FinCEN

Innovation Hours Program

Emerging Themes and Future Role in AML Act Implementation

(May 2019 - February 2021)

March 2021

I. EXECUTIVE SUMMARY

In May 2019, the Financial Crimes Enforcement Network (FinCEN) announced the Innovation Hours Program ("IH Program") to better understand financial services sector innovation related to anti-money laundering (AML) and countering the financing of terrorism (CFT) compliance, and to learn of new financial services offerings and related technologies. The IH Program provides a monthly forum for users and providers of regulatory and financial technology to share information about, and discuss potential opportunities and challenges of, their innovative products and services, to the benefit of both the private sector and government. Since that announcement, FinCEN has met with 65 U.S. and foreign firms, held 19 monthly IH sessions, including one event in New York City jointly hosted by the Office of the Comptroller of the Currency's (OCC) Office of Innovation.

The IH Program supports FinCEN's broader Innovation Initiative, which was launched in December 2018 in conjunction with the release of the *Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing* (December 3, 2018) (Joint Statement). The Innovation Initiative is a multilayered approach to ensure our national security by promoting responsible financial services innovation to further the purposes of the Bank Secrecy Act (BSA) and related AML/CFT efforts.

Since inception, the IH Program has:

1. Improved FinCEN's understanding of the technologies and financial services solutions arriving in the marketplace.
2. Enhanced technology and financial services solution providers' awareness of BSA/AML obligations so their solutions and products will better assist their customers' compliance.
3. Informed FinCEN, Treasury, and other federal government policy and operational deliberations related to emerging technologies and processes, such as artificial intelligence (AI) or digital identity (digital ID).
4. Supported FinCEN efforts to reform the BSA regulatory framework so that it supports responsible innovation and can adapt to rapidly changing technologies and business processes.
5. Helped FinCEN identify vulnerabilities associated with emerging financial technology or value transfers, and inform efforts to address the vulnerability.

FinCEN expects to continue these efforts to fulfill its commitment to incubate responsible AML/CFT innovation. These efforts also will help FinCEN address the new requirements of the AML Act of 2020.[1]

1. The AML Act was enacted as part of the National Defense Authorization Act for Fiscal Year 2021 (*see*, Public Law 116-283, §§ 6001-6314).

II. Introduction

FinCEN's Innovation Initiative is a multilayered effort to ensure our national security by promoting responsible AML/CFT innovation that includes (1) the FinCEN IH Program, (2) exceptive relief pilots that facilitate innovative solutions to address AML/CFT compliance, (3) information sharing programs, and (4) workshops to identify innovative solutions to specific AML/CFT challenges. FinCEN is evaluating other activities to support the Initiative in the long term, such as facilitating demonstration and application testing capabilities (FinCEN innovation hub).

When it launched its Innovation Initiative, FinCEN committed to share the lessons learned through the IH Program to support the adoption of innovative AML/CFT solutions and new financial services products and services that support the goals of the BSA. FinCEN issued an initial status update on the IH Program in July 2020, highlighting the shift from in-person to virtual meetings in response to the COVID-19 pandemic. The update also noted the IH Program would increasingly focus on understanding new and innovative approaches to payments and movements of value while supporting FinCEN's diversity goals through greater outreach to firms founded, owned, or led by underserved groups. This report further describes the high-level themes and policy implications emerging from the IH Program.

Background

Each monthly IH Program session typically involved three separate meetings with individual firms—providers of regulatory and financial technology (RegTech and FinTech)—that applied and were selected to participate in the IH Program. During each meeting, the firm provided information about its solutions or products, focusing on how the solution or product addresses the challenges of AML/CFT or helps to provide financial services that comply with the BSA and its regulatory framework. The firm also demonstrated its product(s) or solution(s), and had a general discussion with FinCEN on its uses and capabilities. During the sessions, the firms had the opportunity to raise general legal, regulatory, or other issues. Participants were cautioned, however, that the IH Program was not (i) a replacement for formal guidance or administrative ruling requests, or (ii) an alternative to the existing procurement processes.[2]

From July 2019 through February 2021, the IH Program held 18 sessions (ten were held remotely because of the COVID-19 pandemic). FinCEN also held a regional IH Program event in New York in November 2019, in partnership with the Office of the Comptroller of the Currency's (OCC's) Office of Innovation. In total, FinCEN met with 65 U.S. and foreign firms (52 in the monthly IH sessions, and 13 during the New York event). Participants in the IH Program were from across the United States and abroad, and included a wide variety of FinTech, RegTech, and supervisory technology (SupTech) firms, as well as financial institutions.

2. Information on the IH Program and its participation requirements and limitations are publicly available at https://www.fincen.gov/resources/fincens-innovation-hours-program.

The firms presented solutions during their IH Program meetings involving AI/machine learning, homomorphic encryption and other privacy enhancing technologies, blockchain/ distributed ledger, digital ID, cybersecurity, biometrics, geolocation, beneficial ownership identification, sanctions screening, risk assessment and mitigation, and other innovative business solutions and technologies. The discussions provided unique opportunities for FinCEN to understand the application of these technologies and the resulting tools or solutions within the financial services and other industries. The meetings also provided insight into both the challenges and opportunities the technologies create for more effectively securing the U.S. financial system and combating illicit financial activity. Additionally, the firms and their solutions had a wide range of customers: banks, credit unions, money services businesses, gaming firms, loan and credit associations, insurance and other financial services firms, as well as the public sector (state and federal regulators, law enforcement and national security agencies, etc.).

Before the IH Program moved to an all-virtual format, FinCEN jointly conducted a special New York Regional Innovation Hours event with the OCC's Office of Innovation in its Manhattan regional office. During this two-day event on November 13-14, 2019, FinCEN met with 13 firms. The interagency cooperation between FinCEN and OCC in hosting this event produced valuable insight into four key areas related to AML/CFT and sanctions regulatory and supervisory technology efforts: identity resolution, information sharing, risk assessment and mitigation, and transaction monitoring/sanctions filtering. Shared themes arising throughout multiple firms' solutions included unique risk assessment or risk identification and mitigation solutions, and challenges associated with ensuring the availability of high-quality data.

III. EMERGING THEMES

The IH Program has provided important insight into opportunities for financial services innovation and how to overcome impediments to adopting that innovation. Prior to the IH Program, FinCEN's understanding of these issues was largely based on interactions with financial institutions. FinCEN had less insight into the perspectives of the firms creating the AML/CFT or sanctions compliance solutions for financial institutions. Now, after more than 18 months of engagement with these firms, FinCEN has a more fulsome understanding of the important issues with industry adoption of responsible AML/CFT innovation.

Availability of Relevant AML/CFT Solutions. The IH Program has confirmed there are various solutions already available for many of the AML/CFT challenges that financial institutions face—particularly supporting compliance with existing funds transfer and recordkeeping requirements[3] for convertible virtual currency exchangers and administrators or use of digital identity solutions for customer identification program (CIP) requirements.[4] However, financial institutions may not be sufficiently aware of these solutions, particularly those being created by new or smaller firms, nor how those solutions may address the financial institutions' compliance needs.

3. *See generally* 31 CFR 1010.410.
4. *See* 31 31 C.F.R. § 1020.220 (FinCEN); 12 C.F.R. § 21.21(c)(2) (OCC); 12 C.F.R. §§ 208.63(b)(2) and 211.24(j)(2) (Federal Reserve); 12 C.F.R. § 326.8(b)(2) (FDIC); and 12 C.F.R. § 748.2(b)(2) (NCUA) (collectively, the CIP rules).

Sources of Financial Institution Reluctance to Innovate. The IH sessions often highlighted that the BSA requirements, in and of themselves, are often not the primary causes of industry reluctance to adopt new technologies (such as digital ID or confidential information sharing technologies). Instead, concerns among client financial institutions often revolved around how their federal or state examiners or their own internal or external auditors would react to attempts to try something new; the Joint Statement and its incorporation into examiner procedures should ameliorate this concern over time.[5] Other common concerns involved potential legal liability that might arise from reliance on the solutions, sensitivity to sharing valuable business information (such as customer-related data) with competitors, and the ability of solutions to meet data privacy laws and regulations.

Digital ID. Technology solution providers emphasized that, based on their experiences, the financial services industry's hesitation to use digital ID solutions included concern for potential examination and internal or external audit risk in adopting these solutions, and those clients are more reluctant to change from better understood existing solutions. Another common concern is the nature of the general contractual liability arrangements under which reliance on third-party provided information and solutions is established. Finally, more fundamental business concerns about sharing customer information or unique business processes also may inhibit the adoption of solutions involving competitors.

Maintaining Confidentiality of Shared Information. Companies demonstrated the existing availability of encrypted homomorphic/zero-knowledge-proof technologies to support the sharing of information and data consistent with data privacy requirements. Yet industry's adoption of these technologies remains limited. From the perspective of these solution providers, the primary challenge in obtaining industry adoption is a fundamental one, notably building trust within industry around the solutions and how competitors will use the shared knowledge. FinCEN's clarifications regarding the acceptable use of the USA PATRIOT Section 314(b) information sharing safe harbor in December 2020, and the AML Act of 2020's further encouragement of information sharing should help further build trust across industry.

Financial Crime Data for Testing. There is a lack of anonymized (also referred to as "synthetic" or "artificial") financial crime data that, if available, would enable AML/CFT product and solution providers (as well as their financial institution customers) to mirror what is seen in reality when reviewing actual criminal activity, associated financial transactions and customer behaviors. Industry's ability to properly train and test applications using AI and machine learning is thereby constrained. This limitation can be partially overcome within individual client relationships and, where there is sufficient trust to support privacy-based information sharing (including sharing of typologies rather than actual customer and transactional data), in broader groupings of client information for a single solution provider. To fill the broader gap in testing data, however, industry is increasingly looking to the public sector. FinCEN's public SAR Statistics database

5. *See* Federal Financial Institutions Examination Council (FFIEC) *Bank Secrecy Act (BSA) /Anti-Money Laundering (AML) Examination Manual*, Scoping and Planning Section, "Developing the BSA/AML Examination Plan" (April 2020), pages 10-11. *See also* "Assessing Compliance with BSA Regulatory Requirements" (February 2021).

(SAR Stats) has become an important tool in addressing this need. Along with FinCEN advisories and other public typology and risk indicator information, solution providers have used the data available through SAR Stats to develop risk assessment, transaction monitoring, and other AML/CFT compliance tools and trainings.

Virtual Currency. Industry and FinCEN have seen a rapid increase in business e-mail compromise and account takeover schemes, ransomware attacks, and other cyber-enabled thefts and frauds, particularly during the COVID-19 pandemic. One common feature of these crimes is their frequent use of convertible virtual currencies (CVC). Through the IH Program, FinCEN has learned of new industry solutions to address the CVC element of these crimes. These solutions providers are already working with victims and law enforcement and are potential information-sharing partners for FinCEN's efforts to responding to virtual currency thefts. The dialogue is leading to the development of broader coordinated efforts to address the growing challenge of the use of CVC for criminal purposes. For example, as part of a special IH Program event in December 2020, FinCEN learned about a series of new innovative solutions developed through tech sprints (also known as "hackathons") to find perpetrators of child sexual abuse materials and to track the perpetrators' use of CVC.

Impact on U.S. Government Policy and FinCEN Priorities

Since its inception, the IH Program also has successfully contributed to a range of U.S. government policy and FinCEN priorities.

Regulatory Reform. The IH Program has increased FinCEN's understanding of the capabilities and limitations in industry AML/CFT efforts by hearing directly from the technology solution providers and financial services innovators. This improved understanding has informed FinCEN's BSA regulatory reform efforts, including the issuance of recent frequently asked questions on suspicious activity reports (SARs). Those broader reform efforts, led by FinCEN and its counterpart federal banking agencies, have focused on enhancing the effectiveness of the AML/CFT regime and focusing compliance examinations on the outcomes of financial institution AML programs. The IH Program also has improved our ability to make future risk-based and data-driven decisions on other areas that may require action, such as the use of digital ID to meet existing BSA customer identification program requirements. This greater understanding of the "possible" enables FinCEN to work more collaboratively with industry to identify potential innovative solutions to challenging AML/CFT issues, including to implement AML Act requirements related to (1) information sharing, (2) pilot programs, and (3) streamlining and making more effective SAR and currency transaction report (CTR) filing requirements and processes.

National Security. The IH Program directly supports FinCEN's efforts to protect U.S. national security. The IH Program enhances FinCEN's ability to address strategic risks threatening U.S. national security, and informs FinCEN's understanding of illicit trends and evolving capabilities across industry to help combat these threats by enabling better detection, prevention, and reporting. The IH Program already has provided FinCEN with new insight into the risks associated with CVC, assisting FinCEN efforts to identify compliance vulnerabilities and potential threats.

Informing Public Policy and Inter-Agency Collaboration. The IH Program supports FinCEN's ability to inform U.S. policy and operational deliberations related to emerging technologies and processes. More broadly, the IH Program is helping create a platform for cross-agency cooperation and coordination of innovation-related efforts, consistent with the related requirements of the AML Act. FinCEN has benefited from the shared experience and insight of innovation offices at partner federal and state regulatory agencies. These relationships have provided best practices and practical lessons that informed the creation and operation of FinCEN's IH Program. This collaborative inter-agency approach also has helped to establish closer ties and information sharing on areas of mutual interest in emerging technologies and financial services. The fruits of this approach have included (1) the joint IH event in New York in November 2019 with the OCC, (2) regular meetings and sharing of insight on shared topics of interest (such as blockchain) with Treasury's Bureau of the Fiscal Service's Office of Financial Innovation and Transformation, and (3) other supportive collaborations with additional federal and state partners, such as New York's Department of Financial Services and its recent CVC-related Techsprint. Further developing this collaboration and information sharing among innovation offices will be crucial to realizing the cross-agency cooperation and coordination of innovation-related efforts envisioned in the AML Act.

IV. FUTURE PLANS

FinCEN's leadership on innovation will expand substantially over the coming years given new authorities provided by the AML Act. Using these new authorities to fully and effectively implement the AML Act's requirements, FinCEN will leverage the IH Program to support the following innovation plans:

FinCEN Organizational Activities

Establish a Formal BSA Innovation Officer. Consistent with the AML Act's requirements, FinCEN will formally establish the position of BSA Innovation Officer. The BSA Innovation Officer will coordinate with the Innovation Officers of other regulatory agencies, law enforcement, and industry on efforts to implement responsible innovation and adopt supportive new technology. Through the BSA Innovation Officer, FinCEN will collaborate with other federal and state innovation offices on efforts relevant to national AML/CFT priorities. The BSA Innovation Officer also will initiate planning for and development of an application test lab and more comprehensive innovation demonstration capabilities.

Expand the IH Program. Building on the success of the IH Program monthly meetings and New York regional event, FinCEN will host additional periodic workshops to facilitate targeted innovation focused on specific threats and vulnerabilities of the U.S. and global financial system, particularly in the area of CVC. These events also will focus on understanding new and innovative approaches to payments and movements of value, as well as supporting FinCEN's diversity goals through greater outreach to firms founded, owned, or led by underserved groups.

Establish a Bank Secrecy Act Advisory Group (BSAAG) Subcommittee on Innovation and Technology. The new Subcommittee will continue the ongoing work already being done in the BSAAG related to the challenges and opportunities of FinTech and RegTech solutions and technologies. FinCEN also will develop the Financial Crimes Tech Symposium series announced on February 4, 2021, and host an inaugural event.

Establish a FinCEN BSA Information Security Officer and BSAAG Subcommittee on Information Security and Confidentiality. This Officer and Subcommittee will work closely with the FinCEN Innovation Officer and BSAAG Subcommittee on Innovation and Technology on efforts to support responsible AML/CFT innovation.

Regulatory and Policy Initiatives

Stand Up a Formal Pilot and Exceptive Relief Program. Consistent with the AML Act requirements, FinCEN will continue to support innovative AML/CFT pilots, particularly those already begun involving the sharing of SAR information among a financial institution's foreign branches, affiliates, and subsidaries. FinCEN also will continue to work with partner agencies to explore the development and use of innovative identity solutions.

Expand Information Sharing Efforts. Consistent with the related requirements of the AML Act, FinCEN will apply insight into how firms are developing new solutions to enable information sharing across financial institutions while protecting Personally Identifiable Information to ongoing efforts to enhance information sharing, including those related to USA PATRIOT Act Section 314(b) safe harbor protections for private sector information sharing.

Support Regulatory Standards for Assessing Innovative Solutions. FinCEN will work with regulatory partners to support the development of appropriate regulatory standards for assessing innovative solutions and their ability to facilitate compliance with BSA requirements. FinCEN also will co-lead the AML Act's required financial technology assessment to analyze the impact of FinTech on financial crimes compliance. To support these efforts, FinCEN will develop proposals for policy, regulatory, and guidance responses to new payment mechanisms and technologies. FinCEN also will draft white papers on industry and U.S. government digital ID and other innovations, and discuss their application for and challenges to AML/CFT compliance. To specifically address the gap in illicit financial activity training data for AI and machine learning solutions, FinCEN will begin the necessary planning to develop a synthetic version of BSA data (with no real BSA or publicly identifiable information) that has illicit financial activities incorporated into it to support stakeholder testing and training.

Improve CIP Requirements and Address Digital ID Challenges. FinCEN will prioritize the inclusion of identity validation solutions in IH Program sessions to enhance FinCEN's understanding of existing solutions that can enable financial institutions subject to the CIP rules (and non-bank financial institutions not subject to those rules) to obtain customer information from third-party sources as part of meeting requirements for validating and verifying identity. FinCEN will focus pilots and exceptive relief efforts on addressing the challenges of validating and verifying identity in an increasingly digital financial services environment. FinCEN also will consider policy and regulatory measures to improve digital ID verification and take steps to help reduce fraud associated with identify theft or synthetic identities and other identity-related challenges.

For Further Information

Questions or comments regarding the contents of this report should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorist financing, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.