APRIL 2025

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 Petra Hrachova, CRCM, CAMS & Jonathan Abratt

AI in Action: Leading the Charge Against Financial Crime

The world of financial regulation is on the cusp of a major transformation, with Artificial Intelligence (AI) taking a leading role in Bank Secrecy Act (BSA) compliance. This shift has been gradually building over decades, starting back in 1993 when the Financial Crimes Enforcement Network (FinCEN) first used its Artificial Intelligence System (FAIS) to spot potential money laundering. Now, three decades later, AI is set to revolutionize how we monitor BSA activities.

AI's Impact on Financial Crime Prevention

AI is no longer a device of the future; it's here and already making a big difference. The Department of the Treasury's 2024 strategy highlights AI's essential role in fighting financial crime. Recently, the Treasury's Office of Payments Integrity announced that it had recovered over $375 million in fraudulent funds thanks to AI-enhanced processes. This demonstrates AI's ability to analyze huge amounts of data, identify risks, and support decision-makers. As fraudsters increasingly use AI, it's crucial for financial institutions to adopt similar strategies to keep pace, if not find ways to get ahead.

On January 21, 2025, the White House announced the creation of "Stargate," a partnership, comprised of OpenAI, SoftBank, Oracle, MGX, Microsoft, NVIDIA, and Arm, that plans to invest $500 billion in AI infrastructure in the U.S. The "Removing Barriers to American Leadership in Artificial Intelligence" Executive Order, issued on January 23, 2025 by President Trump, replaces previous Executive Order 14110 from October 30, 2023. The new directive marks a notable transition from the Biden administration's focus on oversight, risk management, and equity, toward a strategy that emphasizes deregulation and fostering AI innovation to uphold U.S. leadership on the global stage.

> **"AI is no longer a device of the future; it's here and already making a big difference."**

AI in AML: Beyond the Basics

AI's role in Anti-Money Laundering (AML) extends beyond its well-known applications, such as handling sanctions alerts and negative news monitoring. Advances in AI agents and refined prompting techniques are revolutionizing how we interact with these systems, enabling more complex tasks to be executed with greater speed, precision, and flexibility. However, human oversight remains essential. While AI can document processes and decisions, it currently lacks the nuanced judgment required for compliance in financial institutions. Transparency and oversight are key to addressing AI's challenges – while automation can streamline and document complex processes, human expertise is vital for guiding and validating AI's outputs. This ensures accuracy and builds trust among regulators, banks, companies, and consumers alike.

This is where Ankura sets itself apart. We lead the industry with both the resources and expertise to fully harness AI's potential-leveraging Large Language Models (LLMs) to transform complex outputs into easy-to-understand formats and enhancing the human review processes for greater accuracy and efficiency.

Moreover, as AI continues to shape the regulatory space, user-friendly interfaces are essential for making AI more approachable and easier to integrate into existing workflows. A well-designed interface allows users to interact with AI intuitively, reducing resistance to adoption and ensuring seamless implementation. By prioritizing usability, financial institutions can make AI tools accessible to all users, regardless of technical expertise, ultimately driving greater efficiency and adoption.

The Future is Now - Introducing AI AML Analyst

We are at a pivotal moment—30 years after the introduction of FAIS, AI is set to redefine BSA monitoring. With AI leading the way, the future of compliance has never been more promising, and as regulatory expectations evolve, adopting AI today will ensure your institution remains competitive, agile, and ready for the next era of financial crime prevention.

Ankura's AI AML Analyst is at the forefront of this transformation, empowering financial institutions to embrace the future. Ankura's AI AML Analyst is designed to revolutionize compliance operations by managing sanctions, transaction monitoring alerts, and strengthening Know Your Customer (KYC), Know Your Business (KYB), and Enhanced Due Diligence (EDD) processes. Built to streamline compliance and drive efficiency, it empowers institutions to stay ahead of regulatory demands by leveraging AI to enhance BSA compliance—while preserving the critical human oversight needed for documented decision-making.

Designed and developed to seamlessly integrate with existing workflows, Ankura's AI AML Analyst is more than just automation. AI AML Analyst transforms AML processes by combining the power of AI with essential human oversight. It can be tailored to an organization's unique needs, ensuring compliance operations are not only more efficient but also aligned with specific goals and regulatory expectations. By streamlining compliance operations and reducing manual workloads, it allows teams to focus on high-value oversight and critical decision-making.

Now is the Time to Act

For financial institutions, the imperative to adopt AI is undeniable. By transitioning from legacy systems to innovative AI-driven solutions, financial institutions fundamentally transform BSA compliance. Easily integrated and tailored to your organization's unique needs, Ankura's AI AML Analyst provides the technology and tools needed to significantly enhance compliance and boost operational efficiency.

SOURCES

1 https://home.treasury.gov/system/files/136/2024-Illicit-Finance-Strategy.pdf

2 https://home.treasury.gov/news/press-releases/jy2134#:~:text=WASHINGTON%20%E2%80%93%20Today%2C%20the%20U.S.%20Department,beginning%20of%20Fiscal%20Year%202023.

3 https://www.cnn.com/2025/01/21/tech/openai-oracle-softbank-trump-ai-investment/index.html

4 https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/

FOR MORE INFORMATION CONTACT

Petra Hrachova, CRCM, CAMS

Managing Director at Ankura

✉ petra.hrachova@ankura.com

Petra brings over 20 years of experience in compliance, CRA, and BSA officer at community banks, a regulator, and as a consultant. Prior to joining Ankura, Petra worked as a Senior Assistant Bank Examiner at the Federal Reserve Bank routinely helping with supervisory activities for community and regional state member banks. Petra's experience includes starting a de novo bank, where she successfully created and managed compliance, BSA and credit administration programs and where she became knowledgeable of all functional areas of banking.

At Ankura, Petra works with large and small money service businesses including Fintechs and provides expertise in consulting, AML Risk Assessments and Compliance Programs development. She also leads BSA/AML/OFAC independent reviews and performs validation of transaction monitoring systems. Petra also worked on developing and updating the online compliance training modules for a large online training provider.

Petra's current focus is on providing regulatory consulting to banking clients, specifically guidance related to Fintech business lines, remediation plans and establishing Fintech regulatory compliant programs.

FOR MORE INFORMATION CONTACT

Jonathan Abratt

Senior Managing Director at Ankura

✉ jonathan.abratt@ankura.com

Jonathan is a seasoned executive and industry leader with over two decades of experience in payments, fintech, compliance, and risk management. He helps financial institutions, fintechs, and high-growth businesses navigate complex regulations, optimize operations, and implement strategies for sustainable growth.

At Ankura, Jonathan focuses on regulatory compliance, risk management, fraud prevention, and financial disputes, working with clients to mitigate risks and enhance resilience. Previously, as President & COO of Chartwell Compliance, he co-led the firm's rise to become North America's leading fintech compliance advisory and outsourcing provider.

Jonathan's expertise spans alternative and traditional payments, fraud prevention, money transmission licensing, FX and cash flow management, business risk consulting, and IT audit. With leadership roles at Zapper, Pariplay, and 888 Holdings (now Evolve plc), he brings a results-driven approach and a passion for building operationally sound, compliant financial ecosystems.

By Erik Kemme

Challenges in Data Sharing Between Banking Partners

Life in the United States and most modern industrialized countries is driven primarily by data. Google alone processes 20 Petabytes of data every day (1 petabyte = 1 million gigabytes).[1] Economies are built on data; marketing strategies are given life through data. However, a sector that continues to lag behind in the data-driven world of tomorrow is Banking, and in particular how Banks and their business relationships fail to leverage their collective data in their Bank Secrecy Act / Anti-Money Laundering (BSA/AML) Compliance programs.

A good example of where Banks can improve their use of, and sharing of, collective data is the growing Fintech sector. Fintech Banking in the United States has been a steadily increasing sector of the financial world, with the number of Fintech companies in the USA rising from about 4,000 in 2014 to over 10,000 in 2023.[2] Representing transactions in the hundreds of billions of dollars every year, these Fintech companies, often offering banking services to customers young and old, are increasingly concerned with convenience and buzz terms like "frictionless onboarding," which often equates to being able to open a Checking or Savings account with little more than a name and a Social Security Number.

While there are certainly advantages to being able to serve one's customers with as little of an intrusion into their lives as possible, one of the casualties of this shift to Fintech Banking and the use of Neo-Banks has been efficiency and efficacy in the way these partnerships handle AML/BSA Compliance.

For banks, a partnership with a successful Fintech company can be a match made in heaven. The bank, eager for new accounts and deposits, is willing to allow the Fintech to use accounts managed and operated by the bank for the Fintech's customers, particularly as the bank is typically not liable for any losses sustained by those accounts due to fraud or misuse. Instead, those losses are passed to the Fintech partner as an operating loss.

Google alone processes 20 Petabytes of data every day.

Meanwhile, the bank's deposits and account volume skyrocket. The Fintech, eager to offer near-instantaneous banking options (and the associated fees), needs the bank because it needs accounts through which to operate. One would then assume, given the mutual benefit of the arrangement, that collaboration and data sharing would abound! This is typically not the experience for BSA Compliance departments and consultants, and often information must be requested on a customer-by-customer basis. The result is that time, and money, are wasted in efforts coordinating information and data sharing between banking partners, such as providing the partner bank crucial Know Your Customer (KYC) information or promptly warning a partner bank of possible illicit or suspicious behavior. If a Bank allows transactions to move through their accounts on behalf of a Banking Partner, and this results in an average of 2,000 alerts being generated each month on the Bank's side of the relationship, and 1,200 of them require Requests for Information because the Bank does not have access to the data it needs to investigate, this can result in hundreds of hours of unnecessary work every month, just because the partners have not found an efficient way to share information.

Traditional Banks are not immune to the effects of ineffectual data sharing. In the world of money laundering, layering is the act of moving illicit funding via several smaller pieces, typically to obfuscate the source and movement of the funds should they be scrutinized, or to avoid scrutiny altogether. This naturally includes the movement of these funds between separate institutions, done because bad actors are well aware of the lack of transparency between different financial institutions. If a fraudster wishes to cloud the trail of illicit funding they are introducing into the system, they need only move the funds between multiple banks, typically employing multiple names at each. If they manage to avoid thresholds for reporting or detection for even some of those accounts, the lack of information sharing between banks would make the coordinated effort of one person (or group of people) slip through the cracks, with only a portion of suspicious activity ever having been noticed or reported.

While there is a current system in place for the reporting of suspicious activity and data sharing between financial institutions, typically referred to as 314b requests, the program is completely voluntary, which is apparent after even a cursory view of associated statistics. For reference, the number of Suspicious Activity Reports (SARs) filed with regulator FinCEN in 2023 totaled about 4.6 million, but the number of SARs which referenced information received via 314b was less than 30,000. This works out to less than 1% of all SARs filed during the year, which anyone who has worked in BSA/AML Compliance will tell you is woefully low given the reality that a significant majority of money laundering will employ multiple avenues of fund movement through multiple financial institutions.

It is clear from these numbers that utilization of 314b data-sharing requests between institutions is negligible at best and is hampered by its voluntary nature. There are consequences, expensive ones, when these gaps are not addressed. In December 2024, the Consumer Financial Protection Bureau (CFPB) levied suit against Zelle (P2P payment processor), as well as three large Banks (Bank of America, Wells Fargo, and JPMorgan Chase) which are part owners of Zelle's parent company Early Warning Services (along with additional owners Capital One, PNC Bank, Truist, and US Bank). The suit alleges these entities allowed customers to lose more than $870 Million to fraud, all while not sufficiently implementing controls to prevent customers from being victimized. Zelle may be a Fintech, but a Fintech owned and controlled by large banks representing a vast pool of data and knowledge. Deficiencies at the highest levels betray the systemic consequences of poor data sharing and coordination efforts across the financial spectrum.

As financial institutions continue to fight for deposits and compete with increasingly frictionless means of fund transfer (cryptocurrency, P2P payments), the increased need for data and information gathering and sharing will be paramount, as well as new technological advances such as AI to interpret the meaning behind the numbers at scale. In 2023 Stripe, one of the most successful Fintech companies currently, processed $640 Billion in payments, and the Finance as a Service industry has been estimated to climb to over a trillion dollars per year by the early 2030's.[3] Zelle itself, despite its flaws and regulatory obstacles, still processed $481 Billion in transfers in the first quarter of 2024 alone.[4] With an incoming administration in the White House which has signaled a bullish attitude towards virtual currency, Fintech companies and neo-banks will continue to proliferate and the activity they process will become increasingly decentralized and complex. Banks that want to compete and thrive in this era need to educate themselves and understand that increased data sharing and information fluidity between Banks and Banking Partners will keep their customers safer, keep their BSA Compliance costs down, and allow them to scale their programs without the concern of regulatory gaps which may cost them significant financial and reputational losses.

SOURCES

1 https://skill-lync.com/blogs/how-google-handles-over-40000-petabytes-of-data-on-a-daily-basis#:~:text=Google%20has%20built%20one%20of%20the%20largest%20and%20most%20sophisticated,be%20stored%20and%20protected%20securely. Accessed 12/23/2024

2 https://www.statista.com/statistics/1476784/us-number-of-fintechs/#:~:text=The%20number%20of%20fintechs%20in,compared%20to%20the%20previous%20year. Accessed 12/20/2024

3 https://www.globenewswire.com/news-release/2024/10/22/2967018/0/en/Fintech-as-a-Service-Market-Set-to-Reach-USD-1305-7-Billion-by-2032-Driving-Growth-through-Technological-Advancements-and-Increased-Adoption-of-Digital-Financial-Solutions-Research.html#:~:text=In%202023%2C%20Stripe%20processed%20over,to%20enhance%20their%20service%20offerings. Accessed 12/20/2024

4 https://www.azcentral.com/story/money/business/consumers/2024/12/23/zelle-scottsdale-based-operator-sued-consumer-financial-protection-bureau/77174045007/. Accessed 12/23/2024.

FOR MORE INFORMATION CONTACT

Erik Kemme

Director at Ankura

✉ **erik.kemme@ankura.com**

Erik Kemme is a Director with Ankura and has over 7 years of experience in BSA/AML Compliance focusing on KYC, Enhanced Due Diligence, Transactional Monitoring, Fraud Detection, and Quality Control.

Prior to joining Ankura, Erik was a Senior Analyst with compliance consultancy firm AML RightSource LLC where he worked closely with several financial institutions to assist in international wire monitoring and beneficial ownership verification for domestic and international technology startups, as well as enhanced due diligence, transactional monitoring, and risk assessments in the consumer banking space. Erik was also deeply involved in training new analysts, identifying and providing solutions for issues arising from independent testing and internal quality control, as well as communication with clients and additional third-party resources.

The Right Experts at the Right Time Responding to the Increased Global Risk of Financial Crimes

Petra Hrachova
Managing Director

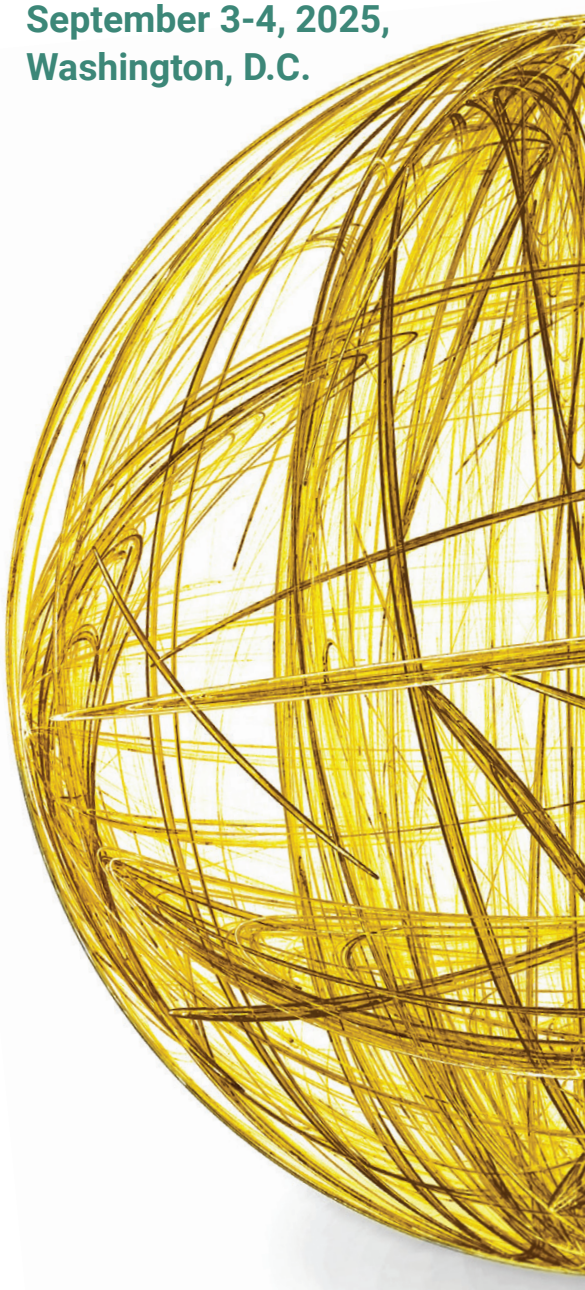
Omar Magana
Managing Director

Kay Toscano
Senior Director

Lauren Ceniviva
Senior Director

PBC conference 2025

September 3-4, 2025, Washington, D.C.



ankura™

PROUD GOLD SPONSOR

By Austin Briggs

An Update on the CSBS Money Transmission Modernization Act (MTMA)

The financial landscape is rapidly evolving, with digital payment solutions becoming increasingly integral to both consumers and businesses. Amidst this shift, the Money Transmission Modernization Act (MTMA) emerged as a pivotal legislative framework, aiming to harmonize the regulatory environment for money transmitters across the United States.

The MTMA was developed by the Conference of State Bank Supervisors (CSBS) in collaboration with state regulators and industry experts. Approved in August 2021, this model legislation establishes a cohesive set of nationwide standards, focusing on net worth (capital), surety bonds, and permissible investments (liquidity) requirements. Its primary goal is to modernize the supervision and regulation of money transmitters, offering a streamlined and consistent approach that mitigates the regulatory burdens previously experienced by these entities due to disparate state laws.

As of January, 41 states have enacted the MTMA, either in full or partially.

As of January, forty-one states have enacted the MTMA, either in full or partially, marking significant progress towards national uniformity. This widespread adoption is crucial, as money transmitters licensed in at least one state adhering to the MTMA now account for 99% of reported money transmission activity. This indicates a substantial shift towards a more unified regulatory framework that facilitates easier multi-state operations for license holders and reduces fragmentation across state lines.

The MTMA introduces several transformative elements:

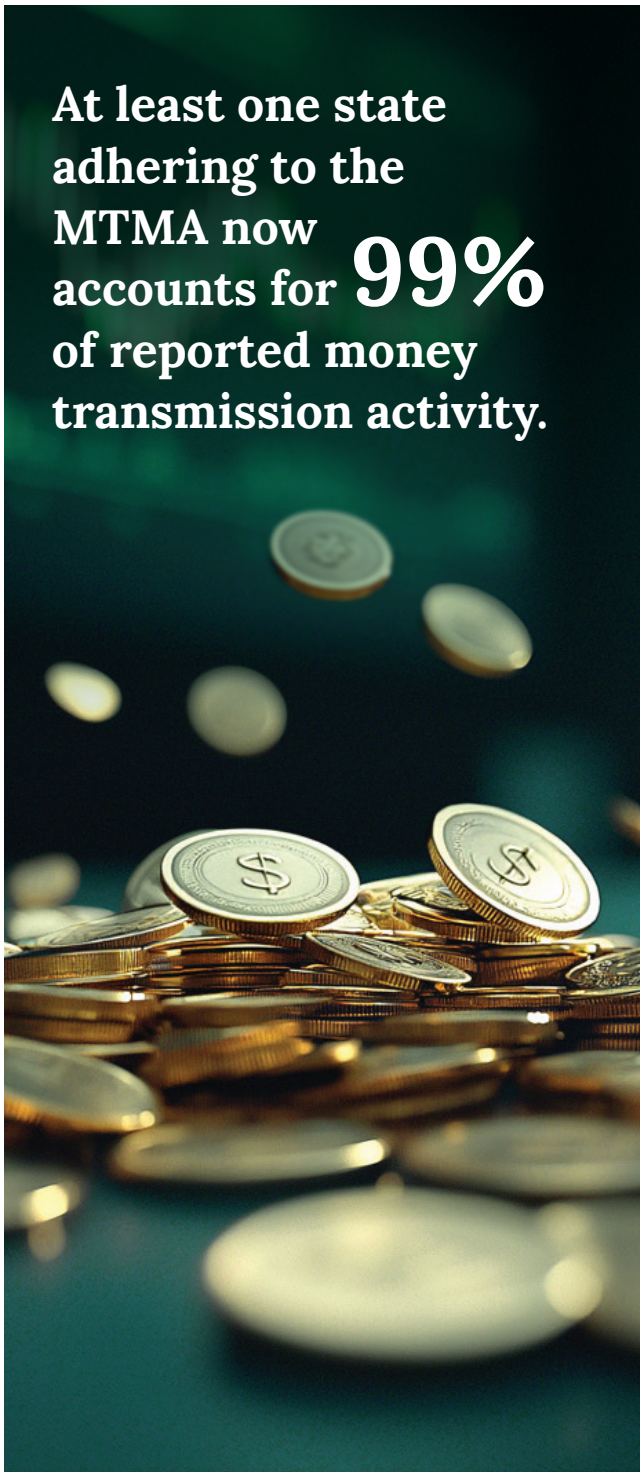
- **Uniform Standards**
  By aligning capital, surety bond, and liquidity requirements, the MTMA ensures that money transmitters operate under consistent safety and soundness prerequisites.
- **Streamlined Licensing Process**
  The Act standardizes the process for licensing money transmitters, incorporating thorough screenings of owners, officers, and directors, and setting out specific exemptions from licensing requirements.
- **Multi-state Supervisory System**
  This system significantly reduces the complexity of operating across multiple states, allowing businesses to expand more efficiently and effectively.
- **Enhanced Consumer Protection**
  By mandating customer disclosures and regulating recordkeeping and reporting, the MTMA enhances transparency and trust within the industry.

The adoption of the MTMA has not been uniform across all states. Some states have fully integrated the Model Act, while others have selectively incorporated its provisions, leading to varied interpretations and applications. This variation can still pose challenges for compliance, as companies must navigate a landscape that, while more cohesive than before, still requires state-by-state consideration.

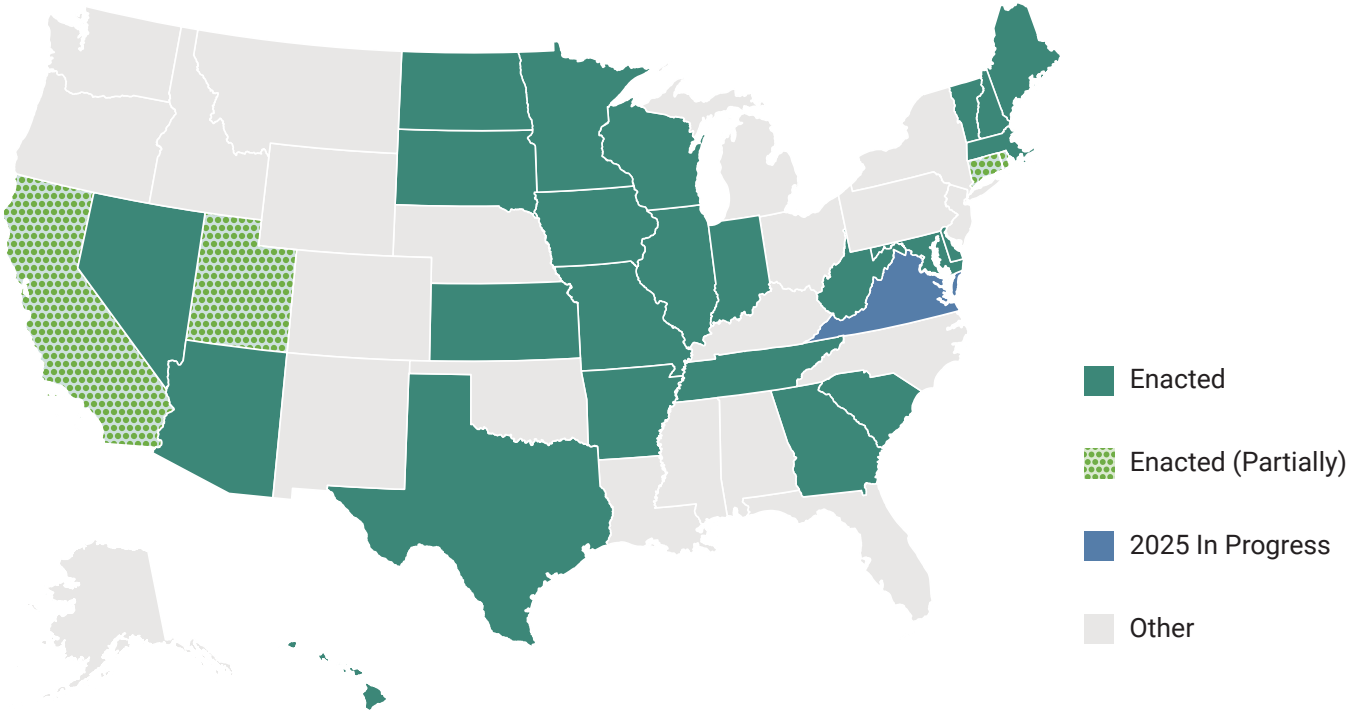
Moreover, the regulation of virtual currency remains a contentious area. The MTMA includes optional provisions for virtual currency regulation, but not all states have embraced these aspects, resulting in a patchwork approach to this growing sector.

The MTMA represents a significant step forward in the regulation of money transmitters, promising to streamline operations and foster growth within the financial services industry. As more states continue to adopt and refine their implementation of the Act, it is expected that the regulatory environment will become increasingly conducive to innovation and expansion.

For companies in the payments and financial technology sectors, staying informed about ongoing developments and maintaining a robust compliance strategy will be essential to navigate this evolving landscape effectively.



Money Transmission Modernization Act Adoption Status Map (Updated 1/15/2025)



SOURCES

1 CSBS Money Transmission Modernization Act (MTMA)
https://www.csbs.org/csbs-money-transmission-modernization-act-mtma

2 US States Adopt Model Money Transmission Act, but Harmonization Remains Elusive
https://www.cooley.com/news/insight/2024/2024-08-20-us-states-adopt-model-money-transmission-act-but-harmonization-remains-elusive

FOR MORE INFORMATION CONTACT

Austin Briggs
Director at Ankura
✉ **austin.briggs@ankura.com**

Austin brings over eight years of professional experience in the financial services industry with a core focus on managing, completing, and maintaining state licensing applications.

Prior to joining Ankura, 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.

Austin received a Bachelor of Science in Sociology from Arizona State University.

By Sherry Tomac, PMP

Five Reasons Experience is Essential to Obtaining Money Transmission Licenses

In the fast-paced world of business consulting, when it comes to choosing a consultant to secure money transmission licenses, experience offers significant advantages. Here are five reasons why seasoned expertise prevails:

1. **Deep Industry Insight**
   Our team, with an average of over 20 years of experience in the money services business (MSB) sector, provides unparalleled insight. This depth of knowledge enables us to anticipate and navigate regulatory challenges with finesse, offering solutions that are informed by years of real-world experience.

2. **Proven Success Record**
   We have successfully guided over 600 financial technology and financial services clients through the licensing process since 2011. These companies range from the Fortune 50 to fintech's biggest unicorns throughout the world. Our track record is a testament to the effectiveness of human expertise. A nuanced understanding of the complex regulatory environment helps us empower businesses to stay compliant.

3. **Strategic Relationships**
   Our long-established relationships with key regulators are a strategic asset that can not easily be replicated. These alliances streamline the licensing process and provide a significant edge, ensuring that our clients benefit from a process that is efficient.

4. **Personalized Service**
   We offer a high-touch, bespoke approach that addresses each client's unique needs with precision and care. Our personalized concierge service means that each project is tailored to fit our clients' goals and objectives, not just generically applied.

5. **Comprehensive Compliance Mastery**
   Our team's extensive experience means we do not just understand compliance—we live it. We expertly navigate the ever-changing regulatory landscape, ensuring that businesses remain ahead of the curve. Our professionals provide the foresight and adaptability that comes with seasoned expertise.

> **“Our strategic relationships with key regulators and personalized, high-touch service give your business an elite competitive edge.”**

In conclusion, the depth of experience and reliability provided by seasoned professionals is essential for money transmission licensing. In fact, experience is not just beneficial, it is essential. Choose a partner that delivers proven expertise and a personalized touch, ensuring your business not only meets regulatory demands but excels in navigating them. Experience the difference with our expert team, where insight and tailored service elevates you to reach your business goals.

FOR MORE INFORMATION CONTACT

Sherry Tomac

Senior Managing Director at Ankura

✉ **sherry.tomac@ankura.com**

Sherry Tomac, Senior Managing Director at Ankura, leads a team of compliance consultants on state licensing engagements and oversees Kaizen process improvements. She has over 20 years of experience managing global projects at Western Union and First Data, focusing on strategic goals like software rollouts and compliance. Sherry also worked at Ernst & Young as an auditor and business consultant for seven years. She is passionate about process improvement, using lean and six sigma tools to enhance operations and reduce waste.

Sherry holds a Project Management Professional (PMP) certification and a Six Sigma Black Belt. She has trained with Toyota Production System Lean Kaizen experts in Japan. Originally from St. Louis, MO, she graduated with a BS in Business Administration from the University of Missouri and moved to Highlands Ranch, CO, 20 years ago.

By Jake Hines

Living the Future Now: How **AI is Shaking Things Up** in Financial Services

AI is no longer a futuristic concept – in fact, it is actively reshaping financial services today, and has been for some time! From fraud detection to more personalized banking, AI is not just a tool, but a strategic driver of transformation in the industry! AI is evolving at an incredible pace - by the time you finish reading this, something will probably have changed - but even in its current state, AI is transforming financial services today.

With use cases ranging from risk management to personalized services, AI is fundamentally reshaping how financial institutions operate on the backend and how they engage with customers.

AI is transforming financial services, setting the stage for a new era in banking.

What are some of the key ways AI is being implemented in financial services today?

1. **Risk Management & Fraud Detection**
   AI's ability to analyze massive datasets in real-time is game-changing for identifying fraud patterns. Machine learning models detect anomalies in transactions, flagging suspicious activity faster than any human could. And since fraudsters are already finding new and creative ways of leveraging AI, financial institutions need to keep current with their technological prowess to keep up.

2. **Credit Risk Assessment**
   AI can help predict defaults by analyzing historical data with almost startling accuracy. This can be leveraged to assist with informed decision-making in lending and reduce financial risk to lenders. With time and proper training, AI can even help to minimize bias that has historically marred the lending space for underrepresented and underserved communities.

3. **Customer Service & Personalization**

   AI-powered chatbots and virtual assistants can now handle everything from routine inquiries to complex transactions, freeing up skilled human agents to focus on higher-value tasks. While some customers may prefer human interaction, AI enhances efficiency and provides 24/7 service. As these AI assistants continue to develop their ability to handle complex financial interactions with near-human precision, they might someday become barely decipherable from their human counterparts - aside from the seemingly encyclopedic knowledge.

   AI-driven personalization is also advancing financial services, offering tailored recommendations based on customer behavior, preferences, and financial goals. Spending patterns, customer habits, and other data can help to determine which financial products customers need, sometimes before they even realize it.

4. **Algorithmic Trading & Investment Management**

   While AI has long been used in investment management, today's AI-powered trading algorithms can execute high-frequency trades in milliseconds - much faster than human traders! These systems continuously learn and adapt to market conditions, providing an edge in investment strategies. AI is helping investors keep up with an uncertain world where the market can turn on a dime.

   Robo-advisors are another major development, offering cost-effective, AI-driven financial planning without the need for human advisors. Some customers even prefer interacting with AI instead of having to disclose sensitive financial details to a person. In addition, AI has opened up investing to those who previously lacked a clear point of entry, whether because of affordability or a lack of understanding, and can create more equitable opportunities in the space.

5. **Regulatory Compliance & Reporting**

   AI is being implemented to help automate compliance reporting, processing legal documents, and flagging potential regulatory risks with incredible efficiency. For example, it can identify even subtle patterns of bias in lending and ensure institutions remain compliant with rapidly evolving regulations. We all know that compliance can be expensive, making AI particularly valuable for smaller firms and enabling them to scale without massive compliance overhead. AI also levels the playing field, allowing innovative financial startups to compete more effectively, whereas before, they may never have gotten off the ground.

So, what is the broader impact on financial institutions?

The benefits of AI in financial services are substantial:

- **Increased Efficiency & Cost Reduction**
  Automating routine tasks saves time, resources, and money while allowing institutions to scale operations without proportional overhead increases. This is game-changing for startups, especially as new and innovative financial products are hitting the market.

- **Better Decision-Making**
  AI processes huge amounts of data to provide deeper insights, improving customer acquisition and retention, risk assessment capabilities, and portfolio management for both businesses and their customers.

- **Enhanced Customer Experience**
  While AI-driven interactions have historically received mixed reactions, personalized services and faster response times ultimately boost customer satisfaction and loyalty. The better the technology becomes, the better it can be leveraged to benefit the customer experience - and that is a win for everyone!

But how can a consultant help my business with AI integration?

Many financial institutions are still determining the best ways to implement AI. That is where consultancy comes in. Experienced Ankura consultants can help to:

- **Identify AI Use Cases**
  We can help assess operations to pinpoint areas where AI can drive innovation or reduce costs. No two companies are the same, so there are often unique ways to leverage the burgeoning technology.

- **Develop an AI Integration Strategy**
  From selecting the right tools to aligning AI initiatives with long-term goals, we can help you plan to ensure smooth AI adoption.

- **Manage Organizational Change**
  AI is not just a technical challenge—it is a whole cultural shift! Employees must understand how to work alongside AI rather than fear job displacement, and trust has to be built around the decision-making capabilities of AI.

- **Ensure Data Strategy & Ethics**
  AI models require high-quality data to be effective. Consultancy firms can help businesses structure data properly while navigating valid and serious ethical concerns like bias, transparency, and regulatory compliance.

AI sounds great, but there must be concerns, right?

Despite its many advantages, AI in financial services comes with some challenges and concerns, which should not be taken lightly:

- **Data Privacy & Security**
  AI's effectiveness truly depends on data, making security and compliance top priorities. In a data-driven world, data protection must be a top consideration for any financial provider planning to integrate AI into their business.
- **Trust in AI Decision-Making**
  Financial providers must ensure proper levels of transparency and explainability, particularly in areas like lending and investment management. This is especially important as AI-assisted decision-making must be able to stand up to regulatory scrutiny.
- **Regulatory Uncertainty**
  While the U.S. is still shaping AI regulations, the European Union is moving quickly. AI implementation needs to conform to both AI-specific regulations (which many states are actively pursuing) and the institution's financial compliance requirements. Compliance frameworks must evolve alongside these changes, which can be a tricky path to navigate.
- **Job Market**
  AI is already having an impact on the job market. There will be a careful line to walk in implementing tools to aid human experts to ensure that AI is not used, especially in the time needed to bridge the gap between leaps in technological advancements and regulatory oversight. Generally, providers seem to be navigating this well, but as the excitement of lower costs and more efficient processes grows, there may be companies that jump the gun on replacing human workers with AI - and this could have ramifications down the line on both economic and regulatory fronts.

What does the future of AI in financial services look like?

AI is no longer futuristic – it is here -- and while it has been revolutionizing the financial ecosystem for years, we have only scratched the surface. Financial institutions will need to balance innovation with risk management, and they will need to leverage the guidance of experts in both technology and compliance to navigate this landscape.

Who knows what the industry will look like in a year, or even a decade? What is certain is that AI's role in financial services will only continue to expand, as will the level of scrutiny applied in the oversight process.

At Ankura, we specialize in helping financial institutions implement AI responsibly by balancing innovation, compliance, and risk. Let us discuss how AI can create real value for your organization!

FOR MORE INFORMATION CONTACT

Jake Hines
Director at Ankura
jake.hines@ankura.com

Jacob (Jake) Hines, Director at Ankura, brings nearly 10 years of experiene 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 aiding in various other regulatory compliance functions.

By Leonardo Pinzon Echeverry, CAMS

Financial Crime in the Illegal Wildlife Trade

What does the silent extinction of endangered species reveal about the hidden corridors of global finance? As financial transactions and environmental health become increasingly linked, a troubling reality emerges: **illegal wildlife trafficking has become a conduit for money laundering**. A single dollar, originating as payment for illicitly traded wildlife, interlaces through an intricate network of international financial institutions and digital currencies before re-entering the economy as 'clean' money. **This is a challenge many prefer to ignore**.

From the depths of remote jungles, where endangered species fight for survival, to the high-tech corridors of global finance, criminal networks are blurring the lines between environmental destruction and financial crime. For compliance officers, financial executives, and Fintech professionals, understanding this intersection is not just about regulatory compliance; it is about responsibility. These professionals are at the frontline of preventing financial systems from being exploited for environmental crimes.

> **"Illegal wildlife trafficking becomes a conduit for money laundering, exploiting global financial systems"**

A Sophisticated Crime Meets Modern Finance

Illegal wildlife trafficking has evolved into a highly organized, transnational operation that leverages modern financial technologies, the **INTERPOL**[1] **reports illegal wildlife products worth up to USD $20 billion per year**, poaching, and the illegal wildlife trade have become a significant area of activity for organized crime groups and are increasingly linked with armed violence, corruption, and other forms of organized crime. The World Economic Forum (WEF)2 paints a stark picture: between 2015 and 2021, **approximately 81% of illegal trade seizures in 162 countries and territories involved plants and animal species**.

Digital currencies and blockchain, while heralding a new era of financial services, have also provided criminals with powerful tools to obscure the origins of illicit funds. This digital camouflage makes it increasingly difficult for regulators and financial institutions to track suspicious transactions. In the relentless scroll of **social media, images of exotic pets flash 24/7, subtly conditioning viewers to accept wildlife ownership and inadvertently driving demand** for the illegal pet trade, creating a lucrative market for traffickers.

Authorities like **FinCEN** have recognized this growing threat. In response, they have issued guidelines such as **FIN-2016-G003: "Advisory to Financial Institutions on Wildlife Trafficking,"** which highlights red flags and suspicious patterns banks should monitor. The **Bank Secrecy Act (BSA) (31 U.S. Code § 5318(h))** also requires institutions to report transactions that may be linked to wildlife trafficking. But these regulations are only effective if compliance & risk professionals and institutions take a proactive approach to enforcement.

The Urgent Need for Enhanced Monitoring

Financial institutions now face a dual challenge. On one hand, they are expected to drive financial innovation through AI and digital currencies; on the other, they must prevent their systems from being exploited by criminal enterprises. This challenge is exacerbated by the reality that the illicit wildlife trade commodifies the world's biodiversity.

To combat this, institutions are investing in advanced, risk-based monitoring systems. By leveraging artificial intelligence and blockchain analytics, banks can detect anomalies such as unusual transaction volumes or sudden shifts toward digital currency use. These tools, combined with strong Know Your Customer (KYC) & Enhanced Due Diligence (EDD) protocols and continuous staff training, form the backbone of a proactive defense against laundering funds derived from wildlife trafficking.

The internet has become a marketplace for illegal wildlife trade, but IFAW3 has been fighting back since 2005. In 2019, they partnered with Baidu to create **the AI Guardian of Endangered Species** (AI Guardian), a sophisticated AI that scans online platforms for illegal wildlife products. With an 86% accuracy rate, AI Guardian is proving to be a game-changer in the fight against this insidious trade

The Journey of Illicit Profits

In a secluded African reserve, a rhino falls victim to a well-orchestrated poaching operation. As its horn is discreetly removed, the illicit profits begin a hidden journey, moving through offshore accounts, shell companies, and digital wallets before fueling a vast global network of financial crime.4 This is not fiction; this is the harsh reality of how environmental devastation and financial crime are intrinsically linked, **impacting over 4.000 animal and plant species**[5]. This may not be in the news or your social media trends, but is there making each illegal transaction a direct attack on our natural heritage.

Red Flags in Wildlife Trafficking

As global trade surges, it is impossible to inspect every shipment or transaction. Instead, financial institutions, law enforcement, and regulators rely on identifying suspicious patterns. Key red flags include:

Operational Red Flags	Wildlife Trade Red Flags
Transactions structured just below reporting thresholds (smurfing) to bypass financial monitoring.	Use of vague or generic product descriptions traffickers may mislabel items to evade detection (e.g., labeling ivory as 'bone carvings' or exotic skins as 'leather goods').
Unrelated individuals or entities funding payments to a vendor, raising concerns about hidden buyers.	Suspicious trade routes wildlife products traveling through non-traditional or indirect routes, possibly indicating smuggling.
Always apply enhanced due diligence (EDD) on hard-to-value commodities—used goods, artwork, rare wildlife products, and exotic plants are often exploited for laundering.	A company primarily engaged in one industry (e.g., textiles) suddenly begins dealing in wildlife products without a logical reason.
Mismatched invoices, unexplained markups, or discrepancies between bills of lading and payment records, indicating trade-based money laundering (TBML).	Frequent reliance on Free Trade Zones (FTZs) if goods are declared in an FTZ but never officially leave, it may indicate smuggling or fraud.
Businesses operating in seemingly unconnected industries—such as a construction company also trading luxury watches or rare animals.	A mismatch between declared weight and shipment contents—a discrepancy between paperwork and actual goods.
Entities with opaque ownership structures or those registered in secrecy jurisdictions, often serving as fronts for illegal trade.	Unusual trade patterns or high-risk commodity sales involving endangered species or protected materials.

Beyond Regulation: A Call for Cross-Sector Collaboration

Addressing wildlife-linked financial crime requires more than regulatory compliance; it demands active collaboration across sectors. NGOs with deep environmental expertise, such as the **World Wildlife Fund** (WWF)[6], provide critical intelligence that bridges fieldwork and regulatory oversight. Governments, businesses, and **financial institutions must work together** to share data, utilize legal frameworks like 314(a) and 314(b) provisions in the U.S., and reinforce laws such as the Lacey Act[7], which prohibits trade in illegally obtained wildlife.

The convergence of money laundering and illegal wildlife trafficking is not a distant issue; it is embedded in our financial systems. The so-called "green gold" is fueling shadow networks that thrive on exploiting both economic and environmental vulnerabilities.

However, combating this crisis requires more than just meeting compliance mandates. Financial institutions must take a leadership role by integrating advanced

analytics into their oversight mechanisms, fostering international cooperation, and forming strategic partnerships with NGOs and local authorities. By doing so, they can transform passive monitoring into proactive defense systems capable of dismantling covert financial networks supporting wildlife trafficking.

A Call to Action

Ultimately, this is a battle for the future, one in which economic growth must not come at the expense of the planet's biodiversity. Financial systems must evolve to be resilient, ethical, and transparent, ensuring that commerce and conservation coexist. The time to act is now. Whether through technological innovation, regulatory enforcement, or cross-sector collaboration, our collective vigilance will determine whether we leave behind a legacy of responsible stewardship or one of unchecked exploitation.

The choice is simple. Act now to create a financial system that safeguards economies and ecosystems or allows criminals to continue exploiting vulnerabilities. The time to act is now. The Ankura Risk Advisory team specializes in helping financial institutions enhance their anti-money laundering (AML) frameworks and risk management programs. **Our experts provide customized risk assessments, regulatory compliance strategies, and training programs** to identify vulnerabilities and strengthen defenses against financial crime linked to wildlife trafficking.

SOURCES

1 INTERPOL "Illegal wildlife trade" 2023 https://shorturl.at/31ggz

2 World Economic Forum "Organized crime, damaging ecosystems" 2024 https://shorturl.at/ZbMbS

3 IFAW "Disrupting wildlife trade with AI" 2024 https://shorturl.at/nEzpU

4 Convention on international trade https://cites.org/eng

5 World Economic Forum "Organized crime, damaging ecosystems" 2024 https://shorturl.at/ZbMbS

6 Take action (WWF) https://www.worldwildlife.org/

7 Lacey Act, 16 U.S.C. §§ 3371–3378.

FOR MORE INFORMATION CONTACT

Leonardo Pinzon Echeverry

Senior Director at Ankura

✉ **leonardo.echeverry@ankura.com**

Leonardo Pinzon Echeverry, CAMS, Senior Director at Ankura, brings more than 14 years of experience in BSA/AML/CTF compliance, regulatory strategies, examinations and risk management across global financial sectors and jurisdictions.

He has held leadership roles at OAS, Trans-Fast, Synapse Financial Technologies, and Small World Financial Services, and serves on the MSBA Board. He holds a B.Sc. and MBA MCM.

By Omar Magan, CAMS

Building a Culture of Compliance: Best Practices for Fintech Startups

Launching a Fintech startup is a challenging endeavor. In a competitive landscape, startups must create a secure, scalable, and user-friendly platform, secure funding, and attract and retain customers. However, once these hurdles are overcome, founders tend to overlook operational matters like compliance governance until it is too late. Establishing a strong compliance culture is crucial for adhering to regulatory standards and maintaining trust with customers and stakeholders.

> **"To Avoid costly mistakes – it is critical to embrace strong compliance practices in the fintech industry."**

In the Fintech space, lack of governance can be a critical factor in regulatory actions, although such cases may not be as widely publicized as those involving traditional financial institutions. Here are some examples where governance issues within Fintech organizations have contributed to costly enforcement actions:

- **In 2015**, a digital currency company was fined $700,000 by the Financial Crimes Enforcement Network (FinCEN) for allegedly failing to comply with anti-money laundering laws. This enforcement action emphasized the necessity for Fintech companies dealing with digital currencies to have solid compliance programs.
- **In 2018**, a lending platform paid an $18 million settlement with the Federal Trade Commission (FTC) for allegedly misleading consumers about hidden fees and unauthorized charges. The case highlighted governance and transparency issues within the Fintech company, underscoring the importance of clear and honest communication with consumers.

In 2020, a German payment processor scandal served as a significant example of governance failure in the Fintech sector. The company collapsed after it was revealed that €1.9 billion was missing from its accounts, exposing severe deficiencies in corporate governance, including inadequate oversight by the board and failures in internal controls.

In 2021, a trading platform was fined $70 million by FINRA due to alleged governance failures. The regulatory body cited systemic supervisory lapses and inadequate oversight mechanisms that failed to protect customers, especially during platform outages and high-volatility trading periods. These issues highlighted the need for robust governance structures to manage operational risks effectively.

In 2025, a coordinated enforcement action by 48 state financial regulators imposed an $80 million fine on a mobile payment service for alleged violations of the Bank Secrecy Act (BSA) and anti-money laundering (AML) laws. The service was found non-compliant with certain regulatory requirements, potentially enabling illicit activities such as money laundering. These examples illustrate the increasing regulatory focus on Fintech companies and the importance of strong governance and compliance practices in the Fintech sector.

Challenges in Compliance for Fintech Startups

As Fintech startups revolutionize the financial landscape, they face the challenge of balancing rapid growth with complex regulatory compliance, often lacking the necessary expertise and risking strategic misalignment. The drive to secure funding can overshadow the importance of embedding compliance into business strategies, potentially leading to significant long-term repercussions. To thrive amid evolving legal landscapes, these startups must integrate compliance into their innovation processes, ensuring it serves as a competitive advantage while maintaining trust and avoiding legal pitfalls.

- **Balancing Growth, Funding, and Compliance**
  Founders often struggle to balance rapid growth with compliance, as the pressure to deliver quick results can lead to overlooking or underfunding compliance, which can cause strategic misalignment if not integrated from the start. While securing funding is crucial, prioritizing short-term growth metrics over compliance strategies can result in significant long-term repercussions. By embedding compliance into their operational framework, startups can mitigate risks and build trust with customers, investors, and partners, which demonstrates a commitment to ethical practices. This approach not only enhances investor confidence but also supports sustainable growth and provides a competitive advantage. Ultimately, integrating compliance into growth strategies from the outset is essential for long-term success.
- **Lack of Expertise in Regulatory Compliance**
  Many founders come from technology or finance backgrounds and may lack the requisite regulatory expertise needed to effectively manage compliance within their organization. This can lead to underestimating the importance and complexity of regulatory requirements and result in delayed compliance measures until regulatory scrutiny or penalties arise. To mitigate these risks, founders should acknowledge the gaps in their compliance expertise and seek necessary qualified staff, resources, and support.

- **Innovation-First Mindset**
  Fintech startups thrive on innovation, often focusing on cutting-edge technologies that differentiate them in the market. This mindset can result in compliance being viewed as a secondary concern or as an impediment to progress. To successfully balance innovation with compliance, Fintech startups must understand that such advancements will not be sustainable without integrating regulatory compliance into the innovation processes.
- **Complex and Evolving Legal Landscape**
  The legal landscape for Fintech is complex and dynamic, where new regulations and updates or amendments to existing regulations can occur frequently. Founders who wear many hats may struggle to keep up with these changes while managing business operations. This can be especially challenging when operating across multiple jurisdictions where different regulatory requirements apply. Fintech founders need to ensure that proactive and strategic processes and controls are in place to ensure the organization is capable of identifying applicable regulatory changes and implementing adequate plans to address those changes in a timely, effective, and sustainable manner.

Building a Culture of Compliance

Commitment from senior management is crucial in cultivating a culture of compliance within any organization, especially in highly regulated industries like Fintech. The tone set by leadership significantly influences the organization's approach to compliance and its integration into everyday business operations. In order to build a strong compliance culture, senior management should lead by example and demonstrate a strong commitment to compliance by allocating resources and prioritizing compliance initiatives. Clear communication channels must also be established to ensure all employees understand the importance of compliance within the context of their roles within the organization and are held accountable for upholding the company's compliance standards. This commitment not only mitigates risks but can also enhance the organization's reputation and trustworthiness, ultimately contributing to its long-term success.

Resource Allocation and Prioritization

One of the most tangible ways senior management can demonstrate a commitment to compliance is by providing the means to support and implement compliance initiatives. This includes investing budget funds to tools and technologies, as well as dedicating human resources to build a strong and qualified compliance team. By prioritizing these allocations, management ensures that compliance is not an afterthought but a fundamental component of the business strategy. Moreover, this investment signals to the entire organization that compliance is significant and essential for achieving long-term success and sustainability.

Leadership by Example

Senior management should set the standard by visibly engaging in compliance activities and adhering to the same compliance expectations of all employees. When leadership models these behaviors, it encourages everyone to take compliance seriously and reinforces the message that compliance is a shared responsibility and not just the domain of the compliance department.

Clear Communication Channels

Effective communication is critical in ensuring that all employees grasp the importance of compliance and understand their specific roles in maintaining it. Senior management should establish clear and open communication channels to effectively disseminate compliance-related information. This can be achieved through various methods, such as updates on regulatory changes via newsletters or intranet postings, training sessions tailored to different departments, and interactive forums or town hall meetings for discussing compliance challenges and solutions. Additionally, creating a centralized compliance portal where employees can access resources, FAQs, and submit compliance questions can enhance accessibility and engagement.

By maintaining transparency and openness, management can foster an environment where employees feel informed, supported, and empowered to uphold compliance standards confidently.

Training and Education Programs

To support compliance initiatives, senior management should implement comprehensive training and education programs tailored to address all relevant compliance requirements affecting the business based on its products, services, and customers served, and equip employees with the knowledge and skills necessary to meet those requirements. Training programs should also be designed to be job-specific and provide the necessary information for all employees to understand how compliance impacts their specific functions. Providing regular training also helps to keep compliance top-of-mind throughout the organization and ensures that employees are up-to-date with the latest regulatory developments.

Encouraging a Culture of Accountability

Senior management should promote a culture where accountability is valued, and employees are encouraged to speak up about compliance concerns without fear of retaliation. This can be achieved by establishing clear reporting mechanisms and whistleblower protections that allow employees to report potential compliance violations safely and confidentially. By fostering a supportive environment, management can ensure that compliance issues are identified and addressed promptly, which in turn can minimize risks to the organization.

The Strategic Edge of Compliance in Fintech Growth

Establishing a strong culture of compliance is not just necessary for regulatory adherence but also serves as a strategic advantage for Fintech startups. By prioritizing compliance and establishing a strong compliance culture, Fintechs can achieve sustainable growth and maintain stakeholder trust amid complex and evolving regulations. A commitment from senior management to integrate compliance into the core business strategy signals dedication to ethical practices and can mitigate risks like fines and reputational damage. Moreover, this focus can enhance investor confidence and foster trust with customers and partners, which in turn offers a competitive edge. Ultimately, startups that embrace compliance are better positioned to adapt to new regulations and market demands, supporting long-term success and innovation in the Fintech landscape.

> **"A core compliance strategy is essential for sustainable growth and maintaining trust with customers and investors."**

FOR MORE INFORMATION CONTACT

Omar Magana, CAMS

Managing Director at Ankura

✉ omar.magana@ankura.com

Omar Magana, CAMS, serves as the Managing Director at Ankura, brings over 20 years of experience in compliance, risk management, and implementing surveillance technologies to reduce financial risk. Omar has a proven track record in the Money Services Business and private banking industries, developing and leading international and domestic AML programs, as well as anti-bribery initiatives.

As a consultant, he has led AML reviews, policy development, risk assessments, and operational improvements for fintech and traditional financial services. He has also enhanced AML systems for customer onboarding, monitoring, reporting, and government sanctions programs.

The Right Experts at the Right Time Responding to the Increased Global Risk of Financial Crimes

Jesus Torres
Managing Director

Eric Gagnon
Managing Director

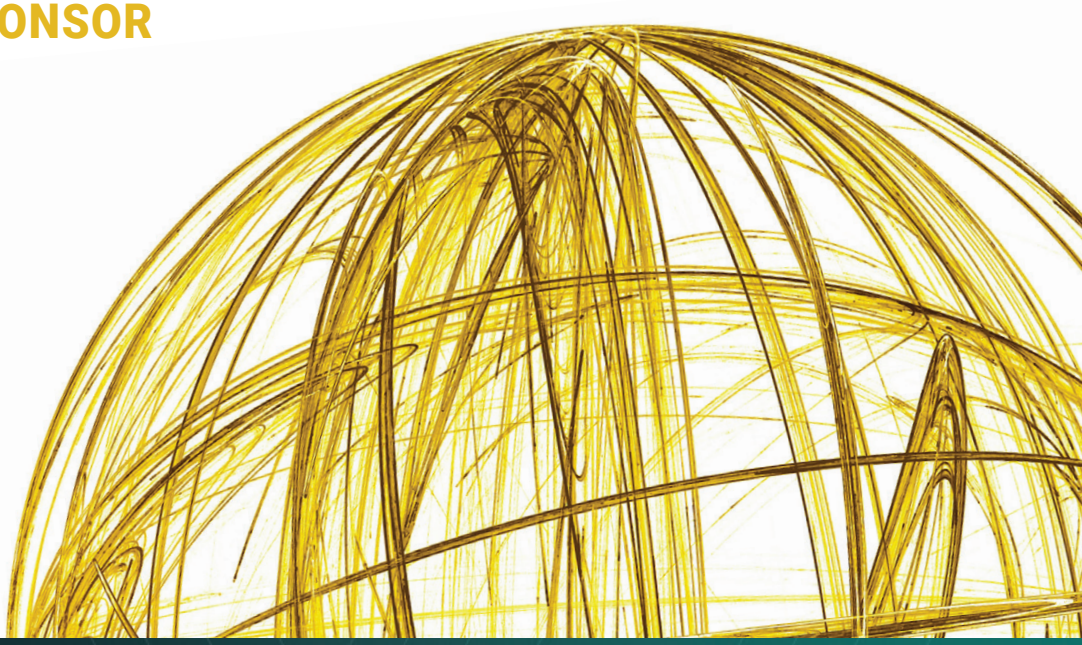
Monique Maranto
Senior Director

ankura™

PROUD GOLD SPONSOR

CBC | SUMMIT USA
CRYPTO BANKING, COMPLIANCE, & PAYMENTS

September 18, 2025,
Washington, D.C.



By Jake Hines

The Top Five Ways Cannabis Reform Could Impact Financial Services in 2025

We are just a couple of months into 2025, and cannabis reform is already poised to massively impact the financial services industry. The changes we might see this year are expected to address longstanding challenges - and open some important new opportunities for financial providers.

> **"2025's cannabis reforms are set to transform the financial landscape, opening new opportunities in banking, lending, and insurance for cannabis-related businesses."**

1. **Enhanced Access to Banking Services**
   Currently, many cannabis-related businesses (CRBs) are forced to operate on a cash-only basis due to federal restrictions. This not only poses operational challenges but also results in many security challenges. Legislative efforts like the Secure and Fair Enforcement (SAFE) Banking Act are aimed at providing "safe harbor" protections to financial institutions who opt to work with the cannabis industry, ensuring they are not penalized for offering much-needed services to CRBs.

   This would likely increase the accessibility of banking, lending, and insurance services for the marijuana industry - and open up new revenue streams for players in those sectors.

2. **Improved Tax Compliance and Deductions**
   The reclassification of cannabis from a Schedule I to a Schedule III substance under the Controlled Substances Act has been a hot topic for quite some time. When we finally see this change come to fruition, it is expected to alleviate many federal restrictions - particularly regarding tax deductions for cannabis businesses.

This change could seriously decrease the financial burdens on CRBs, allowing them to deduct ordinary business expenses like other businesses and potentially leading to increased profitability.

3. **Increased Investment Opportunities**
   With the hotly anticipated federal legalization of cannabis and improved financial access, the cannabis industry is projected to experience enormous growth. This growth will be a boon for the industry, attracting more investors, and hopefully leading to increased capital inflow and market expansion.

   As the legal landscape surrounding cannabis continues to evolve, we should see a more favorable environment for investment in the cannabis sector blossoming.

4. **Enhanced Financial Stability**
   The ability to integrate cannabis businesses into the formal financial system will profoundly enhance financial stability by reducing the risks associated with cash-only operations. This integration would level the playing field for CRBs, putting them on more even footing with other lawful enterprises and creating a more secure business environment - and of course enhancing the security of the profits earned, which would no longer need to be exclusively moved physically.

5. **Streamlined Regulatory Compliance**
   Finally, federal reforms should provide clearer guidelines for financial institutions that want to work with the cannabis industry. Clarity on the regulatory front would both reduce compliance costs and help assuage concerns over legal uncertainties, finally allowing financial providers to offer services to CRBs without the constant fear of federal penalties. The SAFE Banking Act, as one example, would help open the door to protect federally regulated depository institutions that could find a new market in providing financial services to CRBs.

Despite regulatory reform being a slow burn for years, expected changes to the legal framework surrounding cannabis in 2025 have the potential to give the financial services industry a major boost by enhancing access to banking, improving tax compliance, increasing investment opportunities, enhancing financial stability, and streamlining regulatory compliance. With the right changes enacted, the United States can create a more robust and secure financial environment for both cannabis businesses and financial institutions - a true win-win!

> **"A Win-Win for Finance and Cannabis: Enhanced Stability and Compliance"**

FOR MORE INFORMATION CONTACT

Jake Hines

Director at Ankura

✉ jake.hines@ankura.com

Jacob (Jake) Hines, Director at Ankura, brings nearly 10 years of experiene 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 aiding in various other regulatory compliance functions.

By Heather Chester, CAMS

Unmasking the Dark Side of OnlyFans: Combating Human Trafficking and Sexual Exploitation with Effective Research Strategies

While some users have referred to OnlyFans as empowering, unfortunately, the site also plays a role in human trafficking and exploitation. The U.S. Department of State estimates that, at any given time, there are an estimated 27.6 million victims of human trafficking worldwide[1]. With the global population at around 8 billion[2], this represents about 0.345 percent of the population. Many of these victims are trafficked online.

> **"There are an estimated 27.6 million victims of human trafficking worldwide."**

Given the site is largely known for sexual content, OnlyFans makes itself another instrument for human trafficking. In 2023, OnlyFans had 4.12 million creators and 305 million users[3]. If we apply the aforementioned 0.345 percent to those creators, that suggests there are 14,214 victims of human trafficking on the site. As financial institutions, we have tools at our disposal to remain compliant and fight this crime. Through the use of transactional data, Know Your Customer (KYC) information and Open-Source Intelligence (OSINT) collection, we can locate and identify potential trafficker-run and victim OnlyFans profiles.

Once it is suspected a customer may be affiliated with OnlyFans, perhaps through deposits from Fenix Internet (OnlyFans payment processor), the first step will be locating the profile. Creators often do not use their real names on their profiles, and this is even more true for traffickers and their victims. Therefore, finding the people behind OnlyFans profiles can be a challenge.

This is where KYC, obtained by financial institutions, and transactional activity can assist. This can be accomplished via searches of the customer-provided email address and Peer-to-Peer (P2P) counterparties. Many times, the username of the customer's email address is also the customer's online nickname (including on OnlyFans). This can also be true of P2P counterparties. While some P2P counterparties utilize a person's real name, others are pseudonyms that can sometimes be matched to the person's online identity. Searching some of the more frequent, and higher value, P2P counterparties can help to locate the customer's handle. Searching either the email username or P2P pseudonym along with key phrases, such as "OnlyFans" or "linktr.ee", can narrow down results as well as show similar handles which may be associated with the customer. Further, locating a linktr.ee can reveal additional social media and third-party sites linked to the customer. Locating a social media account under the customer's real name can also be beneficial. To generate traffic to an OnlyFans profile or other social media, aliases of those sites often "like" posts and/or are "friends" with the customer's real social media account.

Once the OnlyFans profile has been located, this is where OSINT becomes an even more important tool. Full access to OnlyFans profiles requires a subscription, which may not be allowed by your financial institution. However, even without access to the full profile, there are several key items from the site that can be used to assist in identifying victim profiles. Just as with advertisements, the traffickers can also control victims' OnlyFans profiles. In a survey conducted of human trafficking survivors by Polaris Project, 26 percent had indicated they were exploited on their own social media accounts by their trafficker[4]. t is important to look closely at both OnlyFans and previously identified social media accounts for red flags to indicate possible trafficker-controlled or victim activity.

A consistent feature across OnlyFans' profiles is the presence of pictures. Each creator has a profile picture, typically a banner, and sometimes include additional preview images or videos. Clues from these pictures

can help to distinguish between victim versus freely created profiles. Pictures uploaded by creators with control of their accounts typically will not appear harmed, on drugs, or in danger, as they are promoting their image for views. Further, they are often smiling or showing interest, which suggests they are comfortable with being photographed. The opposite tends to be true of trafficker-run or victim profiles as the victims are being coerced into taking these pictures. The location (think background) of the pictures also provides important clues. Independent creators tend to take pictures in their own homes or on location (high-end hotels, beaches, nightclubs, etc.). As victims are not typically living in their own homes or have the ability to move freely, their photos will often be taken at motels or apartments/houses that appear to have multiple individuals residing inside. Settings such as these usually have very few personal items showing, or may offer clues that multiple individuals are residing at the location (multiple individuals seen in the background, or multiple personal items seen in the photos).

Additional clues may be found in the introduction or description. Each creator provides a short description of the type of content offered on the page. Take note of descriptions that offer to meet offline, offer to provide in-person sexual services, offer content with multiple individuals, or direct the viewer to another site for further services. These may indicate that the OnlyFans profile is not really created for views, but rather as an

advertisement for sexual exploitation. Speaking of advertisements, take note of descriptions that utilize traditional advertising techniques such as lots of emojis (mostly sexual ones) and a surplus of services with almost nothing "off limits."

While the information above may lead us to believe that a customer is a victim of human trafficking, it is still critical to also consider traditional transactional and KYC red flags. These include late-night transactions with hotels, rideshares, or vending machines, a lack of personal expenses, and varying transaction locations indicating constant movement. Additional OSINT tools may include research of the provided address and IP activity, conducting reverse image searches and searches of the provided phone number in advertisement databases.

> **"Financial institutions can leverage KYC and OSINT to uncover and combat human trafficking on platforms like OnlyFans"**

While social media portrays many OnlyFans creators as enjoying a lavish lifestyle, it is also important to remember the space also provides an avenue for human trafficking and exploitation. Using KYC and OSINT information, the above-outlined tools provide a foundation of investigative techniques to ensure timely reporting of this crime. As it is ever adapting to the new technology and laws, these tools can be combined with other OSINT and third-party applications to monitor for, and identify, human trafficking victims.

Our team of experts specializes in services tailored to detecting and reporting on human trafficking, implementing effective controls, and minimizing risks. Ankura can help you stay ahead of these ever-evolving threats with proactive risk management strategies to disrupt illegal activities, protect victims, and ensure compliance with legal and ethical standards.

SOURCES

1 "About Human Trafficking." U.S. Department of State, www.state.gov/humantrafficking/about-human-trafficking/. Accessed 10/01/2025.

2 "Population." United Nations, www.un.org/en/global-issues/population Accessed 10/01/2025.

3 Spangler, Todd. "OnlyFans Payments Hit $10 Billion as Revenues, Creator Earnings Jump in 2023." Variety, 10 Jan. 2024, variety.com/2024/digital/news/onlyfans-payments-2023-financials-revenue-creator-earnings-1236135425/. Accessed 03/01/2025.

4 Polaris Project. "A Roadmap for Systems and Industries to Prevent and Disrupt Human Trafficking: Social Media." Polaris Project, Aug. 2018, https://polarisproject.org/wp-content/uploads/2018/08/A-Roadmap-for-Systems-and-Industries-to-Prevent-and-Disrupt-Human-Trafficking-Social-Media.pdf. Accessed 03/01/2025.

FOR MORE INFORMATION CONTACT

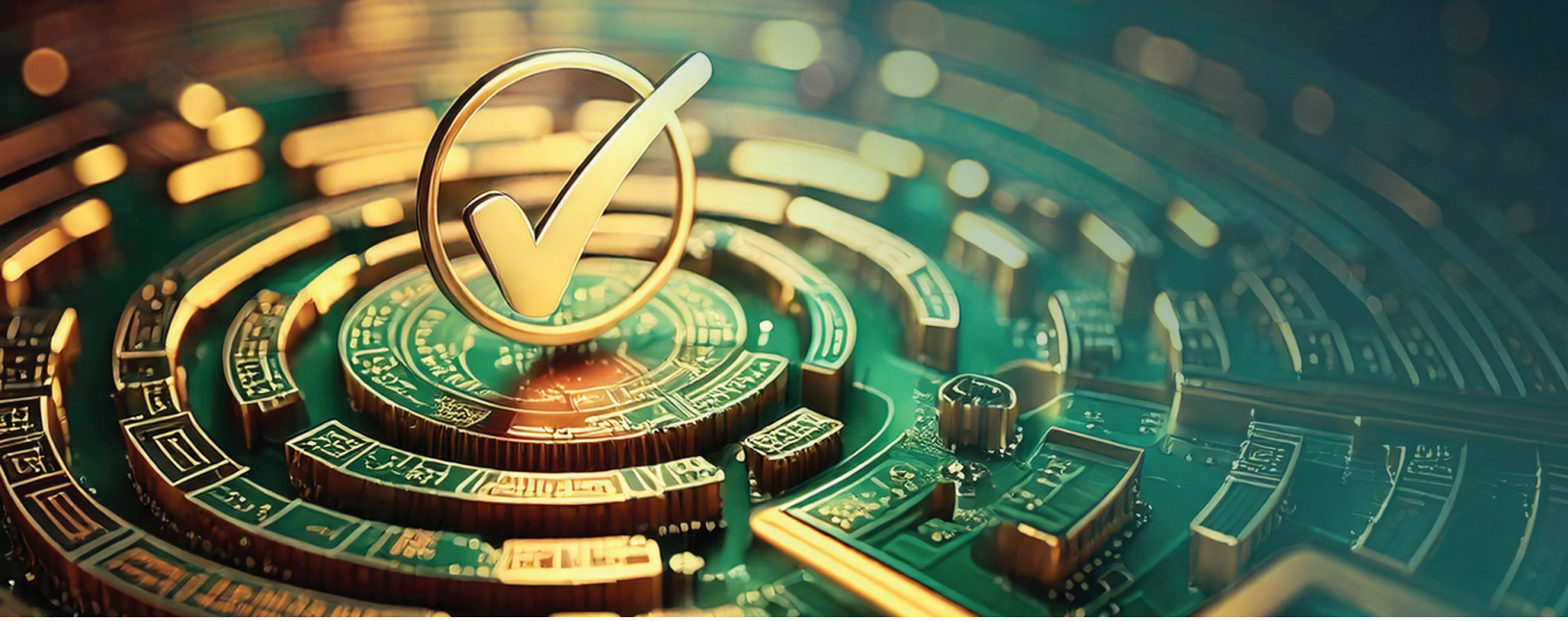
Heather Chester, CAMS

Director at Ankura

✉ heather.chester@ankura.com

Heather Chester, CAMS, Director at Ankura, has over 5 and half years of BSA/AML experience. Prior to joining Chartwell, Heather was employed with AML RightSource LLC where she oversaw staff, managed operations and performed transaction monitoring, risk assessments and quality control across KYC, Enhanced Due Diligence and Investigation workflows for both large and small financial institutions. In addition, she also trained new analysts and performed data management for client reporting metrics.

Heather also spent 9 years as a police and fire dispatcher where she worked in a multi-departmental call center answering 9-1-1 and non-emergency calls. She trained new hires and was certified in several areas of emergency expertise.



By Kay Toscano, CRCM, CAFP

Regulatory Roadmap for Third-Party Compliance in Financial Services

In the rapidly evolving financial ecosystem, financial institutions (FIs) increasingly rely on third parties, including Fintech companies, Banking-as-a-Service (BaaS) providers, and other financial service entities—to expand their capabilities and improve customer experiences. However, such partnerships introduce complex risks that require a structured approach to compliance and governance. Two key regulatory documents provide a roadmap for managing these risks:

- **The 2023 Interagency Guidance on Third-Party Relationships: Risk Management**
- **The 2024 Joint Agency Third-Party Risk Management (TPRM) Guide for Community Banks**

Together, these guides offer a comprehensive framework for both financial institutions and their third-party partners to ensure compliance, mitigate risks, and foster sustainable partnerships. Additionally, recent regulatory enforcement actions illustrate the consequences of poor third-party risk management, offering critical lessons for the industry.

This roadmap is not only crucial for financial institutions seeking to maintain compliance but also for third parties, including Fintechs, BaaS providers, and other financial services, to effectively support their banking partners and align with regulatory expectations.

Understanding the Regulatory Landscape

The 2023 Interagency Guidance sets the foundation for third-party risk management by outlining best practices for risk assessment, due diligence, ongoing monitoring, and governance. This applies broadly across all banking organizations and their third-party relationships. Meanwhile, the 2024 Joint Agency TPRM Guide tailors these principles specifically for community banks, offering practical implementation strategies and considerations for smaller institutions with limited resources.

For both banks and third parties, understanding and adhering to this framework is critical. **The guidance emphasizes that third-party relationships do not absolve banks of their compliance responsibilities,**

meaning that banks must manage and oversee these partnerships as if the activities were conducted in-house. Several recent enforcement actions demonstrate what happens when financial institutions fail to do so.

The Third-Party Relationship Lifecycle

Both documents establish a structured third-party relationship lifecycle, which serves as a roadmap for compliance and risk management.

Planning: Before entering a third-party relationship, financial institutions must assess the strategic benefits and risks of engagement and ensure compliance, security, and financial considerations are thoroughly analyzed. For example, a regional bank considering a partnership with a Fintech company for mobile payment processing should evaluate how the service aligns with its strategic goals, regulatory obligations, and cybersecurity infrastructure. Third parties should be prepared to demonstrate alignment with the financial institution's regulatory and operational expectations, providing clear justifications for their role in the partnership.

Due Diligence & Third-Party Selection: Financial institutions must conduct rigorous evaluations of potential third parties, assessing their legal standing, financial health, risk management controls, and compliance history with regulations including, but not limited to, fair lending and anti-money laundering laws. For instance, a bank engaging a cloud service provider must verify the provider's cybersecurity protocols, data protection measures, and regulatory compliance to mitigate operational risks. Third parties, in turn, should proactively provide comprehensive documentation of their risk management frameworks, security policies, and regulatory adherence to streamline the due diligence process and establish trust.

Contracts should clearly define responsibilities, performance metrics, audit rights, data security provisions, and termination clauses. For example, a

community bank outsourcing loan processing to a third-party vendor must ensure that the contract includes clear service-level agreements (SLAs) outlining response times, compliance requirements, and data access rights. Financial institutions must ensure that contracts facilitate effective risk management and compliance oversight. Third parties should negotiate contracts that align with their operational capabilities while also meeting the stringent regulatory requirements imposed by banking partners.

Ongoing Monitoring: Once a third-party relationship is established, continuous monitoring is essential to verify that performance meets contractual obligations and regulatory requirements. For example, a bank using an external customer service platform should regularly assess whether the provider meets customer service standards, complies with consumer protection laws, and safeguards sensitive customer data. Financial institutions must regularly audit third-party activities, review compliance documentation, and assess risk

exposure. Third parties should maintain transparency by providing timely reports and proactively addressing any concerns raised by their banking partners.

Termination & Exit Strategy: A well-defined termination and exit strategy is critical to ensure minimal disruption in case a third-party relationship needs to be discontinued. If a bank decides to sever ties with a payment processing provider due to performance issues, it must have a clear transition plan to migrate customer transactions seamlessly to another provider or bring the function in-house. Financial institutions must develop contingency plans that allow for a smooth transition of services, safeguarding operational stability. Third parties should cooperate with their banking partners in this process by ensuring that all necessary data, records, and processes are transferred securely and in compliance with regulatory requirements.

The Role of Fintechs, BaaS, and Other Third Parties

For Fintechs, BaaS providers, and financial service firms, these guidelines serve as a comprehensive playbook for establishing strong, compliant relationships with financial institutions. **To achieve regulatory readiness, third parties are required to maintain compliance frameworks that are not only strong but also closely aligned with federal banking regulations.** This involves staying informed about regulatory changes and ensuring that their operational practices meet the stringent standards imposed by the financial sector.

Risk transparency is another critical factor, necessitating that third parties provide clear and comprehensive assessments, audit results, and compliance documentation to their banking partners. This transparency helps build trust and facilitates smoother interactions, as banks can readily verify that their partners are adhering to necessary compliance standards.

Operational resilience is equally important, ensuring that business continuity plans, cybersecurity measures, and risk mitigation strategies are meticulously documented and regularly updated. This preparation is crucial for minimizing disruptions in service and maintaining security, particularly in the face of unforeseen challenges or cyber threats.

Additionally, contractual clarity is necessary to define compliance responsibilities and expectations clearly, thereby mitigating risks and fostering long-term partnerships. Contracts should explicitly outline the roles, responsibilities, and compliance obligations of each party, reducing the likelihood of disputes and ensuring that all parties are aligned in their objectives and practices. When “boilerplate” language is included, it is critical that service providers clarify with their banking partners how each contract provision applies to establish realistic expectations. For example, if a contract stipulates that a service provider is responsible for complying with consumer protection

laws, but the provider only facilitates business-to-business (B2B) payments, the service provider should confirm whether the bank expects the provider to develop and implement consumer protection policies. By adhering to these guidelines and establishing expectations up front, Fintechs and other third parties can effectively support their banking partners, aligning with regulatory requirements and contributing to stable, productive partnerships.

Lessons from Regulatory Enforcement Actions

The 2023 Interagency Guidance and the 2024 Joint Agency TPRM Guide provide a structured framework for financial institutions and their third-party partners to manage risk effectively and ensure compliance. These documents outline best practices for assessing, engaging, and overseeing third-party relationships, emphasizing the importance of due diligence, ongoing monitoring, and governance. However, the practical application of these principles is critical, as evidenced by recent regulatory enforcement actions. **These actions highlight the real-world consequences of inadequate third-party risk management and serve as a stark reminder of the potential pitfalls that financial institutions can face without proper oversight and compliance measures in place.** By examining these enforcement cases, financial institutions can glean valuable lessons on the importance of rigorous TPRM practices, thus enhancing their own strategies and safeguarding against similar issues in the future. Financial institutions that do not implement strong TPRM frameworks risk regulatory penalties, reputational damage, and operational disruptions. The following recent enforcement actions highlight critical failures in third-party risk management and the lessons learned:

BLUE RIDGE BANK (2022) – Insufficient Due Diligence and BSA Compliance Gaps

The OCC's enforcement action against Blue Ridge Bank revealed serious deficiencies in its third-party risk management framework. The bank engaged in partnerships with Fintech firms without establishing adequate oversight mechanisms. As a result, there

were failures in transaction monitoring, leading to significant Bank Secrecy Act / Anti-Money Laundering (BSA/AML) non-compliance and increased exposure to illicit activities. Furthermore, regulators found that the bank's risk assessment processes were inadequate, with missing or incomplete documentation on how Fintech partners adhered to compliance requirements.

LESSON LEARNED

Banks must conduct rigorous pre-engagement due diligence and establish continuous monitoring protocols to identify emerging risks in third-party relationships. A structured TPRM framework should include automated compliance checks, periodic audits, and strong internal controls.

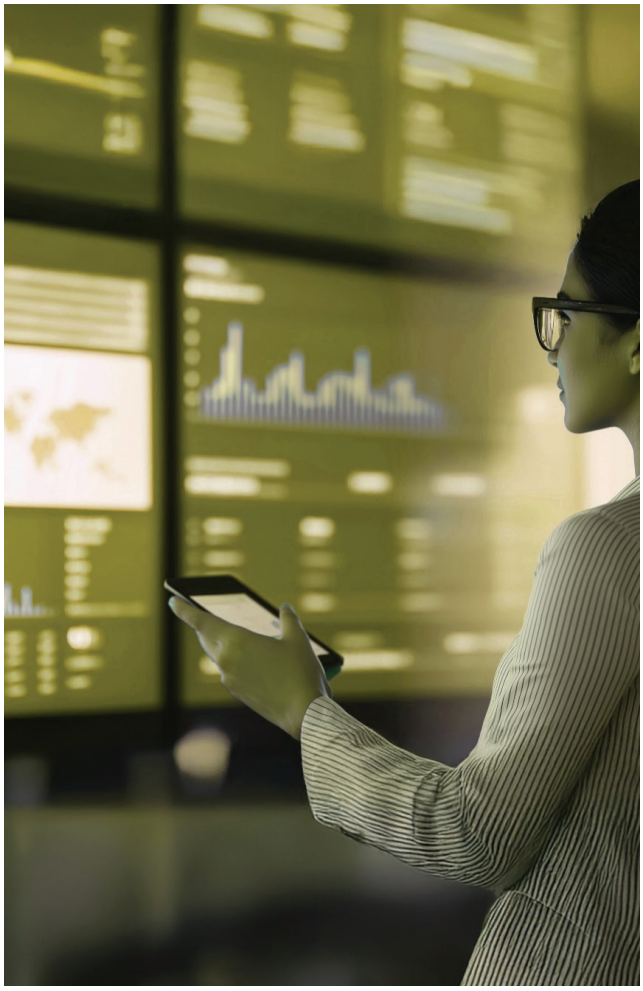
CROSS RIVER BANK (2023) – Consumer Protection Failures in Fintech Lending

The FDIC's consent order against Cross River Bank cited unsafe and unsound banking practices related to third-party credit underwriting and fair lending compliance. The bank had an aggressive Fintech lending strategy, which led to inadequate oversight of third-party credit products.

Regulators found that the bank lacked effective risk controls for loan origination, underwriting practices, and consumer disclosures, leading to potential violations of the Equal Credit Opportunity Act (ECOA) and the Truth in Lending Act (TILA). Additionally, the bank's compliance management system failed to identify and correct unfair lending practices, raising concerns over fair lending violations and potential consumer harm.

LESSON LEARNED

Financial institutions must enforce clear compliance obligations on Fintech partners and integrate automated monitoring systems to track adherence to fair lending laws. Establishing strong credit underwriting guidelines and internal auditing processes can prevent regulatory violations.



LINEAGE BANK (2024) – Inadequate Oversight of Banking-as-a-Service (BaaS) Relationships

The FDIC's enforcement action against Lineage Bank marked a significant moment in BaaS regulation, with regulators citing poor governance, insufficient staffing, and lack of contingency planning in the bank's Fintech partnerships. Lineage Bank partnered with multiple Fintech firms to offer banking services but failed to implement risk controls to oversee third-party activities. Examiners noted that the bank's compliance and internal audit teams were understaffed, leading to delays in addressing regulatory concerns. Furthermore, the bank lacked a structured exit strategy, increasing risks in the event of a failed Fintech partnership.

LESSON LEARNED

Banks engaged in BaaS must establish dedicated governance structures and staff risk management teams to oversee Fintech partnerships effectively. A well-defined exit strategy ensures service continuity while minimizing operational disruptions.

PIERMONT BANK (2024) – Weak IT Risk Controls in Third-Party Management

Regulators issued a consent order against Piermont Bank after identifying deficiencies in IT security, compliance monitoring, and contractual risk oversight with Fintech partners. The bank engaged in high-risk third-party relationships without implementing sufficient cybersecurity protections, making it vulnerable to data breaches and operational failures. Examiners also found deficiencies in vendor contracts, particularly in defining clear security responsibilities and reporting requirements.

LESSON LEARNED

Banks must include cybersecurity risk assessments in their third-party due diligence and continuously monitor IT security controls to mitigate exposure. Establishing strong contractual agreements with Fintech partners that outline cybersecurity obligations, data protection measures, and audit rights is essential to reducing third-party risk.

COMERICA BANK (2024) – Consumer Service Failures in a Third-Party Relationship

The CFPB lawsuit against Comerica Bank demonstrated how third-party mismanagement can directly harm consumers, many of whom were vulnerable seniors collecting much-needed social security benefits. The bank's failure to oversee a government benefits card program led to customer service disruptions, unauthorized fees, and regulatory violations. Regulators found that Comerica's third-party vendor disconnected millions of customer calls, failed to investigate fraud claims, and imposed illegal ATM fees on Social Security recipients.

LESSON LEARNED

Banks must not only ensure compliance in financial transactions but also in customer service delivery and dispute resolution mechanisms. Regular performance audits, consumer protection assessments, and third-party oversight frameworks are critical in maintaining regulatory compliance

Key Takeaways

Recommendations for Banks: Strengthening Third-Party Risk Oversight

These enforcement actions reinforce the need for banks to align their third-party risk management strategies with regulatory expectations. To enhance compliance and operational effectiveness, banks should:

- **Formalize Third-Party Risk Management Programs**
  Banks must ensure that due diligence, risk assessments, contract management, and ongoing monitoring are structured within a documented program. Board approval should be required for high-risk Fintech partnerships, with annual reviews of the effectiveness of third-party relationships.
- **Enhance Fair Lending and Consumer Protection Measures**
  For banks that engage Fintechs who are involved in lending activity or who offer consumer-purpose products and services, compliance programs should include automated fair lending and consumer compliance risk assessments, independent audits, and proactive engagement with regulators. Clear procedures should be in place to address consumer complaints and ensure compliance with applicable consumer protection laws and regulations.
- **Strengthen AML and OFAC Oversight**
  Banks must implement real-time transaction monitoring systems, Fintech-specific AML policies, and enhanced screening processes for high-risk partners. Third-party agreements should include clear escalation protocols for suspicious activity and regulatory reporting obligations.
- **Develop Contingency and Exit Strategies**
  Banks should maintain clear termination protocols for Fintech partnerships, ensuring a seamless transition of customer accounts in the event of partner failure or regulatory non-compliance. Backup plans should include alternative service providers and contractual safeguards to prevent disruption to customers.
- **Improve Data Governance and Reporting**
  Banks must ensure that data-sharing agreements with third parties meet regulatory expectations, including provisions for customer data privacy, audit rights, and compliance certifications. Reporting systems should enable real-time insights into Fintech-driven activities and risk exposure.

Recommendations for Third-Party Providers: Supporting Banking Partners

While banks bear the ultimate regulatory responsibility for third-party activities, Fintechs and payment providers must also take proactive steps to **align with regulatory expectations and strengthen partnerships with banks.**

- **Enhance Compliance Transparency**
  Fintechs should provide banks with detailed compliance documentation, including independent audit reports, written policies and procedures, and risk assessments addressing all applicable regulatory requirements and expectations set by the bank. Banks require clear visibility into regulatory compliance efforts to meet supervisory expectations.

- **Improve Risk Management Capabilities**
  Third-party providers must implement strong internal controls for transaction monitoring, cybersecurity, and fraud prevention. Banks need assurance that Fintechs have strong operational risk frameworks in place to detect and mitigate threats proactively.

- **Facilitate Ongoing Regulatory Reporting**
  Fintechs should establish real-time data-sharing agreements with banks to support regulatory reporting obligations. This includes automated transaction tracking, customer risk assessments, and compliance dashboards that align with bank reporting structures.

- **Collaborate on Consumer Protection Initiatives**
  Since banks remain liable for Fintech-related consumer complaints, third-party providers should develop clear customer dispute resolution processes, consumer education resources, and responsive compliance teams to address regulatory concerns.

- **Prepare for Exit and Contingency Scenarios**
  Fintechs should maintain detailed wind-down plans and transition protocols to minimize disruption in case of contract termination or regulatory enforcement. This includes data portability measures, customer migration strategies, and clear exit agreements with banking partners.

Conclusion | A Compliance-First Approach to Third-Party Relationships

In conclusion, as financial institutions increasingly collaborate with Fintech companies and Banking-as-a-Service (BaaS) providers, it is critical to establish comprehensive third-party risk management frameworks in the financial services sector. The complexity of these partnerships necessitates a vigorous approach to managing risks, as outlined in the 2023 Interagency Guidance and the 2024 Joint Agency TPRM Guide, which emphasize regulatory compliance, thorough risk assessment, and operational resilience.

Recent enforcement actions against banks like Blue Ridge, Cross River, Lineage, Piermont, and Comerica underline the severe consequences of inadequate TPRM practices. These cases underscore the urgent need for financial institutions to maintain vigilant oversight of third-party relationships, ensuring compliance across all operational areas, including cybersecurity and consumer protection. The heightened regulatory scrutiny demands that both banks and their partners adopt a proactive, compliance-first approach to managing third-party engagements.

As financial institutions expand their Fintech partnerships, balancing innovation with compliance becomes paramount. By integrating detailed risk assessments, governance controls, and continuous monitoring, institutions and their third-party providers can leverage compliance as a strategic advantage, fostering secure and sustainable partnerships. Those that strengthen oversight, enhance due diligence, and maintain real-time risk visibility will thrive in this evolving regulatory environment, while those that fail to adapt risk becoming the next subject of enforcement actions.

Disclaimer and Source Documents

This article is based on publicly available regulatory enforcement actions, including consent orders and supervisory findings issued by the Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), Federal Reserve, and Consumer Financial Protection Bureau (CFPB). Specific cases referenced include Blue Ridge Bank (2022), Cross River Bank (2023), Lineage Bank (2024), Comerica Bank (2024), and Piermont Bank (2024). The analysis reflects interpretations of regulatory trends and does not constitute legal advice.

How Ankura Can Help

Navigating the complexities of third-party risk management requires expertise in regulatory compliance, risk assessment, and operational resilience. Ankura works with financial institutions and Fintech companies to develop and implement comprehensive TPRM frameworks that align with regulatory expectations. By conducting thorough assessments, Ankura helps organizations identify gaps in governance, due diligence, and monitoring, ensuring that third-party relationships are managed effectively and in compliance with evolving regulations.

Ankura also supports financial institutions in strengthening their cybersecurity and IT risk management strategies, evaluating third-party IT security controls, and enhancing data protection frameworks. Additionally, Ankura assists in ensuring compliance with consumer protection and fair lending regulations, helping institutions mitigate risks related to ECOA, TILA, and Unfair, Deceptive, or Abusive Acts or Practices (UDAAP). Through collaborative engagement, Ankura enables financial institutions and Fintech providers to build resilient, compliant, and sustainable business relationships, while proactively addressing regulatory requirements and mitigating third-party risks. Navigating the complexities of third-party risk management requires expertise in regulatory compliance, risk assessment, and operational resilience. Ankura specializes in helping financial institutions and Fintech providers build robust compliance programs aligned with regulatory expectations.

Partnering with Ankura ensures that financial institutions and fintech companies can proactively address regulatory requirements, mitigate third-party risks, and build sustainable, compliant business relationships.

FOR MORE INFORMATION CONTACT

Kay Toscano, CRCM, CAFP

Senior Director at Ankura

✉ **kay.toscano@ankura.com**

Kay brings has over 30 years of experience in executive and consulting roles within the financial services and Fintech sectors, specializing in compliance, risk management, and audit. She possesses an extensive understanding of banking processes and associated risks, with a particular proficiency in audit and internal control management. Kay is an expert in developing and implementing Enterprise Risk Management (ERM) and Compliance Management Systems (CMS), focusing on creating robust risk assessment models to enhance organizational resilience. Her skills extend to Third-Party Risk Management and the development of ACH Risk Models to mitigate transaction-related vulnerabilities. Kay has led outsourced CMS-GRC program administration, conducted ACH reviews, and performed BSA/AML/OFAC independent audits, model validations, and CRA assessments, among other compliance audits. Known as an effective change agent and collaborative team leader, she excels in problem-solving and communicating complex risk concepts. Previously, Kay conducted risk-based regulatory compliance consulting for various firms and served in numerous senior roles, including Senior Vice President/Compliance and Bank Secrecy Act/Anti-Money Laundering Officer. Her certifications include Certified Regulatory Compliance Manager (CRCM) and Certified Anti-Money Laundering and Fraud Professional (CAFP). Additionally, she directed regulatory compliance services at a Regtech company and successfully led a $2.7 billion financial institution out of a BSA/AML Enforcement Action by strengthening its risk management framework. Kay is adept at managing third-party risk and ensuring regulatory compliance through comprehensive risk assessments and model development, acting as a primary liaison between internal, external counsel, and regulatory agencies.

Nationwide Multistate Licensing System

NMLS CORNER

Ankura was represented at the 2025 Nationwide Multistate Licensing System (NMLS) Conference and Training from February 11 to 14 in Atlanta, Georgia.

The New Kansas Money Transmission Act (KMTA) became effective on January 1, 2025. All current money transmitter licensees and any future applicants should review the new law in its entirety to determine how the changes will affect your company's money transmission services in Kansas. Click **here** for more information.

This year's conference and the NMLS Ombudsman Meeting focused heavily on NMLS modernization efforts. At the meeting, Ankura's Trish Lagodzinski and Jake Hines proposed enhancements to the NMLS Checklist Compiler and streamlining regulatory communications in NMLS—both of which (and more) are on the modernization agenda. Industry participants included those from mortgage, state licensing, money services business, consumer finance, debt, federal registry, and surety sectors.

AI in Financial Services was the most popular session at the conference, featuring Jake Hines of Ankura discussing AI in financial services and compliance alongside AI experts and industry leaders. Jake provided a unique perspective on how consultancy firms like Ankura can assist in implementing responsible AI in financial businesses as the landscape continues to evolve rapidly. With over 300 attendees and standing room only, it became the most attended session in NMLS conference history!

The conference saw a historic turnout of over 800 regulators and industry leaders, providing attendees an unprecedented chance to connect with peers, regulators, and industry partners. The industry had an invaluable opportunity to discuss the latest trends in licensing and supervision face-to-face with regulators. Other breakout sessions addressed hot topics such as policy shifts, legislative changes, and the expanding impact of the 2024 presidential election on federal nonbank policy.

The Conference of State Bank Supervisors (CSBS) hosted training sessions on NMLS basics, usability testing, and enhancements to user experiences. Sessions also helped users prepare for current and upcoming changes in individual licensing and training resources. Additional sessions targeted cybersecurity and compliance challenges, BSA/AML reviews, call reports, and bank relationships for MSBs.

Overall, #NMLS2025 was a comprehensive platform for both the industry and regulators to share knowledge, address challenges, and discuss exciting future developments in the NMLS ecosystem!

If you would like additional information about AI in Financial Services or wish to discuss how Ankura can assist with your state license acquisition or maintenance needs, please email Jake at **jake.hines@ankura.com**, Jesus at **jesus.torres@ankura.com**, or Trish at **trish.lagodzinski@ankura.com**.

Nationwide Multistate Licensing System

NMLS CORNER

State News from NMLS

Wisconsin Department of Financial Institution Added 6 New License Types to NMLS as of January 2025 including the following four new Company License types and 2 Branch License types for the Wisconsin Department of Financial Institutions:

- **Insurance Premium Finance Company License**
- **Currency Exchange License - (Company License)**
- **Currency Exchange Registration (Main Office-No Activity)- (Company License)**
- **Collection Agency Branch License**
- **Currency Exchange Branch License**

Click **here** for more information.

Existing Wisconsin Collection Agency, Currency Exchange, and Insurance Premium Finance Company Licensees are required to transition the license to NMLS. Additionally, existing Wisconsin Loan Companies are required to transition the license to NMLS. All current Loan Company licensees were required to complete the transition their licenses to NMLS by January 31, 2025. Click **here** for more information.

New Kansas Money Transmission Act (KMTA) became effective on January 1, 2025

The New Kansas Money Transmission Act (KMTA) became effective on January 1, 2025. All current money transmitter licensees and any future applicants should review the new law in its entirety to determine how the changes will affect your company's money transmission services in Kansas. Click **here** for more information.

Minnesota Adds Student Lender Registration to NMLS

NMLS has begun accepting new applications for the Minnesota Department of Commerce Student Lender Registration. According to MN Stat. 58B.051, lenders must be registered with the Department prior to offering services in Minnesota effective January 1, 2025. Click **here** for more information.

Kansas Office of the State Bank Commissioner Added New Earned Wage Access Services Provider License to NMLS on October 21, 2025

The Kansas Office of the State Bank Commissioner started receiving new application filings in NMLS for the Earned Wage Access Services Provider License starting on October 21, 2024. Click **here** for more information.

CA DFPI Added 4 New Registrations to NMLS

NMLS has begun receiving new application filings for the California Department of Financial Protection and Innovation (DFPI). New applicants can now submit these records through NMLS for the following registration types:

- **California Consumer Financial Protection Law (CCFPL) Registration - Student Debt Relief Services**
- **California Consumer Financial Protection Law (CCFPL) Registration - Debt Settlement Services**
- **California Consumer Financial Protection Law (CCFPL) Registration – Income-Based Advances**
- **California Consumer Financial Protection Law (CCFPL) Registration – Education Financing**

Click **here** for more information on the CCFPL and the new registration regulations.

Nationwide Multistate Licensing System

NMLS CORNER

Wisconsin Added Money Transmitter License to NMLS

NMLS began receiving new application filings for the Wisconsin Department of Financial Institutions Money Transmitter License, formerly the Wisconsin Seller of Checks License on October 1, 2024. Act 2

67 is Wisconsin's version of the Money Transmission Modernization Act and became effective January 1, 2025. Click **here** for more information.

Other News from NMLS

NMLS Processing Fee Change, Effective March 1, 2025

In December 2024, the CSBS Board of Directors approved an increase for NMLS processing fees. The fee increase will take effect March 1, 2025.

Starting March 1, 2025, NMLS users will see the new NMLS processing fees reflected in the system. Visit the **NMLS Processing Fee page** on the NMLS Resource Center for more information on NMLS fees, including an overview of the fees that will take effect March 1, 2025.

New Blog – NMLS Modernization: What We've Learned From Users So Far and What's Next

NMLS enhancements completed in July 2024 introduced a new login process for NMLS users, including the ability to access multiple NMLS accounts using a single login.

In October 2024, we surveyed a select group of NMLS users to find out what they think about the system updates. **Read the full blog** to learn about the survey results and find out what's being developed next as part of NMLS modernization.

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. View a **summary** of the updates.

New Blog: NMLS Modernization Phase One Adoption Makes Steady Progress

CSBS completed Phase One of NMLS modernization **enhancements**. Two key enhancements included introducing a new login experience and the ability for NMLS users with more than one NMLS account to access all their accounts using their new, single login. With these enhancements, CSBS set goals to track and achieve user change or "adoption" of the system changes. Specifically, an internal NMLS team has been focused on driving and increasing the number of active individual accounts modernized or "updated."

Key adoption metrics as of October 14, 2024:

- Active Industry Accounts Modernized: **216,713 (28.6%)**
- Accounts Adding Multiple Recovery Options: **107,261 (54.1%)**
- Active Individual Accounts Modernized: **170,234 (24.2%)**
- Estimated Logins with at least one Consolidated Account: **9,320 (76.2%)**

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

LEGISLATIVE UPDATES

- **Massachusetts adopted MTMA – Statue now includes domestic money transmission. Effective date January 1, 2026.**
- **Illinois adopted MTMA – Effective January 1, 2026.**
- **Iowa adopted MTMA – Recently added limited payroll processor exemptions, retroactive to July 2023.**
- **Alaska, Colorado, Mississippi, Nebraska and Virgina have introduced MTMA and is pending.**

By Eric Gagnon

Exam Time: Understanding Exam Ratings

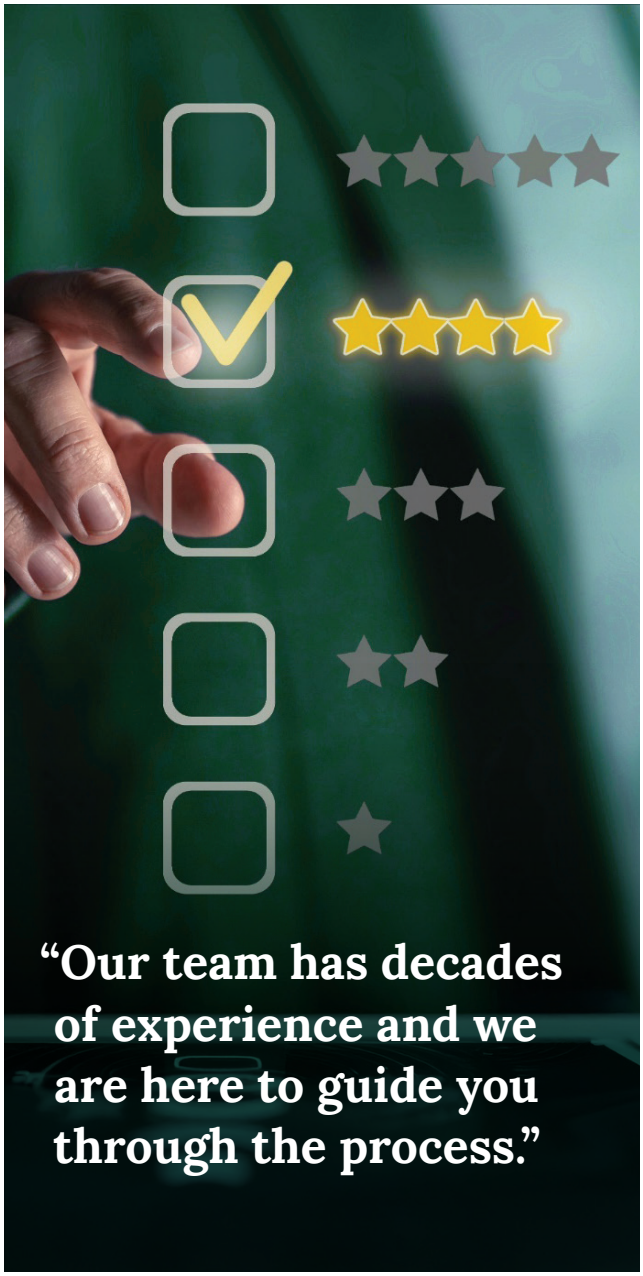
It is inevitable that your Money Service Business (MSB) will eventually receive a much-anticipated (or in some instances, much-dreaded) Exam Engagement letter from one or more states. MSBs licensed in 40 or more states meet the eligibility for a coordinated multi-state exam, a program that enables multiple states to coordinate their examination efforts, aimed at reducing the administrative burden on the licensee. With a large multi-state exam, licensees typically receive notification at least two months prior to the commencement of the multi-state coordinated exam.

> **"It is inevitable that your Money Service Business (MSB) will eventually receive a much-anticipated Exam Engagement letter "**

These examinations can encompass a wide breadth of business areas, including (but not limited to):

- **Changes in ownership, control parties, and executive management**
- **Delegate and agent agreements (along with any associated onboarding and monitoring procedures)**
- **Disclosures and notices to customers**
- **Surety bond coverage**
- **Overall financial condition, safety, and soundness**
- **Permissible investments (including their quality and applicability)**
- **Periodic reporting and reconciliation of transactions to permissible investments**
- **Reporting of any regulatory actions**
- **An increasing number of information technology topics**
- **Disaster recovery plan/business continuity planning and testing**

- **FinCEN renewals**
- **Filing of Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs)**
- **Title 31, Chapter X, Bank Secrecy Act compliance**
- **Title 12, Remittance Rule adherence**
- **Gramm-Leach-Bliley Act considerations**
- **Compliance with the USA Patriot Act**



Once the information has been collected, the interviews have been completed, and the participating states compile their individual state modules/respective components, a composite rating will be assigned. It is important to remember that receiving a "3" rating is not catastrophic – do not panic! A "3" merely indicates that there is room for improvement. You should also walk into your examination knowing that, although a "1" should be the goal, a "1" composite rating is rare. Many money transmitters fall within the "2" and "3" range.

But what do these ratings really mean?

Rating of a "1" (Strong overall Condition)

Money transmitters rated a composite "1" are sound in every respect and in substantial compliance with laws and regulations. Any findings or weaknesses noted are relatively minor and can be corrected in the normal course of business. If you receive a "1," take a breath, celebrate what should certainly be considered a win, and keep moving forward with a focus on maintaining and upgrading your culture of compliance.

Rating "2" (Satisfactory Overall Condition)

Money transmitters rated a composite "2" are fundamentally sound and in substantial compliance with laws and regulations. Only moderate weaknesses are present and can be corrected in the normal course of business with management's capabilities and willingness. If you receive a "2," you are on the right track but still need to make some relatively minor enhancements.

Rating "3" (Marginal Overall Condition)

Money transmitters rated a composite "3" exhibit a combination of weaknesses that range from less than satisfactory to moderately severe, and violations of laws and regulations may be evident and/or recurring. The money transmitter may not be resistant to adverse business conditions. The money transmitter's risk management practices may not be properly scaled to match the organization's size, complexity, and risk profile.

Recordkeeping and adherence to anti-money laundering policies and procedures may be deficient and less than acceptable. If you receive a "3" rating, it is time to buckle down and work on remediation; there are some larger issues present, but with the proper work, you can overcome them.

Rating "4" (Unsatisfactory Overall Condition)

Money transmitters rated a composite "4" exhibit serious weaknesses and/or violations of laws and regulations that may be recurring that cause its overall condition to be unsafe and unsound. Serious financial and/or managerial deficiencies may result in conditions that threaten the money transmitter's viability. A rating of "4" indicates there is significant and urgent work needed to remediate identified issues and should be taken seriously.

Rating "5" (Poor Overall Condition)

Money transmitters rated a composite "5" exhibit critical weaknesses and a combination of other identified weaknesses and/or violations of laws and regulations that may be recurring that cause its overall condition to be considered extremely unsafe and unsound. The volume and severity of problems are beyond management's ability and willingness to control and correct.

Now that you know what your exam rating means, you can effectively decide on a proper course of remediation.

Should your MSB receive an exam engagement letter, we invite you to reach out to us. Our team has decades of experience, and we are here to guide you through the process, along with assisting in addressing any findings that may arise as a result of the examination.

FOR MORE INFORMATION CONTACT

Eric Gagnon

Managing Director at Ankura

✉ **eric.gagnon@ankura.com**

Eric Gagnon is a Managing Director at Ankura (Chartwell Compliance) based in Vermont. Eric has over 22 years of experience in banking, securities, trust, money service business, and lending. He provides a broad range of licensing and consulting services involving the establishment of a new money service business, investment advisory, and consumer finance along with other financial licensing scenarios in the U.S. and Canada.

Eric is a former Examiner with the Vermont Department of Financial Regulation and former Area Financial Manager with the Florida Office of Financial Regulation. During this time Eric was involved with risk-based examinations, investigations, and licensing of money service business (MSB), virtual currency, trust company, bank, credit union, investment advisors, broker dealers, and lending companies.

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.

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 efective 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.

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 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 CAFP, CCI, CRCM, PMI-RMP, and PMP

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

Special thanks to Claire Howard, Marisa Macri, Ian Ciesla, and all the authors for their valuable contributions to this publication.

WE ARE HONORED TO BE RECOGNIZED BY THE FOLLOWING ORGANIZATIONS

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