Risky Business: How Fintech Firms Can Build Better AML and Sanctions Risk Assessments

By Anne Walton and J.P. Brennan, CFE, CBP

Introduction

The year 2023 promises to be exciting for Fintech. On the upside, the web 3.0 economy is poised for significant growth as decentralization favors creatives and community with its lower costs and lower barriers to entry infrastructure. The downside will come in the form of more lawsuits, regulatory uncertainty, perpetuation of scams, and operating in the dust of the crypto fallout and FTX criminal case. This all means this year will be anything but dull.

One of the best moves any up-and-coming Fintech can make is to not repeat lessons of the past, particularly those of 2022; the vast majority of which haven't been complex, per se, and could have likely been mitigated by identifying, understanding, and handling anticipated risks.

Consequently, it is highly advisable to take stock of existing bank partner relationships and revisit your anti-money laundering (AML) and sanctions risk assessment. Clarity on both is critical to weathering any potential regulatory storm focused on Fintech-heavy banks or the Fintech industry itself, particularly those in lending, *neobanks* that provide non-traditional banking, and payments.

One of the easiest lessons that can be implemented into any business can be summed up by the philosopher George Santayana's famous quote: "Those who do not remember the past are condemned to repeat it." There are basic needs that most companies require including internal controls, accounting and financial systems, and compliance to name a few.

This article examines the risks that Fintech firms are facing and what they need to do to create an ongoing AML and sanctions compliance program that will meet regulatory requirements.

For now, let's analyze a Fintech company's compliance needs. One of the most important moves any enterprising Fintech can make, especially in today's regulatory environment, is to put in place a board-approved AML and sanctions policy that is based on a comprehensive risk assessment.

The Importance of AML Risk Assessments

A high-quality and dynamic AML and sanctions risk assessment process is a key element to a best-in-class regulatory compliance program for Fintech firms and the banks. In both cases, full transparency of the inherent risk facing the business by virtue of its customers, third-party relationships, products, and locations as well as the strength of the controls in place to mitigate those risks, enables a Fintech to obtain a clear picture of the current and future risks facing the firm.

Inherent risk is the natural level of risk in a process or activity that is left unmitigated. For example, a third-party payment processor provides fiat on and off ramps for crypto exchanges and product users

(customers) that live all over the world. An inherent risk is that some of those customers may be subject to sanctions by the Office of Foreign Asset Control (OFAC) or reside in a sanctioned country. An AML and sanctions risk assessment attempts to quantify and calculate the level of this risk and others such as the risk inherent in the product that provides cross border payments and access to crypto. U.S. regulatory requirements mandate that a system of controls be in place to mitigate the inherent risks to the business that, among other things, a sanctioned individual will open an account or gain access to the payment product to launder the proceeds of illicit activity.

The strongest and most comprehensive AML and sanctions risk assessments rely on accurate data on all customer and relationship types, geographies, products, and transaction values and volumes. On the control side, details on the performance, frequency, and ownership of compliance controls are necessary to determine the strength and effectiveness of risk mitigation.

A data-driven risk assessment provides great value for Fintech firms of all sizes, whether it's an early-stage start-up getting ready to launch, or an established enterprise. The annual practice of evaluating AML and sanctions risks to the business, including concentration and regulatory risks, demonstrates to regulators that the firm takes its responsibilities as a gatekeeper to the financial system seriously.

Ensuring Success

To guarantee that the risk assessment process is a success; keep in mind the following factors:

Know your why.

To be successful in this endeavor, a Fintech company must be crystal clear on the purpose of a risk assessment. It is a regulatory expectation and best business practice. Moreover, the absence of one isn't a good look. This means that people at ***ALL*** levels—from the board of directors to the most junior team member—need to know that a risk assessment is used to identify money laundering and other illicit finance risks. This is important because it helps protect the business from reputational damage and regulatory fines and penalties.

Risk assessments are demanding processes that often expose elements of the business to increased scrutiny by asking hard questions about products and services. Leaders need to be prepared to be uncomfortable. For example, good data is needed to quantify risk and produce a strong assessment. Data quality and integrity are easy to overlook when a business is in growth mode. Tension may surface when teams are asked to produce customer or product data and can't or won't. In our experience, a strong leader with a compliance mindset that reinforces the value of this process and encourages constructive dialogue between stakeholders is the most successful in risk identification and mitigation. A Fintech can overcome limitations or solve problems such as these when the importance of doing so is known and agreed upon by *everyone* within the organization and reaffirmed by a strong tone at the top.

Share the results.

Talk about it when you are done. Circulate business-relevant results throughout the institution. Present the risk assessment to the board and risk committees, discuss it, and make sure it is understood within the firm.

Too often the process is so demanding and difficult for compliance teams that it ends with silence. Don't let this happen to you. Make a commitment at the launch of the process. Give compliance a platform to

share results with team members in a variety of ways. Use forums such as town halls or informal conversations to reinforce the importance of risk assessment and its value to everyone.

Communication is critical to the development and maintenance of a healthy organizational culture in the Fintech industry and elsewhere. It is sound business advice, and it applies to a compliance cost center as much as it does to a revenue-generating one. Clear, consistent messaging about the risk assessment reinforces the *"why"* and fosters trust among team members.

When people know and understand the results, they may be more apt to use that information as a driver for resource allocation – including technology investments and personnel. Tie the results to the transaction-monitoring coverage strategy and consider if testing and adjustments need to be made to optimize business and compliance functions.

Rinse and repeat.

Do it again and again. Risks are not static, and the assessment (process, execution, circulation) needs to occur on a continuous basis to remain relevant and provide value to senior management.

Conversations about risk assessments as a normal part of business-as-usual need to happen periodically between compliance and the business. Senior management should ensure the assessment is updated to reflect new business lines and remain proportional to the size and complexity of the institution.

Conclusion

AML and sanctions risk assessments are a critical, yet frequently overlooked and underutilized element of a robust compliance program. Despite being time consuming and demanding, the results produced by a rigorous, data-driven assessment provide senior leaders with a road map for the future. These assessments provide a gateway for growth and expose unmitigated risks that may worsen due to weak or absent controls and result in regulatory fines and reputational damage.

Acknowledgments

We would like to thank Anne Walton and J.P. Brennan for providing insight and expertise that greatly assisted this research.

Anne Walton is a Senior Director in the Anti-Money Laundering division of J.S. Held's **Global Investigations practice**. Anne specializes in building and monitoring anti-money laundering (AML) and sanctions compliance programs. Her prior investigative and risk management experience involved evaluating financial crimes compliance (AML / BSA / OFAC) cyber and physical security policies and programs. Anne's past clients include financial institutions in APAC, Europe, and the Middle East; Fortune 500 companies; Fintech; banks serving crypto firms; non-governmental organizations; and local, state, and federal government.

Her expertise also includes Know Your Customer (KYC) evaluations and file reviews and testing; due diligence investigations of entities and high-profile and high-net-worth individuals, physical security risk assessments of critical infrastructure, Department of Homeland Security (DHS) cybersecurity tabletop exercises, and training law enforcement and intelligence analysts via the DHS Advanced Analytic Technique Workshop.

Anne can be reached at anne.walton@jsheld.com or +1 248-564-2301.

JP Brennan is the Global Head of Fintech, Payments, Crypto Compliance and Investigations within the Global Investigations practice at J.S. Held. A certified fraud examiner(CFE) and certified bitcoin professional (CBP), he brings over 20 years of experience in forensic accounting, auditing, litigation consulting, anti-money laundering (AML) compliance, cryptocurrency regulatory compliance, OFAC / sanctions review, and complex enhanced and operational due diligence. He has an in-depth understanding of the complexities that many Fintechs are faced with concerning their regulatory framework as well as those issues from a financial crime compliance perspective.

He has substantial experience in providing complex forensic accounting and financial fraud investigative services, cryptocurrency asset / wallet tracing, development, and implementation of AML programs, outsourced Chief Compliance Officer services, as well as providing managed services for large-scale remediation and compliance projects. His clients include major law firms, cryptocurrency exchanges (centralized / decentralized), digital asset issuers, custodians, multinational banks, funds, payment processors, financial institutions, and investors.

J.P. can be reached at **jp.brennan@jsheld.com** or +1 917 244 8931.