



**International Bancshares
Corporation**

June 11,2021

Via email and electronic submission:

Board of Governors of the Federal Reserve System
Ann Misback, Secretary
Attn: Docket No. OP-1744
20th Street and Constitution Avenue NW
Washington, D.C. 20006
regs.comments@federalreserve.gov

Federal Deposit Insurance Corporation
James P. Sheesley, Assistant Executive Secretary
Attn: RIN 3064-ZA23
550 17th Street NW
Washington, D.C. 20429
comments@fdic.gov

Financial Crimes Enforcement Network
Attn: Policy Division, Docket No. FINCEN-2021-0004
P.O. Box 39
Vienna, VA 22183
<https://regulations.gov>

National Credit Union Administration
Melane Conyers-Ausbrooks, Secretary of the Board
Attn: Docket No. NCUA-2021-0007
1775 Duke Street
Alexandria, VA 22314-3428
<https://regulations.gov>

Office of the Comptroller of the Currency
Chief Counsel's Office
Attn: Comment Processing, Docket ID OCC-2020-0047
400 7th Street SW, Suite 3E-218
Washington, D.C. 20219
<https://regulations.gov>

Re: Comments on Request for Information and Comment Regarding Extent to Which Model Risk Management Principles Support Compliance with Bank Secrecy Act/Anti-Money Laundering and Office of Foreign Assets Control Requirements: Docket Nos. OP-1744, FINCEN-2021-0004, NCUA-2021-0007, and OCC-2020-0047; RIN 3064-ZA23.

Dear Sirs and Madams:

The following comments are submitted by International Bancshares Corporation (“IBC”), a publicly-traded, multi-bank financial holding company headquartered in Laredo, Texas. IBC maintains 186 facilities and 280 ATMs, serving 87 communities in Texas and Oklahoma through five separately chartered banks (“IBC Banks”) ranging in size from approximately \$400 million to \$10 billion, with consolidated assets totaling approximately \$14.5 billion. IBC is one of the largest independent commercial bank holding companies headquartered in Texas.

This letter responds to the joint request for information and comment (“Request”) by the Federal Reserve Board (“FRB”), the Federal Deposit Insurance Corporation (“FDIC”), the Financial Crimes Enforcement Network (“FinCEN”), the National Credit Union Administration (“NCUA”), and the Office of the Comptroller of the Currency (“OCC”, collectively, the “Agencies”) on the extent to which model risk management principles support compliance with Bank Secrecy Act/Anti-Money Laundering (“BSA”) and Office of Foreign Assets Control (“OFAC”) requirements.

The Agencies’ regulations require each bank under their supervision to establish and maintain a BSA compliance program. At a minimum, the BSA compliance program must include:

1. Internal controls to assure ongoing compliance;
2. Independent testing for compliance;
3. Designation of an individual(s), also referred to as the BSA compliance officer(s), responsible for coordinating and monitoring day-to-day compliance; and
4. Training for appropriate personnel.

Banks also have requirements related to suspicious activity reporting, customer identification, customer due diligence, and beneficial ownership. BSA systems are often used to assist banks in meeting these requirements.

Banks must also comply with OFAC's regulations. OFAC encourages banks to take a risk-based approach to designing and implementing an OFAC compliance program. In general, the sanctions programs that OFAC administers require banks to do the following:

1. Block accounts and other property of specified countries, entities, and individuals.
2. Prohibit or reject unlicensed trade and financial transactions with specified countries, entities, and individuals.
3. Report blocked property and rejected transactions to OFAC.

First issued in 2011, the Agencies have all since adopted the Supervisory Guidance on Model Risk Management (“MRMG”), which lays out the three principles for sound model risk management (“MRM”): (1) Model development, implementation, and use; (2) model validation; and (3) governance, policies, and controls. The MRMG principles provide flexibility for banks in developing, implementing, and updating models. Banks may use some or all of the principles in their risk management processes to support meeting the regulatory requirements of an effective BSA/AML compliance program. Along with the

Request, the Agencies have also published an Interagency Statement on Model Risk Management for Bank Systems Supporting Bank Secrecy Act/Anti-Money Laundering Compliance.

The Request generally asks for comments and information regarding the use of models in BSA and OFAC compliance programs and systems. The Agencies have received negative feedback regarding such use, and want to understand what is causing the issues and what, if anything, can be done.

IBC believes the key to solving the Agencies' stated BSA and OFAC model problems is for the Agencies to understand that, overwhelmingly, BSA and OFAC systems, tools, applications, and related risk management cannot be analyzed, built, or improved using traditional risk modelling frameworks. For many areas of BSA and OFAC compliance, the programs and systems are based on simple business rules that do not rise to the level of "models" and thus do not require the same scrutiny and oversight. This is due in part to the lack of clear definition of "model" in the MRMG and all subsequent guidance and rules published by the Agencies. In its Model Risk Management Program, IBC defines "model" as:

The term Model refers to a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates. A model consists of three components: an information input component, which delivers assumptions and data to the model; a processing component, which transforms inputs into estimates; and a reporting component, which translates the estimates into useful business information.

IBC believes that the problems identified by the industry to the Agencies and noted in the Request can largely be addressed and managed by the Agencies', especially their examiners', taking a narrower approach to model categorizations and instead acknowledging that certain BSA and OFAC programs and systems can be successful and compliant using non-model rules and tools.

Overall, IBC suggests the Agencies do two things: (1) issue FAQs which provide insight into the Agencies' application of the MRMG, including specific use cases and factual scenarios; (2) allow each bank to determine, in the absence of willful, gross error, whether a system is a rule or a model for purposes of the MRMG and other applicable risk model requirements. As an alternative to the latter, IBC strongly urges the Agencies to include examples that identify both models and rules, and distinguish between the two, in an FAQ.

The Request lists twelve specific requests for information and comment. IBC has provided comments to the specific issues as noted below.

Comments to Specific Requests

1. What types of systems do banks employ to support BSA/AML and OFAC compliance that they consider models (e.g., automated account/transaction monitoring, interdiction, customer risk rating/scoring)? What types of methodologies or technologies

do these systems use (e.g., judgment-based, artificial intelligence or machine learning, or statistical methodologies or technologies)?

IBC Comment: As an initial matter, IBC takes issue with the Agencies' growing tendency to use the term "model" broadly to include almost all parts of the compliance programs and systems landscape. The Request states that

The term "BSA/AML and OFAC models" is used in the questions below to describe BSA/AML or OFAC compliance systems that a bank considers models, so its interpretation could vary from bank to bank. When providing feedback, please note that the MRMG principles provide flexibility for banks in developing, implementing, and updating models. The extent and nature of model risk varies across models and banks, and a bank's risk management framework is most appropriately tailored when it is commensurate with the nature and materiality of the risk. The agencies are interested in gathering information about industry practices and welcome responses regarding individual banks, as well as common industry practices. (Request at 18981)

IBC takes issue with several assertions in that paragraph. First, the Agencies state that their use of the term "model" is subject to how a bank interprets what constitutes a model. While this should be true and is appreciated, it is not correct in practice. As discussed elsewhere herein, it has more and more frequently been up to the sole discretion of the bank's examiner to decide what constitutes a model, and thus what is subject to the additional MRMG requirements. Banks have neither the ability or opportunity to challenge or change that decision. Second, the Agencies state that the MRMG provides sufficient flexibility *for banks* to develop, implement and update models. Even if that is true, there is a huge disparity between a bank that can manage all of those activities in-house and one that must rely on vendors to provide those solutions. If a mid-sized institution cannot build its own proprietary model and instead relies on third-party solutions that it cannot change or improve independently, the MRMG's "flexibility" is useless. What banks also need is the flexibility to engage with vendors to continually improve models and systems. Finally, the Agencies concede that an appropriate risk management framework is best when it is tailored to the bank's nature and materiality of risk. As discussed herein, the Agencies can allow vendors and banks to better tailor BSA and OFAC compliance systems by providing clear guidance regarding how to implement and manage those relationships and services, as well as providing for a fulsome model standard-setting and certification framework. This would allow vendors and banks to focus on and cost-effectively implement bank-specific model tailoring.

As noted above, IBC's definition of "model" for MRMG purposes is specific and includes several clear components. IBC fundamentally disagrees with categorizing business rules as models for two reasons: (1) rules are not predictive (as models are), and (2) more flexibility is needed to adjust the rules because conditions change more quickly as compared to models. Moreover, the Agencies must

understand that BSA and OFAC compliance is unlike other areas, such as credit risk. For example, BSA and OFAC compliance is evaluated end-to-end with a focus on soundness and risk, a process for which model risk management, and the MRMG, were not tailored.

Increasingly, the Agencies' approach is that business rules become treated as models and subjected to the requirements of model validation and testing. IBC believes that in some cases, this appears to have been the result of requirements imposed by examiners ad hoc. This approach makes bankers feel unable to contradict the examiner's decision and, as a result, they are frequently compelled to treat processes and business rules that are not models as if they were models. For example, is a transaction monitoring system a model if it is based on the application of clear, bright line rules? The issue of identifying the distinction between rules and models is an especially important issue in OFAC compliance, where most of the focus is on filtering using a rules-based approach, not models.

IBC believes that guidance from the Agencies distinguishing between a model and a rule would be the most helpful to their stated goals and compliance with BSA and OFAC obligations. IBC is aware of at least one bank that has over 700 rules, or potential "models," for OFAC searches and compliance, and treating those rules as models would almost certainly crash that system. As the Agencies are well aware, it is not necessary to review every rule on a regular basis, and it is not necessary to subject rules to the same level of scrutiny and testing as models. For many facets of BSA and OFAC compliance, the requirements and triggers are clear and unambiguous and do not require underlying algorithms, machine learning, or risk assessment to build and implement. The rules implemented to meet these obligations do not require the same detailed review and maintenance required of true risk models.

2. To what extent are banks' BSA/AML and OFAC models subject to separate internal oversight for MRM in addition to the normal BSA/AML or OFAC compliance requirements? What additional procedures do banks have for BSA and OFAC models beyond BSA/AML or OFAC compliance requirements?

IBC Comment: Again, IBC takes issue with the Agencies' use of the term "models" as a blanket catchall for various methods, policies, and rules used by banks for BSA and OFAC compliance. Due to the Agencies' increased designation of rules as models, IBC has been forced to treat many of its BSA and OFAC compliance rules as full models, for purposes of MRMG and other regulatory requirements. IBC also conducts additional MRM oversight of its BSA and OFAC models. Internal oversight for MRM that is beyond BSA or OFAC compliance requirements includes (1) having robust and comprehensive model documentation to provide modeling purpose and oversight responsibilities, general modeling approach, data description, and detailed operating procedures, (2) maintaining controls over data integrity and completeness to ensure proper implementation, effective systems

integration and appropriate use, (3) effectively challenging model limitations and key assumptions, and (4) validating significant or material changes to the model.

3. To what extent do banks have policies and procedures, either specific to BSA/AML and OFAC models or applicable to models generally, governing the validation of BSA/AML and OFAC models, including, but not limited to, the validation frequency, minimum standards, and areas of coverage (i.e., which scenarios, thresholds, or components of the model to cover)?

IBC Comment: As discussed below, IBC and its model vendors are greatly hampered in validating and implementing bank-specific scenarios, thresholds, and components of its BSA and OFAC models because of the general need to validate the “off-the-rack” retail model in whole prior to requesting and validating any bank-specific tailoring.

Furthermore, to the extent “models” are used as part of BSA and OFAC compliance, IBC notes the same internal oversight, validation, and procedures it did in its response to FDIC’s Request for Information on Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and Other Services in September of 2020 (“FDIC Model Comment Letter”). As a mid-sized institution, IBC relies heavily on third-party vendors for compliance solutions. IBC must go through a robust review, validation, certification, and implementation process for each vendor and model it uses. The volume of due diligence data and paperwork necessary to negotiate with and on-board a vendor or to implement any model, including a BSA or OFAC compliance model, is staggering.

A large amount of time and effort spent on model and vendor on-boarding is simply duplicative of work and time spent by either the vendor or its previous or current customers. One vendor could be engaged with a number of insured institutions, which are all subject to the same due diligence, annual reporting, and monitoring requirements.

However, that burden could easily be reduced with appropriate standard-setting voluntary certifications. To the extent those requirements can be met by the vendor voluntarily being reviewed and certified by a standard-setting organization (“SSO”) or certification organization (“CO”), the regulatory and reporting burden on insured institutions could decrease precipitously. Already, certain standard-setting voluntary certifications are used to more efficiently conduct due diligence and on-board vendors and models, such as SOC 2 Type II certification. Additionally, models and vendors would face a decreased logistical burden of providing access to systems testing and other due diligence requirements to all of its bank clients. Instead, such vendors may simply go through any required testing or review one time and provide evidence of its successful completion to each of those customers.

Moreover, IBC Banks are required to conduct an annual security attestation for many of their model vendors. This burden is a hurdle to engaging new model

vendors, as each new vendor represents an additional certification that is necessary. If, instead, model vendors were able to be independently reviewed and certified, and insured institutions could rely on such certification, it may be possible to decrease the burden of on-boarding and working with multiple new vendors. This would also result in the Agencies being able to institute industry-wide standards which would add stability and certainty to BSA and OFAC compliance. If the Agencies are going to continue treating business rules and processes as models, IBC strongly urges the Agencies to consider implementing more options for standard-setting review and certification of BSA and OFAC compliance models.

4. To what extent are the risk management principles discussed in the MRMG appropriate for BSA/AML and OFAC models? Please explain why certain principles may be more or less appropriate for bank operations of varying size and complexity? Are there other principles not discussed in the MRMG that would be appropriate for banks to consider?

IBC Comment: It is IBC's understanding that many banks and examiners have been asking the Agencies for additional help and guidance when applying the MRMG to the BSA and OFAC space. IBC believes the Agencies should make clear the exact definition of "model" so that all stakeholders can understand when the MRMG and other model requirements apply. As noted herein, examiners are more and more frequently treating business rules and pseudo-models as full risk models and subject to the MRMG. As a result, banks have to look to and consider MRMG guidance and requirements when developing, implementing, maintaining, and implementing BSA and OFAC compliance solutions.

5. Some bankers have reported that banks' application of MRM to BSA/AML and OFAC models has resulted in substantial delays in implementing, updating, and improving systems. Please describe any factors that might create such delays, including specific examples.

IBC Comment: While no less useful or thoughtful, implementing a business rule instead of a full model for BSA and OFAC compliance is a much quicker and efficient process. Again, many aspects of BSA and OFAC compliance can be satisfied using simple, clear business rules that do not rise to the level of "models." IBC believes the primary issue causing the increase in reported delays is the ever-increasing inclusion of rules into the Agencies', and examiners', interpretation of "model." It is not the case that applying MRM to *actual, traditional* BSA or OFAC models results in *more* delays than MRM application to any other model types, rather the over-application of MRM to simple business rules has greatly increased the time required and burden of implementing, updating, and improving BSA and OFAC compliance systems.

6. Some bankers have reported that banks' application of MRM to BSA/AML and OFAC models has been an impediment to developing and implementing more innovative and effective approaches to BSA/AML and OFAC compliance. Do banks consider MRM

relative to BSA/AML an impediment to innovation? If yes, please describe the factors that create the impediments, including specific examples.

IBC Comment: As otherwise noted herein, the limited use of SSOs and COs and the over-application of MRM to BSA and OFAC compliance systems that do not rise to the level of “model” has hamstrung banks and third-party vendors from more quickly and effectively developing and implementing more innovative solutions for BSA and OFAC compliance. Broader use of SSOs and COs would lead to easier onboarding, more robust specification and tailoring, and more competition in the third-party model market. Clearer guidance regarding the definition and elements of a “model” would also allow quicker and more effective development and implementation of innovative BSA and OFAC compliance rules and non-model alternatives, while also maintaining the protections around *true* models.

7. To what extent do banks' MRM frameworks include testing and validation processes that are more extensive than reviews conducted to meet the independent testing requirement of the BSA? Please explain.

IBC Comment: IBC conducts the following testing and validation of models in addition to the independent testing required by the BSA.

- a. **Internal review:** AML systems team regularly conducts system testing to review and analyze the alerts generated from the AML application, and ensures that the alerts are generated after meeting the required parameters and no activity has been missed. This includes ad-hoc testing and validation.
- b. **External review:** Third party vendors are engaged to complete a tuning and optimization of the AML system covering the transaction monitoring scenarios and Risk Based Due Diligence rules and associated parameters. Additionally, the third party vendor also completes the BSA workflow analysis and country risk

8. To what extent do banks use an outside party to perform validations of BSA/AML and OFAC compliance systems? Does the validation only include BSA/AML and OFAC models, as opposed to other types of models used by the banks? Why are outside parties used to perform validation?

IBC Comment: As more fully discussed in the FDIC Model Comment Letter, IBC and many institutions rely on third-party model validation for the full spectrum of models because building, maintaining, and validating proprietary models can be cost prohibitive for anyone other than the largest banks. The reliance on third parties to perform the validation is driven by the high level of technical expertise necessary to review the complexity of many models.

By and large, small and mid-sized banks are subject to generic systems and models which are designed as a one-size-fits-all solution to BSA and OFAC compliance. The vendor has multiple customers, which all need to independently

validate and certify the models, so its process is not tailored to each customer separately. But for a third-party model, a bank in an urban west coast market is in a different situation than one in the rural Midwest. A third-party model is generally not fitted to such differences.

While there may be some ability to “customize” the programs and models, any significant changes are difficult and, where they can be achieved, take a significant amount of time and cost a great deal. As a result, the banks that rely on outside vendors also have to rely on the vendor’s typologies for BSA and OFAC compliance. Still, at the same time, the banks are required by examiners to conduct model validation, raising the question about why it couldn’t be conducted at the vendor level. As raised by the FDIC in its September 2020 Request, broader allowance of SSOs and COs could help modernize and improve use of third-party models for BSA and OFAC compliance. By doing this, the Agencies can also ensure a consistent, clear, and stable model validation regime.

In order to allow for more robust tailoring to specific bank needs, model certifications should aim to fully test and validate the model across a broad spectrum of setups, calibrations, and/or assumption settings. This would reduce the scope of the bank-specific (“own use”) validation and, in turn, the cost of using third-party models. As noted, most third-party models are not easily altered and function as one-size fits all. If the general model was universally certified and bank-specific tailoring was cheaper, that would likely result in increased own-use validations. Model certifications reports should also clearly state the extent in which a bank can rely on the certification within the validation. For example, if the focus of validation is to ensure proper setup, calibration, and/or assumption setting of a third-party model, then the certification should clearly state the remaining items that need to be validated by the bank. This has the potential of reducing scope creep within an “own use” validation and, in turn, the cost of using third-party models.

9. To what extent do banks employ internally developed BSA/AML or OFAC compliance systems, third-party systems, or both? What challenges arise with such systems considering the principles discussed in the MRMG? Are there challenges that are unique to any one of these systems?

IBC Comment: As a mid-sized institution, IBC relies heavily on third-party vendors and systems to meet its BSA and OFAC obligations, including model vendors. The MRMG is clear that “banks are expected to validate their own use of vendor products,” which is the largest cost driver in the adoption of third-party models. IBC and IBC Banks’ model validation increases the annual cost of the third-party models by as much as 50% to 100%. IBC believes that the MRMG needs to be substantially revised to fully address the use of third-party model certifications, including a more robust certification and standard-setting framework.

10. To what extent do banks' MRM frameworks apply to all models, including BSA/AML and OFAC models? Why or why not?

IBC Comment: Any model that has been included in IBC's model inventory listing is subject to the MRM framework, where the application is commensurate with the model's risk, business activities, as well as the extent and complexity of using the model in the bank's decision-making process.

11. Specific to suspicious activity monitoring systems, the agencies are gathering information about industry practices. The agencies welcome responses to the following, regarding individual bank and common industry practices.

IBC Comment: IBC is generally supportive of using models to allow banks to eliminate or reduce low value BSA or OFAC alerts. While this may result in fewer SARs or CTRs, it should also result in SARs and CTRs of higher quality and law enforcement effectiveness. However, as discussed below, use of models will only be effective if the Agencies give banks insight into how law enforcement uses SAR information and how effective that SAR information is.

a. Suspicious activity monitoring system validation:

i. To what extent do banks validate such systems before implementation?

IBC Comment: Models, and changes to models, are validated based on the model/change's classification (e.g. moderate/high, material/significant, etc.) according to IBC's policies and procedures. A thorough analysis is conducted to validate that models are optimized according to BSA standards. IBC categorizes models and changes to models into risk ratings, and its Model Risk Management Program explains these ratings and the related validation requirements. Material and Significant changes require comprehensive validation based on the model type and risk rating. Models risk rated Moderate and above also generally require comprehensive validation prior to implementation.

ii. Are banks able to implement changes without fully validating such systems? If so, please describe the circumstances.

IBC Comment: Generally no, any change in the system needs to go through comprehensive testing and validation. IBC has three classifications for model changes: Material, Significant, and Insignificant. All three categories require comprehensive validation prior to and after implementation. However, for certain low risk rated models and insignificant changes, full validation is not required prior to implementation. As further noted below, IBC conducts frequent

ongoing testing of those models and changes until the next required full validation of the model.

iii. How frequently do banks validate after implementation?

IBC Comment: The primary validation occurring after implementation is in the context of changes to the model. While nearly all changes are validated prior to implementation, there is no post-implementation validation unless the change is causing errors or complications to IBC's BSA application. If issues arise, then the team works with the IT department and the vendor to fix the errors.

iv. To what extent do banks validate after implementing changes to existing systems (e.g., new scenarios, threshold changes, or adding/changing customer peers or segments)? Please describe the circumstances in which you think this would be appropriate.

IBC Comment: As noted above, IBC validates changes to models after implementation if there are issues with existing scenarios. The AML Systems team develops reports and spreadsheets to monitor threshold changes and new scenarios. The spreadsheets are developed to account for the parameters by different scenarios and the testing is conducted by inputting the alert data in the respective fields to validate appropriate alert generation and changes are incorporated accurately.

v. How do banks validate such systems?

IBC Comment: IBC's Internal Audit Services Department's Model Validation Group is responsible for model validation. If applicable, IBC also relies on the applicable vendor for validation. The level of validation activities is based on the appropriate range and rigor for the specific model being validated. Models are risk rated, and are created, implemented, changed, and validated based on that categorization, along with the categorization of the change (e.g. material/significant/insignificant).

vi. What, if any, compensating controls do banks use if they have not had an opportunity to validate such systems?

IBC Comment: If IBC validation is not necessary prior to implementation based on IBC's policies and procedures, then IBC will conduct periodic, frequent testing as described throughout this Letter until full validation is necessary and completed. IBC reiterates that material or significant changes, and most changes to models risk

rated moderate or higher, are not implemented without prior validation.

- b. Suspicious activity monitoring system benchmarking: What, if any, external or internal data or models do banks use to compare their suspicious activity systems' inputs and outputs for purposes of benchmarking?

IBC Comment: IBC believes the Agencies should provide any additional information they can to assist banks in benchmarking SAR systems. IBC has always strongly urged the Agencies to provide banks more insight into SAR data, how it is used, and to what effect. Any of this additional information would be greatly helpful in testing, building, and improving SAR systems.

- c. Suspicious activity monitoring system back-testing: How do banks attempt to compare outcomes from suspicious activity systems with actual outcomes, given that law enforcement outcomes are often unknown?

IBC Comment: As noted above, IBC has always and continues to advocate for increased SAR data sharing between law enforcement and banks. The Agencies consistently ask banks' opinion on what SAR information is useful and effective, without providing any insight into law enforcement's use of such data. If banks had a better understanding of how SAR data is used and what information is most effective, they could build and better tailor BSA and OFAC compliance systems to best assist law enforcement.

- d. Suspicious activity monitoring system sensitivity analysis: How do banks check the impact of changes to inputs, assumptions, or other factors in their systems to ensure they fall within an expected range?

IBC Comment: Any changes are first implemented in our test and/or development regions. Elaborate testing is conducted to review the test results to ensure that the changes provide the intended results. The results are also compared with the Production region to analyze the impact of the change.

- 12. To what extent do banks calibrate the scope and frequency of MRM testing and validation for BSA/AML and OFAC models based on their materiality? How do they do so?

IBC Comment: The tuning of scenarios has been conducted every eighteen (18) months since implementation. The scenarios have been tuned as a result of the testing. Ad-hoc testing and validation is an ongoing process, and during the course of testing the transaction based Risk Based Due Diligence rules were calibrated.

Given the sheer range of possible model changes, IBC reviews and classifies the changes to models based on the cause, objective and impact to operations and business decisions. Material and significant changes may be subject to validation activities within the appropriate scope and rigor prior to implementation, which will depend on the extent the model is used for decision making, the model's risk profile, as well as the propriety of the model. The frequency of validations are assigned to models based on overall risk rating and resultant consequence of risk occurrence.

Thank you for the opportunity to share IBCs views on these matters.

INTERNATIONAL BANCSHARES CORPORATION



Dalia F. Martinez
Executive Vice President and Corporate Bank Secrecy Act Officer