ROUNDTABLE

Regulatory/Compliance Outlook

EDITOR'S NOTE—This is the latest in a series dealing with the issues facing the real estate finance industry. Each issue we touch on a different topic, asking CMBA's experts for their thoughts on the issue at hand. In this issue of CMFN, we ask three industry players about some of the challenges in today's market. **John Vong** is President of ComplianceEase, a leading provider of risk management solutions to the financial services industry; **Chris Ortigara**, CMB, is a Director with CrossCheck Compliance, a nationwide consulting firm providing regulatory compliance, internal audit, fair lending, and loan review services exclusively to organizations in the financial services industry; and **Joe Tyrrell** is EVP, Corporate Strategy at Ellie Mae, a leading provider of innovative on-demand software solutions and services for the residential mortgage industry. *The views and opinions expressed are solely those of the authors.*

Q: DOES THE CFPB'S BULLETIN REGARDING MARKETING SERVICES AGREEMENTS (MSAS) FORESHADOW THE END OF THESE TYPES OF ARRANGEMENTS?

Vong: Though the CFPB has issued a warning to lenders entering into these agreements and has even fined some lenders for alleged kickbacks and other violations related to MSAs, it isn't a formal regulation. A few larger lending institutions announced earlier this year that they have decided to discontinue MSAs, but whether this is the start of a trend remains to be seen. As long as the CFPB doesn't formally eliminate these agreements, I'm not sure if they will ever completely go away.

I think that the Bulletin is another example of how the CFPB values transparency and borrower choice. We see this in many other CFPB issuances, such as the loan originator compensation rule and the new TILA-RESPA Integrated Disclosure (TRID) rule. For example, under TRID, lenders sourcing services from affiliates have zero tolerance for changes between the new Loan Estimate and Closing Disclosure. Also, one of the main objectives of TRID is to give borrowers more information and choice about how they buy settlement services, and the perception, at least, is that MSAs don't offer this kind of transparency.

Ortigara: Marketing Services Agreements (MSAs) have been under strong examination from the CFPB. There have already been a significant number of enforcement actions by the CFPB related to RESPA, in almost all cases for the payment of improper kickbacks and referral fees. The CFPB has alleged that many MSAs are designed to evade Section 8 of RESPA, which specifically prohibits the payment and acceptance of kickbacks and referral fees.

On October 8th, the CFPB issued Compliance Bulletin 2015-05, describing the substantial risks of MSAs and providing guidance to the mortgage industry. Shortly thereafter, at the Legal and Regulatory MBA Committee meeting on October 18th at the annual MBA conference in San Diego, Paul

...Roundtable Article continued on page 51

Roundtable continued from page 14...

Mondor, Managing Counsel, in the Office of Regulations at CFPB, spoke about MSAs, including the CFPB's receipt of numerous inquiries and whistle blower tips.

The recent Bulletin consists of the CFPB's observations about the legal and regulatory compliance risk associated with MSAs. Determining whether an MSA violates RESPA, according to the Bulletin, requires a review of the facts and circumstances surrounding the creation of each agreement and its implementation. But it is hard to see under what circumstances an MSA would be acceptable to the CFPB.

Previous regulatory interpretations of Section 8 have provided guidance on how to operate MSAs in compliance with RESPA. These interpretations would seem to no longer apply given the current actions by the CFPB. Companies choosing to retain MSAs will be open to potential enforcement action risks. These risks include substantial civil money penalties. Thus, a number of major players in the mortgage industry are no longer willing to retain MSAs. Given these warnings, it would seem any lender choosing to retain or engage in MSAs is taking on substantial risk. So, I would ask any lender that chooses to retain an MSA, why would you? Do you know whether your benefits outweigh your risks?

Tyrrell: I think most risk adverse lenders who were either currently involved in MSA's or looking to create MSA's have already discontinued many of their programs based on the enforcement actions that occurred prior to the bulleting being issued. The bulletin itself certainly may have formalized the bureau's position but anyone looking at recent events could reasonably make the conclusion that MSA's have become an area of scrutiny for the CFPB and while the bureau may not have oversight specifically over realtors they will certainly exercise their authority over lenders, if they believe that consumers are not appropriately protected against relationships that have any semblance to steering or being anti-competitive for the consumer. While MSA's are not illegal, they create extra risk that I suspect many lenders will avoid.

Q: WHAT WILL BE THE BIG COMPLIANCE CHALLENGE FOR LENDERS IN 2016?

Ortigara: As we begin planning for 2016 and give consideration to managing risks, it is important to remember that fair and responsible lending continues to create new and complex challenges for mortgage lenders. With the release of the new HMDA requirements, attention should be on expanding the scope of fair lending risk management plans to two or even three years out.

I thought there was plenty of time to get ready for the "new" HMDA, but according to Loretta Kirkwood, CrossCheck's Managing Director of Fair Lending, the timeframe is actually quite short when you consider the effect on lending operations. This is because the new data collection and reporting will have a significant impact on processes, technology, training, analytics and staffing. Developing an effective plan will involve reviewing and understanding the requirements and developing an implementation plan that addresses all areas affected. It will be equally important to give consideration to how the data will be used and what the data will "show". Analysis should focus on new demographics and the identification of data that is currently available to determine where new risks may emerge.

A few key steps to consider:

- **Processes** – What work flows will require modification to ensure new data is captured accurately on systems and in supporting documentation? What forms will need to be modified?
- **Technology** - What systems will be affected? If there are plans to implement new systems, what testing will be required before selecting a vendor? What phases will be necessary for implementation – setup, testing, and live?
- **Training** – What phases of training are required for which employees? At what point will training be most effective for the implementation team?
- **Analytics** – When will you begin analyzing existing data to identify performance results issues? Who will review the results and manage the changes necessary to limit risks?
- **Staffing** - What is the estimate of time and resources needed to effectively address and manage the process and identify risks? What impact will the additional data requirements have on existing compliance and support staffing?

It will also be important to begin estimating the cost of implementation. Coordinating the impact of regulatory

...Roundtable Article continued on page 52

Roundtable continued from page 51...

change involves a lot of moving parts, but none is more important than determining the associated cost and preparing management for the financial impact.

Fair lending risk management starts with internal controls, but ultimately data is the tool used to identify risk and launch examinations and investigations at the state and federal level. Our advice: Ensure you are ready for the expanded data requirement by beginning sooner than later.

Tyrrell: Better accuracy of data has become critical for lenders and not just for marketing purposes. Whether it's reporting requirements like HMDA and the NMLS Mortgage Call Report or going through State exams, not having a single system of record is a liability that lenders cannot continue to risk. The data in lender's documents absolutely must match their system of record and be the same data that they use to test for compliance. In addition to "Know before you owe," just taking effect October 3, which ushers in a new era of lending of life under TRID, examinations are going to continue to be a focal point for regulators and an increasingly more complex job for lenders as they now must also prove to the regulators that they have a fully functioning Compliance Management System (CMS), which demonstrates compliance at the organizational level, not the loan level, and lenders must show that they are actually implementing consumer driven policies with the associated training for their own employee.

Vong: In 2016, lenders will face two big compliance challenges. The first is TRID fallout: many lenders prepared for the October 3rd start of TRID by investing in technology and redesigning their workflows to take more control of the disclosure and closing processes, but at this point it's unclear how effective all of that preparation was. When the first loans close, and the CFPB examinations and TRID audits begin, we'll be able to see what was executed correctly and what could have been done better. This will help lenders determine how to create a more efficient automated TRID closing process, which will allow them to return to optimal productivity while remaining in compliance.

The second compliance challenge is preparing for the Home Mortgage Disclosure Act (HMDA) rule. The final rule, which was announced in October, will expand the information reported on each loan application and require lenders to report their 2018 loan application register (LAR), which ultimately will be due in March 2019. This means lenders will need to have their technology and processes in place by at least mid-2017 so that they can begin collecting data on the year end mortgage applications that will inevitably spill over into 2018 closings. We recommend lenders make HMDA LAR data processing an ongoing, rather than annual, activity, so that they can spot and address potential red flags early on, before an examiner sees them and before they constitute a pattern. Processing LAR data only once a year is like developing a tax strategy on April 14th—by then it's too late and there isn't a lot you can do.

Q: HOW CAN LENDERS CAN DO TO A BETTER JOB SECURING AND TRANSMITTING DATA/ INFORMATION BETTER?

Tyrrell: It is important to realize that any data has a lifecycle, and hence, securing that data requires protecting its confidentiality and integrity throughout its entire lifecycle. The two most critical stages of any data lifecycle are data-at-rest and data-in-transit. While data is at rest, it is important to protect it against theft or misuse using either cryptographic means or a combination of other acceptable security methods such as access-control. In addition, one of the biggest weakness points for allowing inappropriate access to data-at-rest is actually the lender's own employees. Not necessarily because they are intentionally compromising data, although that occurs as well, but most commonly because they are not well trained on cyber security protocols or practices that can help lender avoid their data being accessed. When data is in transit, it needs to be protected using a secure channel so that if the traffic is intercepted, the data is not exposed or stolen. Depending on the use case, one of several industry-acceptable security protocols can be used to achieve data-in-transit protection. Key to this process is to avoid exporting data out of your system of record at all costs. Leverage the direct integrations that utilize encryption that are available within your system of record. Each time data is exported and then uploaded into websites, it increases the likelihood of that data being compromised in transit.

Vong: The old way of delivering documents through different portals and communicating via insecure email, fax, phone, or courier services is not only ineffective, but could also lead to noncompliance. Lenders need close

...Roundtable Article continued on page 53

Roundtable continued from page 52...

collaboration with their settlement agents and other settlement services providers. The best way to do that is via technology that enables the parties to communicate securely and in real-time, as well as exchange data throughout the closing process to eliminate closing defects.

Our company has developed a solution, called *ClosingXchange™*, that allows lenders and settlement agents to safely communicate and collaborate, while also keeping an audit log of all conversations, documents, status changes, approvals, scheduling of events, changes of circumstance, and delivery timing in a single objective record. In addition, it transmits settlement agent data directly into *ComplianceAnalyzer®* with *TRID Monitor™*, our online compliance management platform, for real-time integrated loan level auditing including pre-close and post-consummation review—identifying fee tolerance variances with valid changed circumstances before loans close.

We believe solutions like ours, that combine collaboration portals with compliance technology, will help protect the security and privacy of borrowers' non-public personal information, improve workflow quality and efficiency, and lead to smoother, more profitable closings.

Ortigara: It seems like every day we are reading or listening to news about successful cyber intrusions into a company's confidential data base. It is disconcerting enough when these companies are major financial institutions or health care organizations. But, when the cyber intrusion is successful and the target is the U.S. military or some high powered government entity entrusted with highly classified material, it makes me wonder how any organization can keep their data safe.

So it was with great interest that I attended the session on "Privacy Technology and Cyber Security and Issues for the Mortgage Industry" on October 20 during the MBA's Annual Conference in San Diego. Roger Cressey, NBC Counter-Terrorism Analyst and former presidential advisor was a key speaker. He provided some valuable insights into protecting your company against cyber-attacks. He talked about why the threat of the environment is only one part of the equation and why managing cyber risk in our interconnected workplace is everyone's responsibility.

Malware programs are being created daily by criminals. Hackers can gain access through vendors, phishing emails, and various socially engineered techniques like malware induced stick drives left on company locations. It is virtually impossible for any entity to keep up with all of these malware programs, so one can forget staying ahead of these programs.

If you can't stay ahead of this, what can you do? You must have an effective system in place to manage your cyber security. First, you can educate your employees. This is more than a discussion about not sharing passwords or leaving them pasted to their underside of their computer. It also includes information about how malware enters a computer as well as the importance of using secure portals and encrypting data to transmit and receive confidential information. Educating your employees can also be accomplished by what the technology industry calls "Table Top Exercises." These exercises involve multiple parties from throughout the organization. Preparation is key. Use resources from within your industry and do research on cybersecurity. Make the scenario as realistic as possible.

Second, you need a process in place to handle situations when a breach has occurred. You need to walk through how and when you will respond when a breach has occurred.

Third, using up to date technology and effective software systems can help. The software will likely not provide 100% protection, but paying attention to what you are using and doing your homework will separate you from companies that do not have a focused and well-monitored program in place. And, perhaps most important, if your organization does not have sufficient internal expertise on cyber security matters, hire an organization that does.