BUTLER | SNOW

Quarterly Report

Mississippi Regulatory Compliance Group

February 2022 *Vol. 33 No. 1*

SUSAN WALDROP – RETIRING ☹

Well, I knew one day this would come, and I

am very excited for Susan, but am a little sad for us. For those of you that have had Susan perform your BSA Independent review, you know that she is an EXPERT on BSA! If she has a question about an issue, she will delve into the manuals and website to make sure she is giving banks the correct answer. If you remember several years ago, Dolgencorp had gone from a listed company to a nonlisted company. She researched that issue at that time and saved a lot of banks from having an exception (and frankly, "taught" the examiners something that they had not known! ☺).

Susan has been with Butler Snow since August 7, 2006. When Butler Snow said I could hire someone to help, Susan was the first person I thought of. Susan and I had worked at Deposit Guaranty together and were actually the only two people in the compliance area for a while. It is important to be able to know that you can count on someone and call on them for anything, and I knew Susan was that person. Susan has not only been a coworker for all of these years, but a very special friend to me. I have told her, though, that we reserve the right to call her and ask her any BSA question after she retires!

We will miss Susan but wish her much happiness in retirement as she enjoys her favorites- family, fishing and football --- during her free time to come.

<Patsy Parkin>

DOJ REDLINING INITIATIVE

In October, the U.S. Department of Justice announced the launch of a new Combatting Redlining Initiative. We are all familiar with the term "redlining" which is illegal discrimination which occurs when lenders avoid lending to individuals living in communities of color because of the race or national origin of the people who live in those areas. This Initiative will be led by the Civil Rights Division's Housing and Civil Enforcement Section in partnership with U.S. Attorney's Offices across the country focusing on making mortgage credit and homeownership accessible to all persons on the same terms, regardless of race, national origin or the neighborhood where they live. The announcement said the Initiative will:

- utilize U.S. Attorneys' Offices as force multipliers and take advantage of local expertise on housing markets and the credit needs of local communities of color;

- Expand the department's analyses of potential redlining to both depository and non-depository institutions (non-depository lenders now make the majority of mortgages in the U.S.);
- Strengthen partnerships with the financial regulatory agencies to ensure identification and referrals of fair lending violations to the Department of Justice; and
- Increase coordination with State Attorneys General on potential fair lending violations.

The press release noted that the gap in homeownership rates between white and Black families is larger today that it was in 1960 before passage of the Fair Housing Act.

The initiative was announced at the same time as the announcement of a settlement agreement among the DOJ, the CFPB, the OCC and Trustmark National Bank to resolve allegations that the bank engaged in redlining Black and Hispanic neighborhoods in Memphis, TN in the 2014-2018 time period. The announcement said the bank agreed to:

- invest $3.85 million in a loan subsidy fund for current and future residents of predominantly Black and Hispanic neighborhoods in the Memphis area,
- dedicate at least four mortgage loan officers or community lending specialists to these neighborhoods,
- open a loan production office in a majority-Black and Hispanic neighborhood in Memphis,
- devote $400,000 to developing community partnerships to provide services to residents of majority-Black and Hispanic neighborhoods in Memphis to increase access to residential mortgage credit,
- devote at least $200,000 per year to advertising, outreach, consumer financial education and credit repair initiatives in and around Memphis, and
- pay a civil money penalty of $5 million to the OCC and CFPB.

The announcement noted that the bank had already established a Fair Lending Oversight Committee and designated a Community Lending Manager to oversee these efforts, and AG Merrick Garland commended Trustmark for its cooperation in swiftly resolving the matter.

This announcement follows on the heels of a redlining settlement last August between the DOJ, the OCC and Cadence Bank N.A. involving allegations the bank engaged in redlining predominately Black and Hispanic neighborhoods in the Houston, TX area. In that settlement, the bank agreed to:

- invest a minimum of $4.17 million in a loan subsidy program to increase residential loans in majority-Black and Hispanic census tracts in the Houston area,
- devote at least $750 thousand in community partnerships to provide to residents of majority-Black and Hispanic census tracts in Houston services related to credit, financial education, homeownership, and foreclosure prevention,
- designate a full-time Director of Community Lending and Development,
- open at least one new full-service branch located in a majority-Black and Hispanic census tract in the Houston area within 12 months,

- assign at least four mortgage loan officers to actively solicit applications from majority Black and Hispanic census tracts in Houston,
- spend at least $125 thousand per year on advertising, outreach, consumer financial education and credit repair counseling in the Houston area, and
- pay a $3 million civil money penalty to the OCC.

In 2016, the DOJ and the CFPB entered into a settlement agreement with BancorpSouth Bank to resolve allegations of redlining majority-minority neighborhoods in the Memphis, TN MSA along with other allegations of discrimination relating to underwriting and pricing of loans to Black applicants. Among other terms, the bank agreed to:

- open at least one new branch or mortgage loan production office in a high-minority (minority population of at least 80%) census tract in addition to the branch the bank had recently opened in a majority minority tract,
- invest $4 million in a loan subsidy program,
- spend a minimum of $100 thousand per year in targeted advertising and outreach to majority-minority neighborhoods,
- partner with community organizations to provide credit, financial education, homeownership counseling, credit repair, and/or foreclosure-prevention services to residents of majority-minority neighborhoods, and
- pay a $3 million civil money penalty to the CFPB.

Similar redlining settlements announced by DOJ in the past include Eagle Bank and Trust of Missouri (2015), Hudson City Savings Bank, N.J. (2015), Union Savings Bank, Ohio (2017), KleinBank, Minn. (2018), and First Merchants Bank, S.D. (2019).

If you are seeing a pattern here, it's because there is one. In addition to the usual fair lending concerns regarding loan underwriting and pricing, the federal banking agencies are devoting substantial resources to identifying suspected redlining and making referrals to the Department of Justice. And, it is not just large banks they are concerned about.

The focus of these enforcement actions has not just been on loan distributions in minority neighborhoods, but also on branch locations and mortgage loan officers that are concentrated in majority white neighborhoods, lack of marketing and outreach efforts targeted specifically to reach minority neighborhoods, and more recently, lack of diversity among loan officers. It is relatively easy for regulators to identify institutions with loan application and origination percentages in any given geographic area that is below their peers. The initial analysis is based simply on the numbers and geographies - differences in percentages between one type neighborhood (e.g., majority white) and another (e.g., majority Black and Hispanic). In an examination, then, the burden will fall to the institution to justify those differences and explain its efforts to reach all neighborhoods.

There are steps an institution can take to help minimize redlining risk. Monitoring is one. Analyzing and understanding how you compare with peers in your assessment/market areas is important. The regulators use HMDA data and a peer group of lenders (bank and non-bank) that have 50% to 200% of the application or origination volume of the institution being examined. This often requires expert assistance to analyze the HMDA data and perform a statistical analysis. There isn't really a way to

compare yourself with peers on anything other than HMDA reportable loans. And it's difficult for non-HMDA reporters to do more than just look at the distributions of their own applications and originations.
Serving minority neighborhoods and low to moderate income areas should be a part of an institutions analysis in determining whether to open or close a new branch or loan production office. Consider where the efforts are currently lacking and where the peer lenders are located. Look at your institution's assessment areas and make sure they do not improperly exclude majority minority tracts. Does the institution market and provide credit regularly outside of its assessment area? Those areas may be considered as REMAs for fair lending and redlining purposes.

Available products should be reviewed to be sure they are available in all areas on at least equal terms and conditions, and new products may need to be considered to improve lending performance in some areas. More institutions are considering special purpose credit programs based on a recent advisory opinion from the CFPB. Loan policies need to be considered as well. For example, do loan policies define "undesirable loans" in a fashion that could be read as discouraging loans in minority neighborhoods.

Diversity in hiring is important. A well-trained and diverse lending staff can make a big difference in lending performance. Consider marketing and outreach efforts. Use diverse models in advertising and on the institution's website, social media and other advertising outlets. Document outreach efforts with community groups, businesses, realtors and others that provide services in minority neighborhoods, even the unsuccessful efforts. Consider partnerships with governmental organizations and community groups that provide housing and credit-related services in those neighborhoods.

A credit needs assessment for LMI and majority-minority tracts in your institution's assessment area could be a great place to start. What are the needs and lending opportunities? What is your competition doing, and where are they located?

At the quarterly meeting, we will have a discussion of redlining, how the regulators are looking at it and more discussion about ways in which to reduce redlining risk.

<Cliff Harrison>

CFPB FAQS ON ELECTRONIC FUNDS TRANSFERS AND REG. E

The CFPB recently revised its FAQs related to the Electronic Funds Transfer Act and Regulation E. As you know, Reg. E establishes limits on consumer liability for unauthorized EFTs and addresses duties to investigate error claims. The original list of FAQs was released in mid-2021 and generally covered violations and requirements of Reg. E. Because we did not cover that original Q&A when it was released, this article will cover both the original and the updated guidance. The updated guidance expanded its scope to cover person-to-person ("P2P") and mobile payment transactions. Since the list of FAQs is designated by the CFPB as a "compliance aid", it is not considered a binding rule on financial institutions. However, the FAQs clarify existing electronic fund transfer rules and provide insight into the CFPB's interpretation of the regulations.

The FAQs consist of 24 sets of questions and answers and are organized into 4 categories: (i) coverage: transactions, (ii) coverage: financial institutions, (iii) error resolution, and

(iv) error resolution: unauthorized EFTs. We discuss each of the categories and questions & answers in more detail below.

Coverage: Transactions

The first five questions and answers address the very basics of Reg. E and the EFT Act and includes definitions and explanations of which transactions are covered under the law. Reg. E and the EFT Act apply to electronic fund transfers that authorize a financial institution to debit or credit a consumer's account. An "account" is broadly defined to include a checking, savings, or other consumer asset account, including a prepaid account. An "electronic fund transfer" means any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account. So, Reg. E covers P2P payments and mobile payment transactions, which includes debit cards, ACH, prepaid accounts, and other electronic transfers to or from a consumer account.

P2P payments allow consumers to send funds to another person without needing to write a check, swipe a physical card, or exchange cash. Depending on the payment provider, a P2P payment can be initiated from a consumer's online bank account portal, prepaid account portal, or mobile application. Covered P2P payments can also include debt card transfers and credit-push payments. Reg. E also covers debt card "pass through" payments.

Coverage: Financial Institutions

This section contains four Q&As and clarifies which financial institutions are covered under Reg. E. Unsurprisingly, the regulation defines "financial institution" broadly to include banks, savings associations, and credit unions, and the definition expands the definition to include "any other person that directly or indirectly holds an account belonging to a consumer, or any other person that issues an access device and agrees with a consumer to provide EFT services."

If a P2P provider or bill payment services directly or indirectly hold an account belonging to a consumer, or if it issues an access device and agrees with a consumer to provide EFT services, it is a financial institution for the purposes of Reg. E. This includes non-bank P2P payment providers.

Understanding what is a financial institution under Reg. E is important because under the regulation, financial institutions generally have error resolution obligations in the event that a consumer notifies the financial institution of an error. For example, a prepaid account whose primary function is to conduct P2P transfers is a non-bank P2P payment provider.

In limited circumstances, a financial institution can be considered a "service provider" under Reg. E. A financial institution who provides EFT services to a consumer but does not hold the consumer's account is a service provider under Reg. E if the financial institution: (i) issues an access device that the consumer can use to access the account and (ii) no agreement exists between the access device-issuing financial institution and the financial institution holding the account.

The ACH rules alone do not generally constitute an agreement for purposes of whether a financial institution meets the definition of "service provider" under Regulation E. However, an ACH agreement combined with another agreement to process payment transfers, such as an ACH agreement under which members specifically agree to honor each other's debit cards, is an

"agreement," and thus the additional requirements for services providers covered under 12 CFR 1005.14 do not apply.

If a debit card pass-through payment was initiated through a non-bank P2P payment provider from a consumer's account held by a depository institution such as a bank or credit union, the depository institution is still considered a financial institution under Reg. E. Accordingly, the depository institution has full error resolution obligations under the regulation.

Error Resolution

This section contains four additional Q&As to clarify error resolution requirements for covered entities under the regulations.

Reg. E broadly defines the term "error" to include an unauthorized EFT, an incorrect EFT to or from the consumer's account, the omission from a periodic statement of an EFT to or from the consumer's account that should have been included, a computational or bookkeeping error made by the financial institution relating to an EFT, the consumer's receipt of an incorrect amount of money from an electronic terminal, an EFT not identified in accordance with the requirements of 12 CFR 1005.9 covering ATM transfers or 12 CFR 1005.10(a) covering preauthorized transfers, a consumer's request for any documentation required by 12 CFR 1005.9 or 1005.10(a) or for additional information or clarification concerning an EFT.

The term "error" does not include a routine inquiry about the consumer's account balance, a request for information for tax or other recordkeeping purposes, or a request for duplicate copies of documentation.

Upon receipt of an oral or written notice of error, Reg. E requires a financial institution to promptly investigate an allegation of error, complete its investigation within the time limits specified in the regulation, report the results within 3 business days after completion of the investigation, and correct the error within 1 business day after determining that an error has occurred.

If a financial institution's private network rules provide less consumer protection than federal law, the private network rules do not change its Reg. E obligations. Finally, financial institutions may not require consumers to file police reports as a condition to initiate an error resolution investigation. The institution must promptly begin its investigation upon receipt of oral or written notice of error.

Error Resolution: Unauthorized EFTs

The final section contains 11 of the Q&As and covers how financial institutions must resolve unauthorized EFTs.

An unauthorized EFT is an EFT from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit. This includes transfers initiated by a person who obtained a consumer's access device through fraud or robbery and ATM transfers induced by force. An unauthorized EFT does not include an EFT initiated (i) by a person who was furnished the access device by the consumer (unless the person notified the financial institution that the person's access was revoked), (ii) with fraudulent intent by the consumer, or (iii) by the financial institution.

If, after its investigation, the financial institution determines that the error was an unauthorized EFT, the liability protections of Reg. E apply. This means that a customer may have some liability.

An EFT initiated from a consumer's account by a fraudster through a non-bank P2P payment provider is an unauthorized EFT. This is true even if the consumer does not have a relationship with or does not recognize the provider. Similarly, an EFT initiated by a fraudster using stolen credentials is an unauthorized EFT. Also, inducing a consumer into sharing account information is an unauthorized EFT, and this includes not just the initial transfer, but all subsequent transfers. If a consumer is fraudulently induced by a fraudster to share account access information that is used to initiate a transfer, that transfer and subsequent transfers are considered unauthorized EFTs.

If an EFT is initiated by a fraudster through a non-bank P2P payment provider that the consumer does not have a relationship with, from the consumer's account with a depository institution, the depository institution is still considered a financial institution with full error resolution obligations under Reg. E.

A financial institution may not consider consumer negligence when determining liability for unauthorized EFTs, and a financial institution may not require a customer to first contact the merchant about the potential unauthorized EFT before it initiates its investigation. Private network rules do not impact the Reg. E definition of unauthorized EFT, and a financial institution may not modify or waive Reg. E protections through the contract between the 2 parties.

We encourage you to read the proposed FAQs, which are available on the federal regulators' websites. Comments on the proposed FAQs are due May 17, 2021, which is 60 days after publication in the Federal Register. The FAQs are available on the CFPB's website. We believe that the list serves as a useful tool for bank compliance and encourage you all to read them.

<Doug Weissinger>

RESPONSES TO FLOOD INSURANCE QUESTIONS BY THE FDIC FROM THE NOVEMBER QUARTERLY MEETING

Napoleon Yancey, FDIC, did presentation on flood insurance at our November meeting. There were several questions from our member banks during the meeting which Napoleon has since provided responses to. Those questions posed and the responses follow.

Q. Where do you get insurable value?

A. This is generally the replacement cost value, found on the hazard insurance policy or appraisal (which would be replacement cost value). If a hazard insurance policy is used, take into consideration that flood insurance insurable value may differ from the hazard insurance coverage because hazard policies do not cover foundations, and the value must be adjusted. The hazard policy should specifically state "replacement cost value."

Q. Slide 10 was a cross-collateralization example. A lender makes numerous business purpose loans to an individual who frequently purchases residential rental houses in several nearby SEC college towns. Currently, the borrower's "credit relationship" at the bank consists of 1 auto loan and 4 rental houses. None of the residences are located in a SFHA. The borrower returns for a new loan that will be secured by a rental house, but this time, the residence is located in a SFHA.

All of the borrower's deeds of trust include cross-collateralization language and the subject transaction included Maximum Obligation Limit language of $170,000. Additional information regarding this transaction follows:

* $425,000 – Total existing outstanding loan balance owed by borrower
* $170,000 - Amount of new loan secured by SFHA rental house
* $205,000 – insurable value of SFHA rental house
* $250,000 Maximum insurance available from NFIP from this structure

Question from meeting: Why does the outstanding $425,000 for properties NOT located in a Standard Flood Hazard Area have to be included with the $170,000 loan?

A. Because the new loan is in a flood hazard area and has cross-collateralization language, any other loan the borrower has is subject to flood insurance requirements because of the cross-collateralization with the loan that IS in a flood hazard area. You would be required to have $250,000 in flood insurance: $170,000 loan secured by the rental house in the flood zone, plus $80,000 for the total existing loan balance.

Q. What is the FDIC's stand when there is a difference in the flood zone from the insurance company and the flood zone from the bank's third party that looks up the flood zone and completed the SFHDF?

A. The FDIC has stated that the bank does not have to correct the flood policy to match the flood search. The flood zone no longer affects premiums.

Q. Can the flood policy be paid for at closing – either the customer is financing the policy, paying for it from the cash out, or bringing a check to closing?

A. The customer can finance the policy and the bank (not the customer) can disburse the funds for the policy directly to the insurance company.

Q. Contents Language in Security Instruments (Slide 7). We have looked at a number of deeds of trust and security agreements and the language varies. Most of what we see references personal property, which is limited to personal property attached to real property. We have advised since it is limited to property attached, such as appliances, that this is not subject to contents insurance. Does the FDIC agree with this?

A. This may vary by state. We recommend being as specific as possible in the collateral agreement. If inventory is listed on the collateral, be specific as to what is included as collateral for the loan.

Q. Cross Collateral and Contents Language (slide 9). What about the amount of coverage when insurance is force placed? The loan is for the balance of the loan at the time of force placement, and then if the force placed premium is added to the balance, the bank would have to include that amount. There are times when the force placed amounts is not known at closing. How would you recommend handling this scenario?

A. If you do not know the exact amount, go a little higher to ensure that you have an amount that IS sufficient. You can

refund the overage once the actual amount is known.

We have talked with the FDIC on possible ways to eliminate the cross-collateralization on current loans on your books. Some of you have sent letters to customers that have cross-collateralization clauses and loans secured by real property in a flood hazard area. The FDIC examiner's opinion (and this is being sent by the local FDIC examiners to Washington) is that if a bank wants to waive or discontinue the cross-collateralization clause, some form of recorded document would need to be prepared. It does not have to be signed by the borrower; only by the bank. We do recommend that if your bank is going to take this or similar measures, you get legal advice on the documents and language to use. As we learn more, we will certainly pass any additional information on to the groups.

Also, if you have talked to some of your compliance counterparts you know that some FDIC examiners have now said that TRID and HMDA violations may occur as a result of cross-collateralized loans. Before you change anything in your process, know that this question has been sent up to FDIC in Washington, and we are all waiting on their response.

Lending has certainly changed over the years! We will keep you posted on any updates we receive from the FDIC. In the meantime, if you have any questions or want to us to review your bank's disclosures for cross-collateralization, please call or email us.

<Patsy Parkin>

FFIEC EXAMINATION PROCEDURE UPDATES

On December 1, 2021, the FFIEC updated its BSA/AML examination procedures to include an Introduction related to Customers as well as updated information for the following specific account types: Politically Exposed Persons (PEPs), Independent Automated Teller Machine Owners and Operators, and Charities and Nonprofit Organizations.

In the new introductory section of the manual, the FFIEC communicated to examiners that no specific customer type will automatically present a higher risk for illicit financial activity. Further, banks are not prohibited from doing business with a certain type of customer simply because of the customer type. Rather, banks should develop policies and procedures to evaluate the facts and circumstances of the specific customer and manage and mitigate the risks accordingly.

The following sections were revised to provide more specific information for risk mitigation and risk factors for PEPs, Independent Automated Teller Machine Owners and Operators, and Charities and Nonprofit Organizations. These revisions are not added because of an increase in scrutiny of these product types or as new instructions, but, rather, to include instructions on how to evaluate the bank's policies, procedures and processes related to these customer types.

The update also added two new subsections for each of these three account types as follows: Examiner Evaluation and Examination and Testing Procedures. The Examiner Evaluation section guides examiners on how to determine whether a bank's policies and procedures are adequate for mitigating risks associated with illicit financial activity by reviewing the bank's CIP, CDD and suspicious activity reporting.

The Examiner Evaluation and Examination and Testing Procedures are intended to be used to determine a bank's compliance with CIP, CDD, beneficial ownership, CTR and SAR requirements through review of written policies, procedures as well as other processes through seven steps.

Examiners should determine: (1) whether the bank has appropriate written, risk-based procedures for conducting CDD; (2) whether the bank's CDD policies and procedures are adequate to develop effective customer risk profiles to identify specific risks; (3) whether the bank has policies, procedures and processes to identify customers who may pose a higher risk for illicit financial activity and whether those policies, procedures and processes are in line with the bank's risk profile; (4) whether the bank's monitoring system is adequate; (5) whether the bank's policies, procedures and processes related to CTRs are adequate; and (6) whether risk-based testing is appropriate, and, if so, select a sample for each product type to determine that the bank collects the appropriate information to understand each customer, incorporates the appropriate information in the risk profile and conduct transaction testing. Finally, examiners should form a conclusion about the bank's policies, procedures and processes related to each specific customer type.

We have recently updated the MRCG/MSRCG manual to reflect these changes and have added additional account types to the high-risk account sections. You will be notified when these updates are available.

<Memrie Fortenberry>

TAKE NOTE!

A few changes for 2022 that you need to note – and one may even make some of you really smile! ☺

As most of you probably know, the FDIC has closed its Memphis office and has moved its Dallas Regional Office. This was effective November 15, 2021. Because of the new Dallas address, **FDIC banks** will need to update their CRA Notice to include the new address immediately:

600 North Pearl Street, Suite 700
Dallas, Texas 75201

We have had a few questions as to whether or not the FDIC's address for Adverse Action notices has also changed. The answer is no; the Walnut Street address is still the correct one to use.

Now for some of you HMDA reporters, get ready to smile!! Effective July 1, 2020, the closed end mortgage threshold went from 25 to 100 mortgage loans. So, for 2021, if you have been a HMDA reporter, but your bank has not originated at least 100 closed end mortgage loans in each of the preceding two calendar years (2020 and 2021) then you no longer have to complete the HMDA LAR. Be sure you can document the number of originations for the two years!

And for a maybe not-so-good HMDA change, effective January 1, 2022 the open-end line of credit threshold decreased from 500 to 200 originated loans for each of the two preceding years. So, if your bank originated at least 200 applicable open-end lines of credit in 2020 and 2021, then you would report 2022 open end lines of credit on the HMDA LAR for 2022.

There is a pretty good HMDA institutional and transactional coverage chart on the CFPB website.

Be sure to forward this information to applicable personnel.

<*Patsy Parkin*>

VALIDATING A BSA/AML MONITORING SYSTEM:

A number of banks now have BSA/AML monitoring systems for identifying potential suspicious activity. Some of the more common systems are Verafin, BAM+, Patriot Officer, and Yellowhammer. Examiners are looking closely at how banks are using these systems and, more importantly, if a bank knows how its monitoring system works whether it is working properly - how it is setup and what parameters have been established. The interesting thing is there is NO regulatory guidance on how to validate a BSA monitoring system!!

Where do you start? As stated above, there are various monitoring systems available. Your bank needs to determine first if it needs a separate monitoring system and if so, which one best meets your needs, based on bank size and the level of risk of your customer base and activities. The bank will need to determine if the monitoring system will interact with the bank's core system in monitoring, and it may need to tweak its practices for recording deposits, wires, monetary instruments and other items to a customer's accounts. For example, if a customer wants to purchase a monetary instrument with cash and the bank does not require the cash to be deposited first to their account, then debited out to purchase the monetary instrument, that cash transaction will not be tied to that customer's account.

One of the things examiners will verify is whether the bank's core system and the monitoring system capture the same items, so if a transaction is suspicious, the monitoring system will pick it up and generate an alert based on the parameters, or "rules," established by the bank. The first thing we do when validating a monitoring system is choose a new account sample for a period of time and compare the CIP information between the core and monitoring systems. Second, we review all account transactions from the account opening date to an "as of" date to see if transaction descriptions, amounts, cash, and posting date are the same for the core and monitoring systems, and that all transactions are being brought over to the monitoring system from the core system. This will "validate" that the systems are "talking" with each other and the same information is being captured. This also goes back to how transactions are captured at the teller line or through other systems, and if they tie back to a customer's account. Another thing to consider is if a customer has multiple accounts, can transactions or the accounts be linked together.

Monitoring systems have different ways that "alerts" may be set. In identifying potential suspicious activity, some systems will set parameters by risk categories or transaction types: cash-intensive customers; international wires; human-trafficking; etc. Others will parse the data further and may, for example, include ranges of cash; ranges of activity by wires, monetary instruments, etc. The key is knowing WHAT parameters the monitoring system uses or has available; HOW the system captures transactions meeting the potential suspicious activity parameters; TESTING to verify that the parameters are properly capturing suspicious activity; and MAINTAINING AND UPDATING software as needed. During an independent validation, testing should be performed to determine if an

alert hit for a potential suspicious transaction, and if not, was there a reason, based on established parameters, why it did not hit.

It is also possible that the parameter settings are generating too many alerts for activity that is not suspicious. Properly validating the system can help determine whether changes in the parameter settings are needed.

Some banks also use the BSA/AML system to prepare CTRs. In these cases, the cash activity from the core system should be verified against the cash activity in the monitoring system to make sure the transactions match.

Training is another area examiners will be interested in. How has your bank ensured the individuals using, maintaining and upgrading the software are aware of the banks changing needs? You will want to be able to demonstrate staff participation in comprehensive software training activities.

The bottom line is BSA/AML monitoring systems can be an excellent tool for a bank in identifying unusual or suspicious activity, but the bank must understand the ins and out of the system and how it is working together with the bank's core system. A bank must ensure that its monitoring system has been adequately and independently "validated" to demonstrate how it is working and that it is being properly used by the bank. A monitoring system is not designed to fully take the place of manual monitoring for suspicious activity. Employees still need to be trained on potential suspicious activity of all types and be fully trained on the bank's BSA/AML policies, procedures, and practices. If you have any questions, please feel free to give us a call.

<Patsy Parkin>

MRCG AND MSRCG FEBRUARY 2022 MEETINGS

The MRCG and MSRCG will hold combined February quarterly meetings on February 17 and February 22, 2022, using the Zoom online webinar format. We will continue our practice of dividing the agenda into two sessions each lasting about an hour and a half.

The first session will be held beginning at 10:00 am on February 17th and will feature presentations on recent changes to the FFIEC BSA/AML Exam Manual, validation and use of BSA/AML monitoring systems, and recent Q&As from the CFPB on Regulation E. .

The second session will begin at 10:00 am on February 22nd and will feature discussion of redlining and the recent DOJ fair lending and redlining initiative, the pending CFPB proposal for data collection on small business loans, and follow-up from the November annual meeting on flood insurance questions.

We look forward to seeing you all online.

<Cliff Harrison>

MRCG-MSRCG COMPLIANCE CALENDAR

01/01/2022 – HMDA open-end coverage threshold permanently adjusts to 200 loans	05/19/2022 - MRCG May Quarterly Meeting
01/06/2022 – Comments due on proposed Reg. B changes for small business loan data collection/reporting.	05/24/2022 - MSRCG May Quarterly Meeting
01/21/2022 – Comments due on CFPB Request for Information on Effectiveness of HMDA Reg. C changes	07/21/2022 - MRCG-MSRCG Joint Steering Committee meeting
02/07/2022 – Comments on FinCEN proposed beneficial ownership reporting rule	08/18/2022 - MRCG August Quarterly Meeting
02/17/2022 – MRCG February Quarterly Meeting	08/23/2022 - MSRCG August Quarterly Meeting
02/22/2022 – MSRCG February Quarterly Meeting	09/15/2022 - MRCG-MSRCG Joint Steering Committee meeting
03/31/2022 – Comments due on CFPB Request for Information on “junk fees”	10/01/2022 – Mandatory compliance date for revised standard QM loans; GSE QM loan category removed
04/21/2022 - MRCG-MSRCG Joint Steering Committee meeting	11/15/2022 – MSRCG November Quarterly Meeting
05/01/2022 – Inter-Agency Rule requiring notice of computer-security incidents within 36 hours effective	11/17/2022 - MRCG November Quarterly Meeting