

Remarks by
Grovetta Gardineer
Deputy Comptroller for Compliance Operations and Policy before the
2015 Association of Military Banks of America Workshop
Leesburg, Virginia
August 31, 2015

Good morning. I am again proud to be with the Association of Military Bankers of America at your annual workshop, and I am honored to be the first in the parade of regulators you have lined up today. On behalf of Comptroller Curry and the Office of the Comptroller of the Currency (OCC), thank you for inviting me to be part of this event.

Before diving into the “OCC Update” as the agenda promises, I want to congratulate Major General Steven Lepper on becoming President and CEO of this organization. Your 35 years as staff judge advocate will serve you well, and no doubt that resolve and mettle you developed at *the Academy* will make you ready for whatever these bankers throw at you. I look forward to working with you, and getting to know you, just as I enjoyed working with your predecessor General Egeland. I know you will be a huge success.

Your theme for this year’s workshop could not be more relevant or timely—“Financial Security in A Virtual World.” That is a big challenge—one that we all grapple with in some way. Over the next few minutes of delivering an “OCC Update,” I hope to share a little about what we, as regulators, are doing to make financial security in a virtual world a little more achievable. First, I will discuss a couple of compliance issues facing banks and thrifts related to serving the military community, then touch on efforts to enhance the readiness of our financial system to withstand cyber attacks, and finally close by sharing some thoughts on responsible innovation.

As I mentioned last year in my remarks to this group, I have not worn a military uniform as some of you have, and as some of you still might. But, my family members have, and I am proud of their service and grateful for the sacrifices made by all veterans and their families. I have a personal sense of connection with your mission, and share your belief that the community you serve is special. The men and women who have served, and the families alongside of them, have earned the unique protections that they enjoy under the law. It is unfortunate that some—nonbank financial service companies and commercial banks—fail them. And yet, it happens. Nonbanks and commercial banks alike continue to fail to provide all the safeguards required by law or worse, actively take advantage of the vulnerabilities unique to our servicemembers and their families. In reviewing compliance with the Servicemembers Civil Relief Act of 2003 (the SCRA), OCC has seen deficiencies in the practices and procedures at some banks related to their SCRA-compliance programs. Banks have been directed to improve SCRA-compliance policies and procedures for determining whether servicemembers are eligible for requested SCRA-related benefits in all accounts the borrower may have, not just the account that is the subject of the request. We also expect that banks ensure that they calculate SCRA benefits correctly and have procedures for verifying the status of servicemembers' eligibility for SCRA protections, before seeking default judgments on extensions of credit, and before initiating the foreclosure or repossession process. In conjunction with deficiencies in an SCRA-compliance program, we sometimes find problems on a wider scale; these failures involve problems with the bank's enterprise-wide compliance risk management program.

Compliance with the 2003 law remains a matter of great concern to the OCC. Simply put, there are banks that continue to fail to have effective policies and procedures across the bank to ensure compliance with the SCRA and to provide the protections afforded to servicemembers

under the law. As military bankers, I know you share our concern. We check for SCRA compliance during every exam cycle at every bank we oversee. Following a 2012 GAO report on mortgage foreclosures that found limitations in federal regulators' oversight of SCRA compliance, we reviewed our SCRA examination program and instituted an annual review of SCRA compliance in the examination process. This review is not required by law, but given the importance of servicemember protections, we require it as an OCC examination mandatory minimum—or, in other words, it is OCC “standard operating procedure.” As a result, we are seeing some progress and finding more robust compliance among the banks we regulate. In 2014, we cited 65 SCRA violations among large, midsized, and community institutions. For the first quarter of 2015, however, OCC examiners have only cited seven SCRA violations. Given this data, I hold out hope that these numbers will continue to trend down for the remainder of the year as compared to 2014.

Another important development for the protection of servicemembers and their loved ones is the recent amendments to the Military Lending Act (MLA) regulations. In July, the Department of Defense (DoD) issued final amendments to expand the coverage of its rules that implement the MLA. As you know, the MLA was enacted in 2006 to address predatory lending practices targeting servicemembers. In 2013, the National Defense Authorization Act made some changes to the MLA, including creating a private right of action. It also gave administrative enforcement authority to the federal banking agencies and the CFPB while the DoD retained MLA rulemaking authority.

The DoD's final rule broadly expands the coverage of the MLA rules to both open-end and closed-end consumer credit. The rule will now apply the protections of the MLA to payday loans (regardless of loan amount or duration), vehicle title loans, refund anticipation loans, deposit

advance loans, installment loans, unsecured open-end lines of credit, and credit cards. It will exclude certain forms of credit, such as residential mortgages and loans to purchase a vehicle, as required by the statute. With the exception of credit cards, which will have a delayed implementation date for at least two years, banks will need to comply with the rule's requirements for covered loans that are established on or after October 3, 2016. As such, change management is critical. Banks should not delay in addressing the new requirements. They need to work on updating their policies, procedures, practices, forms, software, and other applicable resources. Banks should decide the process they will use for performing a covered borrower check to assess whether the borrower is an active duty servicemember or a dependent of a servicemember. The bank may elect to use the safe harbor process of verifying the status of the consumer by using the DoD's database, or it can decide to use an alternative method. As such, banks will likely need to adopt new workflows. In addition, banks must incorporate a mandatory disclosure to consumers into the loan process. The rule, of course, provides an model disclosure statement. Banks also will need to implement program adjustments to calculate the "all-in" Military Annual Percentage Rate, which includes the fees for credit-related ancillary products, such as credit default insurance and debt suspension plans.

Like you, the OCC will need to prepare for the upcoming changes. The OCC intends to work with the other federal agencies to develop examination procedures over the next year so that we are prepared to review our supervised institutions for compliance with the MLA and the DoD's implementing rule.

If consumer compliance failures get you on to the business pages of local newspapers, cybersecurity failures will land you on the front page of the *New York Times*. That is a fact that veterans and the DoD community know all too well. It is also a fact that keeps many bankers and

regulators up at night. Make no mistake, cyber threats against financial institutions of all sizes are increasing and becoming more and more sophisticated. That's why improving cybersecurity has been a personal priority for Comptroller Curry. And that's why over the past couple years, the OCC and other member agencies of the Federal Financial Institutions Examination Council have worked to improve coordination and communication among regulators and supervised institutions and to enhance awareness of current threats and vulnerabilities so institutions can act quickly to mitigate the risks. Even more significantly, the FFIEC agencies have established a cybersecurity assessment tool to help banks and examiners assess the maturity of cybersecurity programs.

Now, I don't want to take away Deputy Comptroller Beth Dugan's thunder. Beth's team represented the OCC in developing the FFIEC cybersecurity assessment tool that the FFIEC agencies released in June. She will discuss the tool with you during the Cybersecurity Panel later today. But, the cybersecurity assessment tool represents a significant step forward in the supervision of banks and thrifts as it relates to cybersecurity. It provides a common framework for assessment across institutions, and over time, will allow regulators and bankers to track their progress and have better view of the industry's ability to withstand cyberattacks. The tool also helps bankers and examiners talk through issues facing individual banks. The use of the assessment tool is optional for financial institutions; however, OCC examiners will use it to supplement exam work to gain a more complete understanding of an institution's inherent risk, risk management practices, and controls related to cybersecurity. While we will never really know if these measures actually thwart a specific attack, we can be certain that more breaches will occur if we do not commit to being vigilant and continuously enhancing our ability to prevent, detect, and recover from cyber incidents.

Up to this point in my remarks, I have focused on risks—compliance risk related to SCRA and implementation of the MLA and, briefly on cybersecurity risks. Now, I'd like to switch gears and talk about something more and more people are discussing within the banking industry—innovation. Since I am a regulator and a compliance professional, let me qualify that by saying, I'd like to talk about *responsible* innovation. Responsible innovation in the financial services industry is something Comptroller Curry called attention to in August.¹

There is little doubt that we are at a point in the industry's evolution where we expect tremendous innovation. New stories about financial innovation appear every day, not only in banking trade publications, but in national newspapers highlighting neobanks, innovation labs, new products, and services. It's impossible to escape the conversation about innovation right now. Why?

Well, technology is driving innovation. Generational change is driving innovation. The demand for efficiency is driving innovation. And, the need to seek new profit opportunities is driving innovation. Customers demand instant, mobile access to everything, and we are seeing customers turn to alternative service providers in droves when traditional financial service providers can't satisfy their appetite.

Services like Square and Apple Pay have the potential to disrupt dominant pay processors as they reduce the barriers to entry for business and consumers transacting payments—everywhere. Apple Pay registered more than one million credit cards within the first 72 hours of operation. Square processes more than \$30 billion in transactions per year. New forms of

¹ See NR2015-111, "Comptroller Discusses Responsible Innovation, Risk Management" (<http://www.occ.gov/news-issuances/news-releases/2015/nr-occ-2015-111.html>).

payment processing may turn out to be an innovation that banks can assimilate into their processes to make things work more efficiently. They may only bring incremental change.

Other innovations may strike closer to the heart of *what banking is* and compete directly with banks' role as a provider of credit and a safe place to store wealth. Crowdsourced lending and peer-to-peer lending are gaining traction. Lending Club uses technology to connect borrowers and investors and has facilitated more than \$2.7 billion in consumer loans. That is a lending portfolio bigger than 97 percent of the lending portfolios in the banking industry. Kickstarter and GoFundMe have been providing seed funding and credit for several years as laboratories for consumer products. Businesses also are being financed in new ways, such as payments-based lending. Square Capital, a division of credit card processor Square, advances money to businesses, which is then paid back by taking a portion of each payment transacted through Square. People everywhere have the ability to transfer funds to one another with the click of an app. More than 1,400 banks have incorporated Popmoney into their systems to allow peer-to-peer transfers.

Responsible innovation requires careful risk management and a great deal of scrutiny to ensure that it delivers its promise safely and soundly, consistent with applicable laws and regulations, and in a way that ensures adequate consumer protections. That caution, however, cannot and should not stop the wheels of innovation from turning. If the current financial service industry participants fail to innovate, someone else will, and today's service providers will become historical footnotes. We need new approaches that meet the changing needs of consumers, businesses, and communities so that banks can continue to be a source of strength for the nation's economy and your local communities. As the primary regulator for national banks and federal savings associations, the Comptroller understands that one of our jobs is to support

and even encourage innovation that helps banks serve their public purpose. In fact, the ability to adapt to the changing needs of bank customers has been a hallmark of the national bank charter since President Lincoln created the national banking system in 1863.

At the OCC, we've launched a new initiative that encourages and supports responsible innovation among the institutions we oversee. What we want to do is develop a framework to evaluate new and innovative financial products and services. By doing so, we can eliminate the misperception that it is too difficult to innovate in the regulated space—a perception that may be contributing to more and more innovation occurring outside the regulated financial industry. The Comptroller has assembled a team of representatives from across the agency that includes policy experts, examiners, lawyers, and others focused on the question of “What can the OCC do to support responsible innovation that better meets customer and community needs in safe and sound manner?” As a result of the effort, the agency hopes to improve its ability to identify and understand new trends and new technology, as well as the emerging needs of financial services customers so that the OCC can more quickly evaluate those products that require regulatory approval, consider the supervision implications of the innovation, and identify any risks associated with them. After all, responsible innovation holds the key to “Financial Security in A Virtual World.” It just might hold the key to more prosperity, too.

Steve, thank you again for inviting the OCC and me to join this workshop and congratulations on hosting such a terrific event. I also want to thank all of you for your continued commitment to serving America's military members and their families. These events provide important opportunities for regulators and industry participants to hear from one another and discuss the challenges we face together. While these events provide a terrific forum, you don't have to wait for events like these to discuss the concerns you have. Those of you from

large and midsize banks have dedicated teams of examiners who can answer your questions. Likewise, community banks and thrifts have an assigned portfolio manager and a local Assistant Deputy Comptroller who know your institution and can discuss your concerns. These experienced examiners also can reach out to the agency's national network of experts for additional insight and information so that you can benefit from our view across the financial system.

Thank you for listening and I look forward to answering your questions and hearing the other speakers today.