Remarks of Jacob J. Lew
Conference on The Future of Global Finance: Populism, Technology and Regulation
Columbia University
October 20, 2017

Thank you Dean Janow for that kind introduction, and thanks to Trish Mosser for organizing this gathering on a timely and important topic. It is a pleasure to join you today.

We gather at a time when technological developments in finance and broader global challenges come together in a way that makes it vital to approach innovative financial technology in a careful, coordinated and thoughtful manner, so that doors to progress continue to swing open rather than closed.

Technology is advancing more rapidly than ever before, with the promise of faster, more accessible and more efficient practices. At the same time, long standing concerns about privacy are further complicated by the proliferation of malign state actors and decentralized criminal and political forces that expose all of us to the risk that powerful tools and centralized information can cause harm if they fall into the wrong hands. Contemporary issues like the ownership of information and digital fingerprints present both opportunities and challenges. Old problems do not go away simply by shifting from bricks and mortar to digital business practices: consumer protection and financial stability remain ongoing core concerns.

In a competitive world, where nations seek to protect the rights of their citizens, but also look for ways to encourage domestic economic growth, issues like privacy concerns and the ownership of data can too easily become a cover for non-tariff barriers or backdoor taxes. Efforts to require data localization, for example, work against many of the natural advantages of a global technology platform, but are too often a common response. And in this increasingly global marketplace, the challenge to develop clear regulatory guidance is both a domestic and international concern, with consistency across jurisdictions critical to efficiency, but so difficult to achieve.

I would like to begin with a reminder of the benefits that technology, like modern payment processing, provide and then turn to a constructive approach to managing the risks and the inevitable regulatory response. The many benefits are a powerful reason to get this right.

Speed and efficiency in payment processing facilitates commerce and financial inclusion and is a catalyst for growth and shared economic opportunity.

From inventory management that has made it obsolete for businesses to hold costly stockpiles of spare parts to consumers having the commercial world at their fingertips, saving them time and travel expense – financial technology is reshaping the world of commerce, and will continue to do so in the future.

In terms of financial inclusion – increasing the number of people connected to the formal financial system -- technology lowers the cost of service and opens a door for the unbanked in both the most advanced countries and the developing world to get a foothold on a more secure financial future. When men and women who previously lived in a cash economy start to build a financial record and establish payment histories, it means that they will ultimately have greater access to capital for both entrepreneurial endeavors and family security. Technology based payment platforms can also accommodate first time savers as they begin to build a nest egg.

The need to be physically present to conduct commerce is becoming a thing of the past. This means that in places where brick and mortar branches are simply uneconomic there is now a real opportunity to connect billions of people worldwide to the financial system. In India alone, nearly one billion people have been registered in a digital financial network with secure biometric identification for each person registered. The suite of services available on the platform is only now beginning to grow, but the door is open. From Malaysia to Mexico to Nigeria, we have seen successful experiments in electronic payments and banking open a path to financial inclusion. And in developed countries like the US, where millions remain unbanked, we see a path ahead to closing that gap.

One can look at financial inclusion as a way to improve the economic condition of an individual and his or her family. And that is important, whether a woman in Africa is seeking hundreds of dollars to invest in a farm or a construction worker in Alabama needs access to capital to purchase the tools to start a home building business. In addition to personal opportunity, access to capital helps boost broader economic and job growth, particularly since small and medium size enterprises are so often the engines of enduring economic progress.

Finally, financial inclusion makes our world safer. When we shrink the cash economy, we make it harder for malign actors – whether criminals or terrorists -- to take advantage of an economy that operates in the shadows. I have long argued that the ideas of financial inclusion and combatting money laundering and other malign activities go hand in hand. And the idea of choosing one at the expense of the other is counterproductive to both goals. I am proud that we made progress on these issues when I was in office, and the challenge is one that requires ongoing attention.

With so many advantages, why, you might ask, would anyone do anything to slow the march of progress?

And this brings us back to the risks. I will focus on three in particular today: cyber security, concentration of risk at central points, and systemic risk that can emerge when trusted old platforms, with long established oversight, are replaced by new processes that are not yet subject to appropriate safeguards.

Cyber security, once relegated to the technical world is no longer an esoteric topic left in the tech department. It is a strategic risk that in government is addressed by the most senior executives – in government at the level of the Secretary -- and in the business world, it is now a C suite issue. And that is where it should be.

It is safe to say that no one in this room has been untouched by cyber risk. Whether a credit card stolen online, or personal information hacked from a financial institution, insurance company or government agency, free credit monitoring is becoming the new normal. The centralization of data in systems that make it easy for us to transact business, apply for credit, process our medical claims, opens a door to bad actors who have powerful incentives to outsmart any protections we build.

As Secretary of the Treasury, I was proud that we developed a tool that made it easier and faster to access personal tax records when applying for a mortgage, and frustrated when we had to take it down and slow it down because imposters figured out how to use information available on the dark web to masquerade as legitimate taxpayers and get access to prior year tax returns and file for refunds before the actual taxpayer. The goal of speeding up legitimate access had to be slowed down to make it safe in a world of cybercrime, where secure verification practices are essential to blocking bad actors.

When you look at the scale of hacking, whether government systems, credit card platforms, health insurance processors or credit bureaus – the possibility of causing massive exposure to harm cannot be treated lightly. It is bad enough to steal the credit card or tax refund of one or a hundred innocent customers and taxpayers. At a larger level, the risk of corrupting trusted systems could undermine commerce and security in a far broader way. At the extreme, it presents a risk to financial stability and national security.

The answer is not to erect a stop sign to block new technology. The challenge is to invest in the highest level of cyber security possible, and to educate users on practices that they can employ to protect themselves. And to recognize that it is not a battle that you can win once and turn from, because new threats will constantly appear.

Information is the key to building a strong defense. Evidence of an attack or a malicious practice cannot remain in the silo where it first appears. Information must flow freely within a sector and between sectors to quickly contain damage, even as the repair begins. This means that the stigma of being attacked needs to disappear. It cannot be considered a sign of failure to report an attack, but rather, a sign of good corporate or governmental citizenship. There cannot be any suspicion that sharing such information, or the technology to combat the threat, is an antitrust practice. Reputationally, the risk should be that failure to disclose an attack not the attack itself is the risk to be avoided.

We did much both through executive action and finally in terms of legislation to foster this approach. One of my early actions as Secretary of the Treasury was to insist that we develop trusted and cleared relationships in major financial institutions so we could share in real time information about threats, while there was still time to address them, even if the source of the information was classified. We developed reporting mechanisms for businesses to share with appropriate government offices information about exposures.

Withholding information, whether to protect franchise reputation, or worse, to permit economic rent seeking that may come with early knowledge of an attack, should be treated as a violation of trust, and if there is illegal activity, should be prosecuted.

The largest financial institutions have the resources to build their own defenses, but many smaller firms do not, and even the largest financial institutions employ smaller contractors, which can open the window to risk unless we are all in this together. That means developing best practices, insisting that contractors meet best practices and educating customers in sometimes inconvenient practices, like dual factor identification, which can make all of us safer. And technology can help here as well, through unique digital identifiers and tokens that permit users to be safer, without requiring each of us to remember a myriad of personal codes that no human memory can store, and that are immediately compromised if we write them down or store them on our systems.

The financial sector in the US has made a great deal of progress, but much remains to be done. And even if the sector itself was “safe”, slower progress in vitally connected sectors – from the electric grid to telecommunications – means the challenge is far from resolved.

Businesses must manage their exposure to risk by earning a reputation for candor and full disclosure, and when an incident occurs, they must respond quickly, transparently and effectively. Sadly, we too often see that this lesson has not been learned, and the consequence fosters public distrust rather than greater confidence.

A second risk is that centralizing information permits both efficiency and transparency, but also creates larger potential points of failure. I learned this as we worked to address one of the big problems that led to the financial crisis in 2007-2008 – an opaque derivatives trading system, where the inability to know the exposure of financial institutions accelerated and broadened the panicked sales of assets and deepened the damage of the crisis. The solution was to create centralized derivatives clearing platforms so we now know what stands behind traded derivatives and the level of risk within a portfolio or an institution. Centralized clearing has made our financial system safer, and therefore, reduced the risk that a financial crisis would again bring down our economies. But at the same time, the integrity of these central platforms presented a new challenge and we needed to develop standards to make sure that the new clearinghouses themselves could weather extreme stress and maintain liquidity and operational integrity.

As new technologies and a growing number of independent payment processors carry much of global commerce, there will be questions about the financial soundness of those platforms and their ability to withstand the shocks that inevitably occur when some parties fail or act badly. The ability to demonstrate that a large and global financial platform can maintain liquidity and operational integrity -- even if subject to stress -- is crucial.

And this leads to my third risk, that new technology needs to embrace the need for oversight to develop in an appropriate way. Long established practices and systems are monitored through banking or security oversight, which puts up guardrails to ensure safety and soundness. A new fin tech application that does not take traditional deposits or trade in securities may not fit the old model, but concerns about safety and soundness may still be real. What about payment cards that look more and more like they are storing savings? Or a global payment systems where failure to maintain overnight liquidity could raise financial stability concerns?

Emerging business models require solutions that fit the new challenges. It does not mean a one size fits all approach, where we use a single hammer to treat every new innovation as an old fashioned nail. It means that we need to have an open process of inquiry that asks the questions about what risks require oversight and regulation, and what is the appropriate and least burdensome way to provide that security. And as we are seeing this week in bipartisan legislation to deal with advertising on social media, if important vulnerabilities are not addressed by self-governance, a public response will not be far behind.

In so many parts of the financial system, we are seeing the development of new business models that do not fit old patterns. As Secretary, I urged that we ask tough questions but only act if necessary. For example, in our review of the asset

management industry. It is critical that asking tough questions not be treated as an obstacle to progress. To the contrary, it should be embraced as a way to make sure that sensible rules of the road for the future can be developed and to strengthen the ability of our oversight processes to detect real risks rather than either responding mechanically with old answers, or by shutting off the radar we need to detect or prevent the next financial crisis.

What is the right government response?

Regulators should remain open to innovation; whether checking accounts, credit cards or ATMs private innovation opens doors to new practices that often disrupt and improve on what came before. But old policy concerns, from adequacy of resources to assure uninterrupted service, to levels of consumer fees and interest rates, to preventing illegal money transfers are still real.

The US has traditionally been a global leader, first in developing domestic standards and then along with other leaders we have collaborated to establish best practices as a global norm. In the last decade, the US and the UK responded most effectively to domestic financial stability concerns after the financial crisis, and we worked together through the G20 to establish the Financial Stability Board to promote global standards. I applaud the work that Mark Carney has done at the FSB and worked closely with him to make sure that we would leave behind lasting legacy of safer and sounder practices, which I believe we have. We also worked in the G7 to begin a similar practice of sharing best practices and information on cyber security.

With our uniquely decentralized regulatory system in the US, as the chairman of the Financial Stability Oversight Council, I tried to drive the work of independent regulators to address emerging issues in a consistent manner. But independent regulators are just that, and it is an ongoing challenge to minimize the development of inconsistent standards. Work like the US National Institute for Technology Standards establishing uniform best practices on cyber security helped in this emerging area to promote a common approach, but in the end of the day, decisions on appropriate standards for bank examiners will be made at the level of each regulator.

Rising populist sentiment against globalization makes this kind of collaboration more challenging. During the financial crisis it was essential to stop the collapse of major financial institutions to prevent a depression, but there is lingering cynicism about deferring to elite and expert voices and institutions. There are questions about how this reliance affected pre-crisis regulatory policies. And even though taxpayers in the US were paid back the capital used to stop the crisis, the lasting memory is that institutions that were too big to fail got help while Main Street businesses largely had to fend for themselves.

In US political debate, the FSB, for example, is too often treated as a mysterious foreign meeting of international bankers to impose its will on our domestic policy. In fact, working through the FSB, with partners like the UK, the US has convinced countries around the world to adopt practices more like our own.

Without harmonization, compliance will be more complicated and costly, and may create a competitive disadvantage to firms in countries with high standards. This is one of many examples where we need to make the case for confidence in expert bodies, and push back on the notion that elite institutions should not be trusted. In a well-informed political debate it would not be possible to dismiss the FSB with fears of black helicopters invading our sovereign spaces.

At the same time, ironically, some question the need to maintain the higher oversight standards adopted post-crisis. For example, from the outcry one hears about the process for designating systemically significant financial institutions for enhanced oversight, one would think that hundreds or even thousands of institutions had been named, not that you can count the number of designated institutions on your fingers. In reality, this authority has been used judiciously, and decisions have been reversed as the facts change and the risk level changes.

Privacy and ownership of information – even where it resides – are important issues, where reasonable approaches can vary widely. In the US there is a tendency to be more comfortable when information is held by a private party – even a large business rather than a governmental entity. In Europe, the opposite holds true – where there is widespread discomfort with large companies, particularly foreign companies, controlling too much information.

It is important to work towards widely accepted standards, because a balkanized approach is not only inefficient, it can become an obstacle to truly global systems. It is easy to see how concerns about privacy standards, consumer protections or information accessibility for law enforcement and regulatory oversight can become an excuse for countries to demand control and require local servers – which is antithetical to an efficient global information platform. We see in Europe deep distrust of US technology companies, over where information should be stored, who should own it, and how it should be taxed. European efforts to use tax and state aid authorities reflect this pressure. Harmonized standards reduce these risks as well.

The long-term environment will be more conducive to emerging technologies if rules are clear and stable, and industry embraces the goal of getting it right rather than avoiding oversight, which is not a sustainable objective. And even if it was, the industry would become more vulnerable to criticism when anything goes wrong – whether preventable or not.

In the US, we faced many of these issues over the last few years-- from the emergence of virtual currencies to the expanded use of prepaid cards that are a form of both payment processing and storing wealth. We tried hard to work through approaches that would permit new technologies to flourish, while applying appropriate levels of oversight of traditional concerns.

In the case of virtual currencies, I was always skeptical about storing wealth in virtual currencies with highly volatile valuations, but the paramount public policy concern was how to make sure a cash like and anonymous medium of commerce did not expand the space for illicit finance. We tried to strike a balance that permitted experimentation and oversight, and whether one is a fan of one cybercurrency or another, there is no denying that the underlying blockchain technology, now used by major financial institutions, is an innovation that will have a lasting impact on the efficiency and integrity of our financial system. And it is important that space for innovation continues to remain open.

Let me close with a final thought: good corporate governance is key to building and maintaining confidence in new financial systems and processes. It is hard to earn confidence and easy to lose it. Both the financial crisis and the fact that financial institutions took irresponsibly large risks and needed taxpayer assistance to end the crisis have left us in an environment where the challenge of building and keeping trust is even greater.

Whether marketing practices at a firm like Wells Fargo, or the management of a cyber-attack at a firm like Equifax, it is critical to avoid even the appearance that financial businesses engage in practices that mislead consumers or withhold critical information to promote a stronger bottom line or personal profit. I will leave to regulators and prosecutors to determine when and where enforcement actions are warranted. But it is clear to me that the future climate for broad acceptance of technological advances will be stronger, both in the US and internationally, if industry self-governance embraces the highest standards, and treats violations of those standards as unacceptable, and if there is a cooperative approach to framing new regulatory approaches to address new business models.

As we reach the ten-year anniversary of the financial crisis of 2007-2008, it naturally slips farther back in our memories. But we know that there will be financial crises in the future, even if we do not know when or what the cause will be. Our challenge is to prepare as best as we can to avoid foreseeable crises, and to rebound quickly if and when a crisis occurs. At the same time, we need to encourage an environment where innovation and investment flourish.

To me, this means that we should maintain reforms that have improved financial stability and confidence in our financial system. And for emerging technologies, we should aspire to clarity and stability about the rules of the

road going forward. Highly political battles that suggest dramatic changes are likely each time the political pendulum swings one way or the other do not help. There are legitimate concerns that financial institutions – new and old -- need to know the lay of the land to comply and concentrate on doing their business, and that constantly changing ground rules increase compliance burdens. The answer is not to lower our guard to real risks, but to navigate and stick to a sensible and balanced approach.

Thank you and I look forward to the discussion and questions in the remaining time we have together.