

Who would have thought the Crypto world would have evolved so much and so fast since it's introduction to the world in 2009, and with that, that the ever-increasing need for effective measures to combat fraud and corruption, which has been a hot topic in recent years, especially surrounding the events that took place in 2022 starting with Terra USD and its sister token Luna all the way to the collapse of crypto giant FTX. As the industry has grown and the losses from fraud and lack of controls with it, regulators around the world have taken notice, with the U.S. leading the way and thus, many other countries following suit to introduce new crypto compliance regulations, with even at state level taking it upon themselves to introduce heavy compliance requirements. But what does this all mean for the future of companies in the crypto space?

CRYPTO REGULATIONS IN THE U.S.

Cryptocurrency regulation in the U.S. is still relatively new, but it is evolving, and very quickly. The U.S. Securities and Exchange Commission (SEC) has been the primary regulator of cryptocurrencies, with heavy push from other agencies, such as the Commodity Futures Trading Commission (CFTC) and the Financial Crimes Enforcement Network (FinCEN), which have also been involved in the regulatory process.

The SEC, in addition to its focus on protecting investors from potential scams and ensuring that they have access to accurate information, has also worked on creating a more comprehensive regulatory framework by issuing a series of guidance documents that outline the requirements for registering and operating token projects, as well as the requirements for financial intermediaries dealing with Cryptocurrency, while the CFTC has taken a hands-on approach, issuing guidance documents and providing advice on the legal and regulatory requirements for Cryptocurrency derivatives and taken action against companies that have violated these laws, and it does stop there, agencies at the state level such as the New York State Department of Financial Services (NYDFS) has aggressively started to enforce and fine several crypto related companies millions of dollars for BSA/AML and Compliance program deficiencies.

With all these agencies shifting much of their focus to cryptocurrencies, fraud must have come to a stop and with that money laundering and corruption…right? Well, not really.

There were multiple instances of companies that were fined by or settled with regulators in 2022 due to lack Anti-Money Laundering (AML) regulations, pervasive compliance deficiencies, lack of transaction monitoring and anti-fraud controls, cybersecurity deficiencies, insider abuse, and overall lack or regulatory governance, with fines to crypto financial institutions and its employees more than doubling compared to 2021, and the start of 2023 with a total of more than $100 million in fines before January ends. One of the events that caused the most controversy and damaged placed severe lack of trust on crypto financial institutions is the case of FTX. These events have further highlighted a need for enhanced regulation and scrutiny of cryptocurrency, segregation of duties, incorporation and enhancement of BSA/AML, registration, and licensing requirements and pushing for companies to start really doing their due diligence and take a proactive approach towards compliance and detecting fraud. The series of events the past year have shown that what was early on believed to be the technology to end corruption, insider abuse, fraud, and other financial crimes simply is not working and will not work unless agencies, auditor, banks, investors, and even customers are actively on the lookout. So, what now?

Well, with the losses that have taken place for companies and individuals, banks now have started de-risking, and those that have not, are surely trying to play catchup as they see the potential for financial penalties for not following regulatory guidance and having to react and rushing compliance measures, in addition to fines or settlements, the reputational damage, negative public perception, and difficulties raising capital. Sadly, much

which could have been prevented were it not thanks to the historic mentality and approach from companies towards compliance as a last order of business since it is seen as a non-revenue generating business aspect.

WHAT HAVE WE LEARNED, AND CAN IT BE USED TO REBUILD?

I see this as a reboot of the system, it is a way to start fresh again and learn from the mistakes made in 2022 and prior years.

When Crypto discussions took place a decade ago, everyone talked about a decentralized currency, but then if that was the case, then what happened with FTX and Three Arrows Capital? These are core examples of centralization which resulted in millions turning into just smoke and mirrors under the control of fraudsters.

Regulatory oversight was something controversial and challenged constantly but had there been clear regulation in place and adequate programs, perhaps a lot of what happened would have either been come to light early on or been prevented, instead everyone was late to the show where millions were defrauded from investors and consumers.

Anyone can make blatant remarks, offer products that make no sense, offering beyond incredible interest rates, or promise gains, but as with all reasonable and safe investments, and people forgot that if something sounds too good to be true, it usually is.

From all of these comes the learning part, and most importantly learning from a crypto finance company and compliance perspective how to prevent these events from repeating themselves.

Companies will need to challenge themselves and rise to the expectations of consumers, the regulators, and potential sponsor banks which are now going to be paying close attention as they too become responsible for compliance deficiencies.

STARTING WITH A STRONG FOUNDATION

Companies entering or currently in the crypto market should look at their program to determine if at minimum they have the following:

- Strong risk management: Implement robust risk management systems and procedures to identify and mitigate potential issues before they become a problem
- Adequate compliance: Ensure that the company follows all relevant laws and regulations in the countries where it operates, including anti-money laundering (AML) and know-your-customer (KYC) requirements and that your compliance department is well qualified in these areas
- Robust security measures: Implement strong security measures to protect against hacking, theft, and other cyber threats. This can include things like two-factor authentication, multi-signature wallets, and regular security audits
- Transparency: Be open and transparent with customers, partners and regulators about the company's business practices, and provide clear and accurate information about the company's products and services

Strong governance: Ensure that the company has strong governance and internal controls in place, including a Board of Directors that is independent and has the necessary expertise to oversee the company's operations.

Strong customer support: Provide strong customer support to help customers navigate any issues and to build trust and loyalty.

Continuous review and improvements: Regularly review the company's policies and procedures and make improvements as necessary to ensure they align with the industry standards, regulations, and best practices.

"Regulatory oversight was something controversial and challenged constantly but had there been clear regulation in place and adequate programs, perhaps a lot of what happened would have either been come to light early on or been prevented"

In addition, here are a few of the cryptocurrency fraud trends that companies need to ensure they have adequate systems and controls in place to detect and prevent:

- Money Transfer Scams: Scammers often trick victims into transferring money to their own wallet. This is often done through convincing individuals to change their bank details or through fake payment services
- Phishing Attacks: Phishing attacks involve sending emails or messages that contain malicious links or attachments. If clicked, these links or attachments can install malicious software (Malware) and/or steal personal information
- Fake ICOs: Initial coin offerings (ICO) are becoming increasingly popular, but unfortunately, so are fake ICOs. Fake ICOs often have websites that look legitimate but are instead designed to steal investors' money by luring them to invest into these ICOs which promise outlandish returns but are usually nothing more than a Ponzi scheme or fraudulent investment
- Pyramid and Ponzi Schemes: Pyramid and Ponzi schemes involve paying higher members of the pyramid with money from lower members. Such schemes are illegal and can lead to financial losses for members involved

Pump and Dump schemes: These schemes involve bad actors buying a large number of low-priced cryptocurrencies and then artificially inflating the price through social media marketing and other tactics. When the price has gone up, the bad actors then sell their holdings at a large profit, leaving the investors with worthless coins.

Pig Butchering: - includes a sophisticated new twist that combines a romance scam with an investment spin. According to the Federal Bureau of Investigation (FBI), the term "pig butchering" refers to a time-tested, heavily scripted, and contact intensive process to fatten up the prey before slaughter. This scam is predominately executed by a ring of cryptocurrency scammers on dating apps and social media sites in search of victims as an evolved version or romance scams that gets the victim to invest in crypto.

Market manipulation: Bad actors may use malicious bots to artificially manipulate the price of cryptocurrencies, or even to spread false news about certain coins to manipulate their prices.

Fake cryptocurrency wallets: Cybercriminals may design fake cryptocurrency wallets that look like the real thing but contain malicious code. Victims may end up downloading malware or giving away their private keys, which can lead to loss of funds or a compromised security system.

These are just the tip of the iceberg on list of things that partner, or sponsor banks and investors will start to look at more closely as everyone realizes the array of risks that come with crypto. What was once early on believed to be safe, due to the decentralized, self-compliant currency in a way due its undisturbed audit trail that would force everyone to play by the rules, has turned out to be just as if not riskier than fiat currency without the proper technology and programs in place to supervise. Banks, regulatory authorities, and individual investors have realized there is plenty of work to be done before being able to trust crypto businesses and ensuring everyone involved is doing the right thing and being held accountable.

With innovation come risks and learning, and 2022 proved there are still plenty of risks from an operational standpoint with cryptocurrencies and banks may take some time to regain trust in how companies are operating and managing risks and for public perception to change

CRYPTOCURRENCIES: "What was once early on believed to be safe, due to the decentralized, self-compliant currency in a way due its undisturbed audit trail that would force everyone to play by the rules, has turned out to be just as, if not riskier than fiat currency without the proper technology and programs in place to supervise. "

HELPING YOU PREPARE FOR A COMPLIANT FUTURE

Cryptocurrency regulation is an ever-evolving landscape, and it is important for companies to stay up to date on the latest developments. Our team provides is an organization that promotes regulatory compliance and has the expertise to prepare new and existing companies, to stay informed, keep up to date with the latest developments in virtual currency regulations by monitoring relevant government websites, industry associations, and legal publications. We work every day to develop a compliance program to aid investor protection, KYC/AML compliance, and anti-fraud measures by assisting with creation and implementation of policies, procedures, and controls to ensure compliance with existing and future regulations. This can include things like conducting regular internal audits, training employees on compliance policies, establishing cross company relationships to ensure you have the appropriate technology, vendors, and systems necessary and develop contingency plans in case of regulatory enforcement actions or other legal challenges.

It is worth noting that regulations and compliance requirements can vary widely depending on the jurisdiction, so it is important for virtual currency companies to become aware of the specific regulations and changes to come in the countries or regions where they intend to operate and help prevent another year like 2022 for the crypto markets.

JUAN SAA, ASSOCIATE AT ANKURA, has over eight years of BSA/AML, fraud, and sanctions experience. Prior to joining Ankura, Juan worked at Robinhood as a Fraud Investigator with a special focus on regulatory inquiries and escalated cases as a result of internal and external referrals involving account takeovers, elder financial exploitation, and potential self-harm claims. Prior to Robinhood, Juan worked at Franklin Templeton as an AML and Fraud Analyst overseeing U.S. registered mutual funds and was responsible for BSA/AML compliance, fraud investigations, regulatory filings, as well as sanctions screening. While still at Franklin Templeton, Juan was promoted to Senior AML and Trade Compliance Analyst overseeing outside broker-held products registered in Luxembourg and South America. He was responsible for high-risk jurisdictions ensuring proper enhanced due diligence, KYC and proof of regulation for clients and introducing dealers were in place. Juan also assisted as a consultant for the operations and sales divisions for client onboarding. For more information, please email Juan at juan.saa@ankura.com.

OFAC SENSITIVITY TESTING:

What Your Organization should Consider to Effectively Test its OFAC Screening Software Programs

By Trisha Shirey, CBAP

It is no secret that Office of Foreign Assets Control (OFAC) recommends that organizations take a risk-based approach when implementing and/or updating their Sanctions Compliance Program (SCP), but what exactly does that mean, and how do organizations tie everything together and feel confident about their OFAC screening processes and software programs?

Although there is limited guidance on sensitivity testing, it has become more of a focus during model validations, so it is important to understand what an organization can do to complete the testing in the most effective and meaningful way to support its OFAC risk appetite documented in the OFAC Risk Assessment, and work with vendors when gaps have been identified. There are several components that an organization should review and consider prior to conducting OFAC sensitivity testing. Those include, but are not limited to, data quality, understanding the customer base and foreign presence, products and services offered, and volumes of transactions and the various payment channels they flow through. Let's look at each component and take a deeper dive in how each should be considered while preparing to conduct sensitivity testing.

DATA QUALITY – GARBAGE IN, GARBAGE OUT

Data quality is pivotal in all monitoring for BSA/AML/OFAC related functions. If the data input into the software program is garbage (not complete, valid, accurate, or consistent), the output from the software is going to be faulty. It is essential to understand how the various data sources are being ingested into the software program, and to have internal controls in place to mitigate consequences of incomplete and inaccurate data input. Any gaps identified in data quality will impact OFAC screening results, including high false positive rates and potential violations. If gaps are identified, it is important to include sensitivity testing related to those gaps to identify the root cause and impact, which may include exposure to regulatory violations and penalties.

KNOW YOUR CUSTOMER BASE AND FOREIGN PRESENCE

Knowing your customers and understanding the geographical location of your customer base as well as your organization is an important component when conducting sensitivity testing. Your organization's current OFAC Risk Assessment should identify customer and geographical risks. Your organization should review its OFAC hits on foreign individual names and entities, and the related sanctions to understand the specific risks. Identified risk areas should be considered when gathering sample testing data specific to your organization's customer base and potential OFAC risk.

PRODUCTS AND SERVICES

Organizations should identify the products and services that pose heightened sanctions risk and include them in the OFAC Risk Assessment. Understanding products and services offered will aid in identifying gaps and limitations of the sanctions

screening software. Those gaps and limitations should be considered when conducting OFAC Sensitivity Testing.

VOLUMES OF TRANSACTIONS AND PAYMENT METHODS OFFERED

It is important for organizations to understand and analyze their customer's foreign transactional activity and conduct thorough testing related to the geographical locations of those foreign transactions. Sensitivity Testing should include jurisdictions based on the organization's actual transaction data. Organizations should utilize their OFAC Risk Assessment to identify these risks.

Thoroughly performed and documented OFAC Sensitivity Testing will detect the OFAC risks and allow the organization to appropriately mitigate and limit any exposure to OFAC violations and penalties.

An in-depth analysis will allow your organization to understand and create a balance between false negatives and false positives and provide support for current set thresholds and configurations so that they align with the Bank's risk appetite.

TESTING AND ANALYSIS

Testing should be conducted based on various degradation methods such as concatenation, soundex/phoenetic/multilingual name differences, adding punctuation(s), adding/removing text character, word(s) separating, etc. The risk exposure should be considered based on the likelihood of failure in the tested category and sanctions screening software not triggering an alert. For example, what is the likelihood that someone can input a name on a wire and concatenate it so there is no spacing, but the name is 100% name match otherwise: Mohammed Akram vs. MohammedAkram. This scenario should likely be considered a high-risk test category. It is imperative for your organization to understand the variances in which the sanctions screening in place will not generate hits.

The analysis should be conducted to identify the degree of degradation in which the system does not return expected results and the degree in which there is an increase in false positives. The Pass Rate (Match/Pass Percentage) for each set of degradations should be considered (count of true hits divided by count of names sent for each degradation category). An in-depth analysis will allow your organization to understand and create a balance between false negatives and false positives and provide support for current set thresholds and configurations so that they align with the Bank's risk appetite. This process will also identify test categories that your organization would consider high risk that the screening software does not generate alerts on and may support decreasing thresholds. If there are potential gaps identified, it is important to have a process in place to communicate and work with your vendor to get resolution. There may be gaps that are low risk considering your customer base and products and services offered. The testing, analysis, and results should be documented and approved by management.

Remember, OFAC is risk based! Thoroughly performed and documented OFAC Sensitivity Testing will detect the OFAC risks and allow the organization to appropriately mitigate and limit any exposure to OFAC violations and penalties.

TRISHA SHIREY, CBAP, DIRECTOR AT MVB BANK, has over 11 years of experience in financial services, deposit operations, BSA/AML Compliance, and fraud detection and is an experienced operator in the Fintech as well as Fintech Compliance industries. Trisha is considered an expert in Verafin software for transaction monitoring. Working daily with the system for many years has allowed her to gain great knowledge of all Verafin's intricacies, making for successful implementations and enhancements for transaction monitoring across a range of financial products. For more information, please email Trisha at ✉ tshirey@mvbbanking.com.

MORE THAN JUST CHECKING THE BOX:

How proactive FinCrime compliance can speed up time to market and foster innovation

By Tobias Schweiger, CEO & Co-Founder, Hawk AI

Compliance is often seen as a bottleneck to growth, particularly for the banking and Fintech industries where time-to-market is key. However, this is a shortsighted perspective. Any business looking beyond 12 months can and should use compliance as a key driver of growth and innovation.

Building a proactive compliance mindset, no matter your business maturity, will set a foundation of sustainable growth and innovation. This establishes trust and creates an accelerator instead of a bottleneck, while at the same time reducing costs and preparing for increasing regulatory scrutiny. This scrutiny can slow down growth drastically, to the point of being destructive to the business at hand.

ESTABLISHING AND CEMENTING TRUST

Establishing trust with potential partners, and customers is crucial, as reputation can be quickly tarnished. A dedicated and rigorous adherence to compliance is one of the most effective ways to signal the robustness of a business. Risky partners can have disastrous consequences for entire industries; see the recent FTX collapse (among others) and its global impact across the crypto industry. It's important to begin building a positive reputation early on, as it's much easier to do so from the start than to try and regain trust after a violation has occurred.

RESPONDING TO INCREASING REGULATORY SCRUTINY

Although young Fintechs may have less stringent compliance requirements to begin with, regulators will scrutinize them more closely as they grow. But it's not just growth that attracts scrutiny, external factors beyond your control also play a significant part. U.S. regulators clearly indicated Anti-Money Laundering is a priority with the Anti-Money Laundering Act of 2020. In Germany, the regulator BaFIN has responded to weaknesses that helped the Wirecard fraud scandal take place by increasing oversight. Many European Fintechs are now feeling the pressure, which will only continue as fincrime becomes more complex. Taking a proactive approach to compliance is wise, as many compliance items are long-term plays, and it's better to be prepared for future needs. The adage "an ounce of prevention is worth a pound of cure" strongly applies to compliance.

CREATE A GO-TO-MARKET ACCELERATOR

A lack of agility in compliance can impede business operations, but a proactive approach can actually speed up progress. Financial institutions don't want to wait six to nine months to launch products or new businesses because they're waiting for the compliance go-ahead; they want to turn things on and capture the market with the competitive advantage they've crafted.

To maintain agility and avoid overburdening compliance teams, financial institutions should implement processes and systems that can quickly adapt to changing regulations.

START WITH THE RIGHT TOOLS TO AVOID HEADCOUNT PRESSURE AS YOU SCALE

Proactively adopting compliance technology that aligns with your goals is crucial for sustained success. While a top-of-the-line solution isn't necessary initially, it's important to consider technology that can grow with your business requirements. Investing in the right tools can prevent unnecessary cost escalation, and relying solely on personnel isn't a viable strategy to combat financial crime. Your tools should become more precise, not less, as your business expands.

Fincrime compliance is a necessary part of any financial business, whether directly through regulation, or via expectations of partners and customers. If it's here to stay, businesses of all sizes would do well to consider the opportunity it offers.

TOBIAS IS THE CEO & CO-FOUNDER OF HAWK AI, which develops and operates a cloud-based software platform for the automated detection of suspected cases of financial crime and money laundering. Tobias was Vice President Operations at ACI Worldwide's SaaS unit and before that CFO/COO at PAY.ON AG, which was sold to ACI for $200 million in 2015. Tobias' previous positions include Senior Vice President Finance Operations at ProSiebenSat.1 Media SE and Roland Berger Strategy Consultants. He started his career in product management and engineering at mobile operator Telefonica O2.

National Multistate Licensing System & Registry

NMLS CORNER

NMLS Policy Guidebook Updates Available

An updated version of the NMLS Policy Guidebook has been posted to the NMLS Resource Center and the Regulator Resource Center. Click here to view a summary of the updates.

MSB Call Report Form Version Update

The NMLS Money Services Businesses (MSB) Call Report will be upgraded to Form Version 2 on April 1, 2023. The new form version will be effective starting with the first quarter 2023 MSB Call Report filing. For more information, see the Form Version 2 section of the Money Services Businesses Call Report page of the NMLS Resource Center.

State News from NMLS:

NMLS Annual Renewal Ends Dec. 31 - Reinstatement Period Begins Jan. 2, 2023

NMLS annual renewal ended Dec. 31, 2022, at midnight ET. The reinstatement period will begin Jan. 2, 2023, and end Feb. 28, 2023, at midnight ET.

If you are a state licensee who missed the renewal period, visit the Annual Renewal page here on the NMLS Resource Center to find out if your state agency participates in a late renewal or reinstatement period. Select your state from the dropdown list under Step 3 – Review Deadlines, Requirements, and Fees to get further details.

Louisiana Adds New License Types to NMLS on January 1

NMLS is receiving new applications for the Louisiana Office of Financial Institutions. New applicants and will be able to submit these records through NMLS for the following license types:

- Virtual Currency Business Activity License
- Virtual Currency Limited Activity Registration

Applicants are now able to view the license requirements on the State Agency Licensing page for the Virtual Currency Business Activity License and Virtual Currency Limited Activity Registration

Starting January 1, the Louisiana Office of Financial Institutions will begin receiving new Electronic Surety Bonds (ESB) through NMLS for the following license type:

- Virtual Currency Business Activity License

The Virtual Currency Business Activity License and Virtual Currency Limited Activity Registration authorize Virtual Currency Exchanging and Trading Services. Both NMLS Checklists are similar, however, the Virtual Currency Limited Activity Registration covers Virtual Currency Exchanging and Trading Services not to exceed thirty-five thousand dollars annually.

Who is required to have a The Virtual Currency Business Activity License?

Pursuant to LSA-R.S. 6:1384, "a person shall not engage in virtual currency business activity, or hold itself out as being able to engage in virtual currency business activity, with or on behalf of a resident unless the person is one of the following:

(1) Licensed in this state by the department pursuant to R.S. 6:1385.

(2) Registered with the department and operating pursuant to R.S. 6:1390.

(3) Exempt from licensure or registration pursuant to R.S. 6:1383."

LSA-R.S. 6:1383 (22) defines, "Virtual currency business activity" as any of the following:

(a) Exchanging, transferring, or storing virtual currency or engaging in virtual currency administration, whether directly or through an agreement with a virtual currency control services vendor.

(b) Holding electronic precious metals or electronic certificates representing interests in precious metals on behalf of another person or issuing shares or electronic certificates representing interests in precious metals.

(c) Exchanging one or more digital representations of value used within one or more online games, game platforms, or family of games for either of the following:

(i) Virtual currency offered by or on behalf of the same publisher from which the original digital representation of value was received.

(ii) Legal tender or bank credit outside the online game, game platform, or family of games offered by or on behalf of the same publisher from which the original digital representation of value was received.

Activities Authorized Under This License

This license authorizes the following activities…

Virtual Currency Exchanging and Trading Services

NMLS Initial Processing Fee
LA License/Registration Fee: $5,000

- Virtual Currency Limited Activity Registration

Who Is Required to Have This License?

Pursuant to LSA-R.S. 6:1389, a person whose volume of virtual currency business activity in United States dollar equivalent of virtual currency will not exceed thirty-five thousand dollars annually may engage in virtual currency business activity with, or on behalf of, a resident under a registration without first obtaining a license.

Activities Authorized Under This License

This license authorizes the following activities…

Virtual Currency Exchanging and Trading Services, which will not exceed thirty-five thousand dollars annually.

NMLS Initial Processing Fee
LA License/Registration Fee: $750

Illinois Department of Financial and Professional Regulation Advises Licensees About Phishing Scam

The Illinois Department of Financial and Professional Regulation is aware of a phishing email that looks like an email from IDFPR. The email asks you to click a link to "complete your most recent up to date membership license certificate" and states that licensees must do so within 24 hours to avoid a license suspension.

The email comes from an email account not affiliated with IDFPR. If you receive an email like this, do NOT click any links and delete the email. If you have questions about the authenticity of an email from the Division of Banking or Division of Financial Institutions, please email IL.Banks@illinois.gov or FPR.DFI.Director@Illinois.gov.

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.

We are pleased to welcome the following individuals to the team.

Kay Toscano, CRM, CAFP

Director - Federal Compliance

Kathryn ("Kay") is a Director with Ankura and brings more than 30 years of audit, risk and compliance, including BSA, AML and Fraud experience to the team. Kay is a compliance, risk management and audit professional with extensive experience in the financial services sector. She has a significant understanding of key banking processes, associated risks, and remediation procedures and sound ability in audit and internal control management.

Keith Brown

Associate – Banking Compliance

Keith Brown is a Analyst with Ankura and has over six years of BSA/AML compliance experience focusing primarily on AML and fraud investigations. Keith has worked in various investigations roles with several financial institutions, such as PNC Bank, Aerotek – Wells Fargo and Barclays Bank.

Vick Ekizian, CAMS, PMI-RmP, CCFI

Director – Global Outsourced Compliance

Vick bring over 13 years' experience serving in various regulatory compliance and business control functions in the public and private sectors. He has had the opportunity to work in a variety of institutions honing his experiences in banking, cross-border payments, cryptocurrency, and regulatory examination and supervision. Vick has a diverse skillset centered around helping financial institutions build, maintain and comply with consumer and financial crimes compliance programs.

Samantha Heim, CAMS

Associate – Banking Compliance

Samantha "Sam" Heim is a Banking Analyst with Ankura and has over five years of experience in BSA/AML Compliance focusing on SAR reporting, Transaction Monitoring, Fraud Detection, and Quality Control. Prior to joining, Sam was a Quality Control focused Senior Analyst with AML RightSource LLC where she worked closely with several national and global financial institutions to assist in internal quality control of SAR reports related to money laundering, fraud, and identity theft.

Risk, Forensics & 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 effective 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:

- Internationally prominent U.S. payments licensing and compliance advisory outsourcing practice
- The Regulatory Divisions of the California Department of Business Oversight and the Floria Office of Financial Regula-tions
- MSBs such as Western Union, First Data, and Sigue
- State and nationally chartered banks
- The Federal Bureau of Investigation's Financial Crimes and Terrorist Financial Crimes and Terrorist Financing
- Assistant director at the Office of the Comptroller of the Currecy (OCC) Assistant Director of Enforcement

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 staff have serviced, worked at, or supervised a statistically significant portion of all licensed U.S. money transmitters.

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.

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.

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.

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

Through its subsidiary, MVB Bank, Inc., and the Bank's subsidiaries, MVB Community Development Corporation, and Paladin, 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.

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.

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.

CHARTWELL IS NOW ANKURA

Culture and Honors

Team Retreat 2023

Our team came together in San Juan, Puerto Rico to collaborate, understand how we can better serve our clients, and engage in team building activities.

In Memoriam

Shannon Rice

1978–2022

"Shannon burned a very incandescent and bright light."
—Jonathan Abratt

PHOTO:
Puget Sound, WA, where Shannon loved to fish with her family

Subscribe Today

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

SIGN UP

We are honored to be recognized by the following organizations:

RECOGNITION HELIOS HR APOLLO AWARDS™ WINNER

CorporateLiveWire 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

CHARTWELL IS NOW ANKURA

485 Lexington Ave, New York, NY 10017 | chartwellcompliance.com