Remarks by

Thomas J. Curry

Comptroller of the Currency

Before the

BITS Emerging Payments Forum

Washington, D.C.

June 3, 2015

Good morning. For as long as I can remember, we've been hearing predictions that the cashless economy is on its way. Obviously, we haven't gotten there yet, and we may never get there in any literal sense. It's fair to say that coins and bills still remain fixtures of our payments system. But each time we reach for our credit cards or debit cards or smartphones to complete a transaction at a point of sale terminal, we are reminded of how digital payments have transformed the way buyers and sellers connect. Conferences like this one provide further proof of that fact, and I'm delighted to join you today.

In my time with you, I'd like to explore the implications that changing delivery channels and technologies may have on banks and their customers and the role that regulation and supervisors play in these issues.

The first question I often hear in these discussions is whether banks will still be relevant in the not too distant future, or whether new technologies and players will supplant traditional banks. There is no question that depository institutions occupy a very

important place in today's larger payments universe. But that begs the question of how important will banks be in tomorrow's payments systems. We hear it all the time that banks are unable to compete with aggressive newcomers for market share. But we've heard that before. In fact, almost every key financial innovation in recent years has inspired predictions that traditional financial institutions would soon fall hopelessly behind. This will be an ongoing strategic threat. To date, financial institutions have succeeded despite those predictions.

The tendency to underestimate the dynamism of the banking system should be resisted because banks have been the source of so many of the innovative products and technologies of recent years. Consider, for example, the way banks embraced, and in some cases developed, automated teller machines, Internet banking, mobile applications, and more. Nearly 15 years ago, one of my predecessors noted that the number of OCC-supervised banks offering on-line banking had more than doubled during the previous 15 months—that at a time when there were several thousand more national banks than there are today. Today, practically all banks offer their customers a more or less comprehensive menu of online products and services. According to a 2013 Pew survey, 51 percent of all U.S. adults report that they banked online, a number that has undoubtedly grown substantially since then.

In other words, banks traditionally have been leading users of technology. I believe that when historians look back at it, they will conclude that online banking was one of a handful of computer applications that turned the PC from an interesting toy to an indispensable tool for millions of Americans, which in turn helped drive the development of a more computer-literate, technology-based society.

Likewise, I believe the predictions that new technologies will make traditional banks obsolete also are misplaced. Banks of all sizes are playing important roles as pioneers and partners in the development and adaptation of emerging payments technologies. Their partners are some of the biggest names in technology—Apple, Google, and Microsoft come to mind—but also some of the smallest, as banks seek out promising start-ups with technologies that can be quickly and efficiently brought to market. Banks are engaged in organizations like BITS and the Bank Innovators Council, through which they share brainpower and financial resources. Some banks are setting up innovation incubators, where they have the freedom to pursue, implement, and field-test new technologies.

This activity underscores why banks are such formidable technology competitors. Banks enjoy the advantages of name recognition and marketing prowess, which are products of years of experience, investment and trust. After hitting bottom during the financial crisis, surveys show that banks have made significant progress rebuilding public trust, which is especially critical to success in the financial technology realm.

The growing use and reliance on e-banking facilities raises a second set of questions that I believe the industry and regulators must collectively address. First, how do we ensure continued access to banking services for all Americans? Technological advances present both great opportunities and challenges. Policy issues related to the digital divide between those with access to the latest technology and those without may be amplified when banks reduce their brick and mortar branch presence particularly in low- to moderate-income communities. One of my challenges to you today is to consider how we can harness emerging technologies to better serve the unbanked or underbanked

segments of our society and to ensure that all our neighborhoods and citizens have access to safe and affordable banking services.

Safe and secured financial transactions are the cornerstone upon which our payments and banking systems are built, and it's an area where the industry and regulators share some common goals. Unfortunately, the same technologies many of you in this room have employed to provide new and efficient delivery channels for your customers are also being used aggressively by hackers and criminal elements, which brings me to the all-important question of cybersecurity. Cyber criminals will also probe emerging payments systems for vulnerabilities that they can exploit to engage in money laundering, which has broad national security implications.

I believe banks have an advantage over many of their non-bank competitors in the cybersecurity and anti-money laundering arenas in part because of the regulatory regime that they operate in and the industry's collective interest in protecting the security of the payments system. In addition to ensuring that banks adhere to various regulatory standards and policy guidance, regulators provide an additional set of highly trained eyes to the process of determining what risks banks face and how well they manage those risks. In addition, regulators provide technical expertise that is particularly important to community banks.

For example, recognizing the changing dynamics of the payments industry, the OCC created a dedicated Payments Risk policy group, whose director, Kathy Oldenborg, was with you yesterday. Kathy and her team provide examination support, training, and guidance to our examiners and act as a resource for our institutions on these and the more traditional payment structures across the retail and wholesale payments landscape. We

also established a Critical Infrastructure policy group, which develops and coordinates the OCC's cybersecurity policy initiatives.

One of my top priorities as Comptroller—and, until recently, as chairman of the Federal Financial Institutions Examination Council, or FFIEC, the body that coordinates bank supervisory efforts—has been to address the risks that cyber threats pose to individual banks and the banking system. This effort necessarily requires extensive and ongoing coordination among regulators and banks, large bank and small banks, regulators and the rest of Government, and the financial sector and other critical infrastructure sectors. BITS and the national and state banking associations have taken a welcome leadership role in this area.

On an interagency basis, we created an interagency Cybersecurity and Critical Infrastructure Working Group under the FFIEC umbrella to increase cybersecurity awareness, promote best practices in the industry, and to strengthen regulatory oversight of cybersecurity readiness. Last year, the banking agencies conducted a joint assessment of cybersecurity preparedness at more than 500 institutions, which provided a great deal of helpful information for regulators and bankers alike. We summarized our findings in a paper containing key observations and questions that chief executive officers and boards of directors may consider when assessing their institutions' cybersecurity preparedness. The FFIEC importantly recommended that financial institutions of all sizes participate in the Financial Services Information Sharing and Analysis Center, or FS-ISAC, a non-profit, information-sharing forum established by financial services industry participants to facilitate the sharing of physical and cybersecurity threat and vulnerability information.

The free flow of real time information about threats is critical to our cybersecurity defenses.

As a follow-up, the FFIEC will soon be releasing a Cybersecurity Assessment Tool that financial institutions will find useful in evaluating their inherent cybersecurity risks, including those in existing and emerging payment areas, and their risk management capabilities. The results will shed light on how well cybersecurity measures already undertaken comport with the bank's cybersecurity risks. I want to emphasize that the assessment tool is exactly that. It is a tool to help banks, particularly community banks, to defend against cybersecurity threats. Those threats are real and they are unlikely to abate anytime soon. In fact, they are more likely to increase. I would caution against anyone viewing this effort and the OCC's complementary cybersecurity examination program as an unnecessary regulatory burden. The time to act is now.

At the same time, individual FFIEC members are enhancing their incident analysis, crisis management, training, and policy development, while also expanding their focus on technology service providers' cybersecurity preparedness. And we at the OCC are continuing to improve our collaboration with other agencies and communicate the importance of cybersecurity awareness and best practices among financial industry participants and regulators.

My point here is that regulation adds significant value in the areas that we're discussing today. For example, efforts are well underway to bring e-commerce and emerging payments systems deployed by non-bank players under greater regulatory scrutiny. Using authority granted by the Dodd-Frank Act, we can ensure a more level

playing field and protections for customers of non-banks. Certainly, they deserve no less.

But there is no denying that regulation can be burdensome—and expensive. Regulatory burden is something we at the OCC worry about a good deal, and we are doing everything possible to ensure that our regulations are rational, relevant, and cost effective. In one such initiative, the OCC and the other banking agencies are holding hearings around the country in connection with the Economic Growth and Regulatory Paperwork Reduction Act of 1994, better known as EGRPRA. Through these hearings and through the written comments we receive from bankers and others, we are discovering ways to cut regulatory burden without jeopardizing safety and soundness and compliance safeguards. We have focused considerable attention on ensuring that the Bank Secrecy Act, which was enacted in 1970, remains equal to the challenge of defending our financial system from those who seek to use it against us. In particular, we are working with our colleagues to find better ways to use technology to provide more accurate and timely information to law enforcement and regulators, while simultaneously reducing cost and burden.

One of the lessons we have learned in the bank regulatory community is that collaboration is vital, especially in dealing with highly complex, rapidly evolving challenges like cybersecurity. I'm referring not only about collaboration and cooperation among the banking agencies, but also among financial providers. As I've already noted, the big part of what we're doing at the regulatory level to meet these challenges is to encourage financial institutions to share information and best practices. Similarly, as I

said earlier, we encourage partnerships between banks and technology companies to leverage each other's strengths and compensate for each other's weaknesses.

Competition, of course, has been programmed into our national DNA, and it would be futile to suggest otherwise or to deny the myriad of benefits that come from it. Fair competition in the payments system—indeed, in financial services generally—will encourage providers to step up their game and provide consumers with more and better choices at lower cost.

I believe that is an outcome we can all support.