VERAFIN

October 11, 2022

Verafin Solutions ULC
18 Hebron Way
St. John's, Newfoundland and Labrador
Canada A1C 2B8

Mr. Theodore J. Dowd, Deputy Chief Counsel
Chief Counsel's Office
Office of the Comptroller of the Currency
400 7th Street SW, Suite 3E-218
Washington, DC 20219

Subject: OCC Information Collection - *Bank Secrecy Act/Money Laundering Risk Assessment*
OMB Control Number 1557-0231

Dear Mr. Dowd:

Verafin appreciates the opportunity to comment on the recent Office of the Comptroller of Currency (OCC) notice and request for comment (RFC) on the revision of the information collection found in current regulations related to its *Bank Secrecy Act/Money Laundering Risk Assessment*, also known as the *Money Laundering Risk* (MLR) System as published in the Federal Register.[1]

The RFC solicits feedback from respondents (i.e., OCC-supervised community and trust *banks*) and the public on topics related to its annual *Risk Factor Summary (RFS) Form*, which collects information about certain higher-risk products, services, customers, and geographies (PSC). Specifically, the *RFS Form* updates described in the RFC include new and deleted PSCs, as well as the addition of two new *Money Transmit*ter types related to crypto-assets (i.e., exchanges and kiosks).

We have provided below details on Verafin, along with our general comments on the MLR System, *RFS Form* and annual submission process, including our suggestions for possible improvements to the current process. We have also provided responses to the specific questions posed in the RFC that we are in a position to answer, based on our experience and on the feedback we receive from our customers regarding their own MLR/RFS processes, experiences and challenges.

VERAFIN - AN INDUSTRY LEADER

Verafin is the industry leader in enterprise anti-financial crime management solutions, providing a secure, cloud-based software platform for fraud detection and management, BSA/AML compliance management, high-risk customer management, and information sharing. More than 3500 banks, credit unions and money services businesses, use Verafin to effectively fight financial crime and comply with regulations.

Leveraging its unique big data intelligence, visual storytelling, and collaborative investigation capabilities, Verafin significantly reduces false positive alerts, delivers context-rich insights, and streamlines the daunting BSA/AML compliance processes that financial institutions face today.

Verafin's all-in-one anti-financial crime platform provides digital asset companies with a full fiat-to-blockchain view of cryptocurrency activity. Verafin enhances the investigative process with visual investigation tools, case management, and regulatory reporting capabilities, increasing the efficiency and effectiveness of digital asset compliance programs.

---

[1] https://www.federalregister.gov/documents/2022/09/08/2022-19375/agency-information-collection-activities-information-collection-revision-submission-for-omb-review

Verafin also hosts the free FRAMLxchange, an association of financial institutions which facilitates information sharing between 314(b)-registered financial institutions to identify, monitor and report suspected money-laundering or terrorist financing.

GENERAL COMMENTS

Verafin has a long history of providing support to OCC-regulated community banks for their BSA/AML programs, including AML transaction monitoring, OFAC sanctions screening, and in supporting their overall BSA/AML risk assessment and higher-risk customer (HRC) management processes. We understand that the OCC collects the MLR/RFS information annually, and uses it for the following key activities:

1) BSA/AML Risk Assessment
2) Resource Allocation
3) Peer Reporting

Our comments below are based on a review of the RFC, the updated *RFS Form*, and the OCC's *MLR Supporting Statement* provided to the Office of Management and Budget for its review (NB: We did not have access to a copy of the OCC's MLR User Guide provided to banks to support the information collection process).

BSA/AML Risk Assessment

The OCC uses the MLR/RFS information to evaluate, on an annual basis, BSA/AML and OFAC risks in *individual* banks, as well as aggregate risks across banks and PSCs. In reviewing the *RFS Form*, we note that it includes more than 150 data fields covering 71 PSCs[2] grouped into 11 categories. In contrast, the FFIEC's *BSA/AML Examination Manual* identifies 29 categories of higher-risk PSCs for banks to consider when assessing their BSA/AML and OFAC risks, but notes that the identification of risk categories is *bank-specific*; in fact, there are *"no required risk categories, and the number and detail of these categories vary based on the bank's size or complexity, and organizational structure. Any single indicator does not necessarily determine the existence of lower or higher risk."[3]* Moreover, "*covered financial institutions are not required or expected to automatically categorize as "high risk" products or customer types listed in government publications*."[4] Agency guidance also has consistently clarified that there is no *one-size-fits-all* set of higher-risk categories, emphasizing that the risk-based approach is unique to each institution, and that "*no customer type presents a single level of uniform risk or a particular risk profile related to money laundering, terrorist financing, or other illicit financial activity."[5]*

Thus, although government publications may list specific products or customer types, it "*is not a requirement that covered financial institutions use a specific method or categorization to establish a customer risk profile*."[6] In the case of the MLR/RFS, therefore, imposing a rigid reporting structure of specific PSCs, and a prescriptive approach to identifying and assessing ML/TF risk, may be antithetical to the intent and practice of a bank's application of the risk-based approach within its BSA/AML and OFAC compliance programs.

Resource Allocation

Bank compliance staff and examiners alike have a vested interest in understanding the ML/TF risks posed by a bank's operations, both in relation to its own safety and soundness, as well as to the broader financial system. As noted by the FFIEC,[7] "*a well-developed BSA/AML risk assessment assists the bank in identifying ML/TF and other illicit financial activity risks and in developing appropriate internal controls (i.e., policies, procedures, and processes).*" Thus, the BSA/AML Risk Assessment process describes, guides and demonstrates how, on an ongoing basis, the bank will:

---

[2]

 NB: The RFC indicates that two (2) new crypto-asset-related items were being added under the *Money Transmitters* category (i.e., administrators and exchangers of virtual currency, and crypto ATM operators), however, the updated *RFS Form* we reviewed did not contain these additions. Presumably, this would increase the total number of PSCs from 71 to 73, by adding four (4) additional data fields (i.e., *Total Number*, and *Total Volume* for each).

[3] https://bsaaml.ffiec.gov/manual/BSAAMLRiskAssessment/01

[4] https://www.fincen.gov/sites/default/files/2020-08/FinCEN%20Guidance%20CDD%20508%20FINAL_2.pdf

[5] https://www.occ.treas.gov/news-issuances/bulletins/2022/bulletin-2022-18.html

[6] https://www.fincen.gov/sites/default/files/2020-08/FinCEN%20Guidance%20CDD%20508%20FINAL_2.pdf

[7] https://bsaaml.ffiec.gov/manual/BSAAMLRiskAssessment/01

1) identify and assess categories of risk (e.g., PSCs)
2) develop the necessary internal controls, and
3) mitigate the overall risk

In the context of an examination, the goal is to "*review the bank's BSA/AML risk assessment process, and determine whether the bank has adequately identified the ML/TF and other illicit financial activity risks within its banking operations*" (i.e., to ensure that the bank has identified *all* ML/TF risks, and is managing them in accordance with their Board-approved policies and procedures to ensure those risks are properly mitigated). And as the OCC correctly points out, "*[t]his risk assessment is critical for protecting U.S. financial institutions of all sizes from potential abuse from money laundering and terrorist financing.*"

The OCC's *MLR Supplementary Statement* notes that MLR/RFS information is used to "*identify those institutions, and business activities within institutions, that **pose heightened risk** and to allocate **examination resources** accordingly.*" (Emphasis added) While a heightened risk of ML/TF could place increased demands on examination resources, just as the statement suggests, here the definition of *heightened risk* is critical.

Specifically, the data collected through the MLR System provides the OCC with a representation of the *inherent risk* of certain set of PSCs (see **item 1** above), based only the number and volume of each; however, *inherent risk* does not necessarily equate to, or correlate directly with, *heightened risk*.

For example, a well-managed program at Bank A, with large numbers of customers and high volumes of transactions in most PSC categories, may have a high degree of inherent risk, but a relatively low degree of residual risk due to the effectiveness of the bank's internal controls (see **item 3** above). As such, it may present significantly *less* risk than a smaller, less well-managed program at Bank B, with only a few customers and low transaction volumes (i.e., where the *residual risk* remains high due to the bank's lack of any corresponding internal controls).

In other words, higher numbers of customers/accounts and/or transaction volumes, within each PSCs or groups of PSCs captured in the MLR/RFS data, *does not* necessarily correlate to a heightened risk of money laundering or terrorist financing because it fails to account for the internal controls the bank has put in place to manage and mitigate those same risks.

In this scenario, the MLR/RFS data could mistakenly suggest that Bank A has a "heightened risk" and, as such, should be allocated additional examination resources. Use of *inherent risk* as a proxy for *heightened risk*, therefore, could cause an over-allocation of resources to some banks, and an under-allocation of resources to others. It is also unclear the exact extent to which differences in MLR/RFS data impact resource allocation decisions (e.g., exactly how the collected numbers and volumes of PSCs relate to assigning examination resources to various districts or individual banks), or whether the level of resources assigned, based on *inherent risk* data, were sufficient and matched the degree of *heightened risk* encountered or not.

Peer Reporting
In addition to its own use of the MLR/RFS data (e.g., for the purposes allocating exam resources, as discussed above), the RFC states that "*[the] OCC also provides bank-specific and anonymized peer group information gathered through the MLR system to each individual reporting bank. Peer group data can be used by banks to determine outliers, inconsistencies, or deviations from standard norms. Banks can also conduct comparison and trend analyses concerning their data and peer data.*" While this may be possible for banks who adopt the exact set of PSCs contained in the *RFS Form*, some MLR/RFS data may be more granular than might otherwise be necessary for the bank to manage the ML/TF risks it identified through its BSA/AML Risk Assessment process.

Banks also may need to go to internal systems and operational resources outside of BSA/AML and OFAC compliance to obtain the data necessary to meet the OCC's annual MLR/RFS reporting obligations, but they may not otherwise use the PSC-specific data in their BSA/AML program. Anonymized, aggregate peer benchmarking data that is associated with measures of inherent risks for a specific set of PSCs (i.e., that are *not identical* to the higher-risk risk categories a bank also identifies through its own ongoing BSA/AML Risk Assessment process) may be of limited value. Gathering and

reporting a data for the *RFS Form* that does not align with the higher-risk categories identified by the bank' during its BSA/AML Risk Assessment processes reduces the bank's resources available to identify suspicious activity and provide information that could be useful to law enforcement in identifying and prosecuting ML/TF and other financial crimes.

Responses to Specific Questions

a) *Whether the collection of information is necessary for the proper performance of the functions of the agency, including whether the information has practical utility*

Based on our *General Comments* above, we question the prudential and supervisory benefit of the annual information collection represented by the *RFS Form,* and wonder if the OCC might be able to achieve the same goals without the additional reporting burden that results from imposing a prescriptive set of categories upon a framework that is intended to be risk-based, flexible and bank-specific.

The OCC acknowledges that it expects BSA/AML and OFAC risks to change as "new products and services are introduced, existing products and services change, and banks expand through mergers and acquisitions." However, unlike the bank's own BSA/AML risk assessment, which is regularly assessed and evaluated as product and services change (and prompts changes to the risk categories and risk factors that are being tracked and managed), the MLR does not allow for such changes to be captured in a timely manner, thereby limiting the utility of the information in highlighting emerging risks. The annual collection of data on *Total Number* and *Total Volume* for a limited set of PSCs may not be particularly responsive to identifying emerging areas of heightened risk that should perhaps become a focus of examination efforts (though such areas of emergent, heightened risk likely *are* identified during the bank's ongoing BSA/AML Risk Assessment process).

b) *The accuracy of the agency's estimate of the burden of the collection of information*

The level of effort and total cost of resources required for a bank to gather and annually report MLR/RFS data can vary greatly. It will depend, at least in part, on the extent to which the risk categories identified through the bank's BSA/AML Risk Assessment align with/adhere to the PSCs identified on the *RFS Form*.

According to its *MLR Supporting Statement*, the OCC "*has observed that the systems most banks currently maintain for MLR data collection purposes already support ready access to the data; thus, the changes to the MLR will not require additional significant investment in technology or systems to collect and report this data*," and that, based on these existing systems and the proposed changes to the MLR platform, "*the additional MLR data collection burden associated with the proposed changes will be minimal for banks of all sizes.*" In our experience, however, banks do not always have *ready access* to the requested data, because they do not always fully align their programs and processes with the same specific set of 71 PSCs used in the *RFS Form*. (They do, however, typically focus on a relevant subset of the 29 risk categories outlined in the FFIEC Examination Manual, some of which are also PSCs.)

Even if there was perfect alignment between PSCs and the bank's BSA/AML risk categories, it is also our experience that even a seemingly minor change to the information being requested (e.g., a few new PSCs or two new types of Money Transmitter related top crypto-assets) may impact the upfront and/or ongoing burden associated with gathering and reporting the new information.

Beyond the changes required to its IT systems, whenever the form or format of the requested data changes, banks also may need to make corresponding updates to their documented internal controls (e.g., BSA/AML and OFAC policies, process and procedures), and/or develop and deliver additional training to affected staff. These activities impose an additional burden on banks that may not be adequately accounted for in the OCC's current estimates.

c) *Ways to enhance the quality, utility, and clarity of the information to be collected*

The OCC could examine alternative ways of achieving the same objectives currently served by the MLR System. For example, the *RFS Form* could use the categories outlined in the FFIEC Examination Manual rather than the current set of PSCs. Use of the BSA/AML and OFAC *Quantity of Risk* matrices provided in Appendices J and M, respectively, could also be considered as these reflect a consideration of BSA-reporting data, as well as at least some level of mitigated ML/TF risks, which collectively are likely to provide a better indication of *heightened risk*.

d) *Ways to minimize the burden of the collection on respondents, including through the use of automated collection techniques or other forms of information technology*

In addition to the comments and suggestions already provided, the OCC should be careful not to inadvertently appropriate the risk-based approach and make the BSA/AML Risk Assessment process unnecessarily rigid and prescriptive.

We appreciate the opportunity to provide feedback and look forward to serving as a resource on this and other important financial crime and compliance topics.

Sincerely,

Andrea King
Head of Government Relations, Verafin

Submitted to: 1. *prainfo@occ.treas.gov*