

**Embargoed Until Delivery
Monday, February 24, 2014**

Remarks of Debbie Matz
Chairman
National Credit Union Administration
at the
Credit Union National Association's
2014 Governmental Affairs Conference

Washington, D.C.

Remarks

Thank you, Paul. It seems like I was just here at the GAC. It's hard to believe another year has come and gone so quickly.

Looking back, 2013 was a very good year for credit unions. It ended on a high note when I got a call from our general counsel with wonderful news. I know that sounds like an oxymoron; wonderful news from an attorney. How often does that happen?

He shared the news that NCUA would receive \$1.4 billion. This was NCUA's share of the JPMorgan Chase settlement with the Department of Justice. And since the net settlement proceeds were deposited in the Corporate Stabilization Fund, the NCUA Board decided that credit unions will not pay a corporate assessment in 2014—for the first time since 2008.

After we secured our fourth settlement, raising our total recoveries to \$1.75 billion, the *Wall Street Journal* called NCUA “the John Wayne of Washington financial regulators.”

The *Journal* reported that NCUA has been “unusually tough” on Wall Street firms that sold faulty mortgage-backed securities to credit unions. And I reaffirm to you today: We remain “unusually tough” in holding accountable those parties responsible for selling faulty investments to corporate credit unions. And we're not done yet.

We are still seeking recoveries in 15 separate lawsuits. Any further recoveries will reduce future assessments to credit unions. And if we ultimately recover enough money to outpace losses from the corporates' legacy assets, then by 2021—when the Corporate Stabilization Fund expires—NCUA may even be able to provide a rebate. Even better than a good news call from an attorney, would be a good news call from a regulator. And I hope NCUA will be able to make that call.

Now lately, I've been doing a lot of thinking about the role of the regulator. I think I've figured out a different way to describe it: While optimists see the glass as half full and pessimists see the glass as half empty, regulators instead worry the glass could shatter and cut someone's hand. That explains why NCUA is constantly on the lookout for threats to the safety and soundness of the credit union industry.

During my first few years as Chairman, it was hard to take the long view—because it felt like my role was triage. As we moved from crisis to crisis, I had to ask tough questions that often required painful answers. Questions like:

- Which credit unions are in critical condition?
- How can we save them?
- Which ones need to be conserved?

But this past year, safety and soundness metrics remained strong, and trends are moving in the right direction. Net worth and loans are growing. Delinquencies and charge-offs are stable. Membership is at an all-time high. But there are still risks on the horizon and beyond.

So today, let's recognize together the progress that has brought us to where we are. Then let's discuss how we can build on that progress together and prepare for what tomorrow may bring.

This past year, the credit union industry turned a corner. Certainly, that has a lot to do with the economy, with the housing market and, dare I say, even with NCUA oversight, especially over troubled credit unions.

It also has a lot to do with your commitment to your members. This includes high-tech innovations, like smartphone apps and mobile deposit features that you're making to keep existing members satisfied and to attract new, younger members. You continue to adapt and transform yourselves for the 21st century.

I'm proud that as you transform to better serve your members, NCUA also continues to transform to better regulate credit unions. We've modernized regulations, and removed burdens wherever we can, without compromising safety and soundness.

In fact, we've exempted more than 4,000 small credit unions from certain regulations like interest rate risk, emergency liquidity, and risk-based capital. We've helped more than 2,000 credit unions expand services to nearly 20 million low-income members. We've streamlined our exam reports and modified documents of resolution to focus only on material issues that can threaten a credit union. That's just to name a few.

Often the regulations we've modernized came to our attention from you—credit union officials.

Keep the suggestions coming; we're always listening.

We've also restructured the agency to be more efficient. And we've strengthened our workforce. We've brought on employees with specialized backgrounds to improve the exam process. This also creates new opportunities for you to use a wider array of financial products.

We've come a long way in a few years. But we can, and must, do more to make sure credit unions remain strong and resilient into the future. To that end, I want to talk about two areas that deserve increased attention, from you and from us, in the days ahead.

First, is the impact of volatile and rising interest rates. With the unemployment rate falling, and the economy gaining momentum, a changing interest rate environment is not only on the way, it is already underway.

Credit unions can't afford to ignore this because ignoring rising rates is like pitching a tent on a beach at low tide. You don't want to pitch your portfolio's tent in a low-rate environment when rates are near historic lows and market experts are asking:

- How much will interest rates rise?
- And how quickly?

The uptick in rates during the second and third quarters of last year caused unrealized gains to become unrealized losses for thousands of you. This swing from unrealized gains to unrealized losses marks a dangerous warning of things to come. For now, these unrealized losses exist only on your books. But paper losses can turn into real losses. That happened during the savings and loan crisis.

I understand chasing yields seems appealing while long-term rates are rising and short-term rates remain low. It's easy to fall into a trap of chasing near-term profits by concentrating your portfolio in long-term investments. However, I can tell you, falling into this trap will imperil your credit union. Diving into long-term, fixed-rate investments will leave you vulnerable when short-term rates start to rise.

The bottom line is, carrying these long-term assets while paying out more to depositors can stress your earnings. So you need to be really careful not to make dramatic changes to your investment portfolio if those changes will impair your ability to deal with rising rates. Instead, be aware that conditions are changing. The tide is shifting. So plan to move your tent before the tide rolls in. And make sure your credit union is in a safe position.

The second serious risk on the horizon involves information security. To demonstrate just how much is at stake for your credit union, and how vulnerable the entire financial services industry may be to cyber-attacks, I am going to share three recent examples:

The first example is one we all know too well. Just a few months ago, cyber-thieves stole the names, addresses, and phone numbers of 110 million people who shopped at Target. That's more than the combined populations of California, Texas, and my home state of New York.

The data breach at Target is the story of a double standard. While financial institutions are required by law to protect sensitive personal information, data protection standards for retailers are too often simply not adequate. That is neither healthy nor fair.

You may recall the data breach began when hackers cracked the network of one of Target's third-party vendors. This serves as a reminder that a data breach—even if it's outside the financial system—can have enormous negative repercussions inside the financial system.

No matter how far removed a given data breach is from your credit union, if it affects your members, you can pay dearly—both in terms of your reputation and your balance sheet. After all, it is you, not the retailer, who is responsible for monitoring accounts more closely and reissuing plastic cards to your affected members. It is you who must shell out as much as \$15 for every new card. And it is you who must reassure members that their accounts are still safe.

Of course, cyber-thieves have seen Target's well-known "bulls-eye" logo as an invitation. But they've also targeted credit unions.

Which brings me to the second example: Hackers broke into a medium-size credit union and used the credit union's passwords to access one of the larger credit bureaus. From there, the hackers stole credit reports on hundreds of people who weren't even credit union members.

The lesson learned is that cyber-thieves can hack into your credit union as an entry point to access data and systems that have nothing to do with your credit union.

Now, I know some of you are thinking: My credit union has never been attacked. My IT staff has this covered. So why should I be concerned? Because there is another threat that is more dangerous than what most of you have seen and dealt with before.

The third example reveals a much different type of attacker—cyber-terrorists—who are now targeting credit unions. When these attackers break through, websites crash. Members are unable to access their accounts. It can take hours to bring systems back online.

After the dust settles, foreign extremists claim responsibility and deliver their anti-American messages. These “denial of service” attacks are part of an alarming and growing pattern of cyber-terrorism against our country, designed to get our attention and shut us down.

But there’s an even worse scenario. Imagine that the hackers in the first two examples had been motivated by terrorism, not money. What if cyber-terrorists—not cyber-thieves—managed to infiltrate systems and compromise or destroy data? Imagine cyber-terrorists stealing passwords from your credit union and using your credit union as an entry point to gain access to every payment system and every vendor with which you have a digital relationship. Think about the damage they could do.

Then imagine that the hackers in the third example had done more than temporarily interrupt service. What if the cyber-terrorists had done this merely as a diversion? We have already seen cases where denial of service attacks were launched to distract IT staff. Hackers simply wait until security teams are focused on the attack at the front door and then they break in through a back window.

Attacks like this have already hit financial institutions. And they happen fast.

A global security company reported a case where, after hackers stole account information and created counterfeit debit cards, thieves were able to withdraw \$9 million from ATMs of a single European bank across 46 cities in just two hours. It took a large, sophisticated criminal network to coordinate such a devastating, focused attack. But ask yourself: What if those attackers had instead been motivated by terrorism? Then think about the damage they could have done.

Cyber-terrorism is a new kind of scenario, one that requires all of us to stay constantly vigilant. Because the worst-case scenario doesn't just deny services, it destroys security and dismantles systems. After all, what makes cyber-terrorists different from cyber-thieves is their objective. Terrorists want to cripple or destroy critical infrastructure here in the United States. They want to use your credit union to break into larger financial institutions, with the goal of bringing down the entire financial system.

These attacks are like poison-tipped darts. Where they hit doesn't matter. Once that poison is in the bloodstream, it moves quickly through the system. As these examples illustrate, these darts could hit your credit union. So it's up to you to keep your systems secure every day.

If you saw NCUA's first Supervisory Letter for 2014, you know our top priority alongside interest rate risk is cyber-security. Examiners will be looking to see how credit unions are implementing appropriate risk mitigation controls to better protect, detect, and recover from cyber-attacks. This includes vendor due diligence, strong password policies, proper patch management, employee training, and network monitoring.

So I strongly encourage you to make sure your IT staff and vendors are on top of emerging cyber-threats. The bottom line is: You need experts you can count on to answer the very tough question: Is my credit union really protected?

So what can you do? Get educated. Not just you, but your employees and your colleagues as well. Share cyber-security best practices with each other at your league meetings, chapter meetings, and professional groups. Participate in national information-sharing forums.

These are great resources to learn about cyber-threats and hacker tactics against financial institutions. Links to some of these forums are now posted on our [website](#). I hope that by working together and with CUNA's Technology Council, you will have access to the best information available from these vigilant organizations.

This is not just a priority for NCUA. Congress is holding hearings and considering legislation on cyber-security. And President Obama has made strengthening our nation's cyber-security framework a national priority.

To achieve the president's goal of combatting cyber-attacks, the National Institute of Standards and Technology (NIST) recently developed a voluntary national cyber-security framework for private enterprises including credit unions. I encourage you and your staff to review the NIST framework, and to evaluate how these new standards could further protect your credit union, and your members.

You may be surprised to know, you are not the only ones who get examined on important information-security measures. Like other government agencies, NCUA must adhere to stringent security standards.

Every year, NCUA's Inspector General oversees an audit of our information technology controls and security procedures. NCUA has security measures in place to protect your members' information. To log in, examiners use secure government smart cards, and both their hard drives and thumb drives are encrypted. In addition, to make sure that personal information will not be exposed, it is always deleted before exams are uploaded to our system.

We are also partnering with other agencies to further strengthen cyber-security. NCUA partners directly with the law enforcement and intelligence communities, as well as other federal financial services regulators, as part of a new working group. Over the next several months, the working group will focus on better understanding the cyber-threats and vulnerabilities facing financial institutions.

We are working with industry experts to review any necessary changes to our supervisory processes in the wake of increasingly sophisticated cyber-attacks. We are exploring ways to improve information sharing to help us all be better prepared. In the coming months, our working group plans to hold an industry webinar, both to help you better understand current cyber-threats, and to share new ways to work together. NCUA will also be issuing guidance to credit unions based on findings and recommendations of the working group.

Taking practical steps to address cyber-security concerns is not only about protecting your credit union and protecting your members. It's also about protecting the entire financial system.

It's like the old story about two men in a canoe: One looks at the other and says, "Hey, you have a problem. There's a leak on your side of the boat."

When it comes to taking security measures to protect the industry, we are all in this together. So NCUA needs to be ready. The credit union system needs to be ready. Working together, we will be ready.

Keeping a house in order requires constant maintenance. Yes, the worst of the storm is behind us. The sun is starting to peek out from the clouds. So now is the time to fix the roof.

One year ago, I made a promise to you: "NCUA will not hold credit unions back." I said that our success will be measured by your success. No matter what the New Year brings, no matter what challenges we face, our future depends on open communication.

At NCUA, we build on our progress by continuing to listen to you, communicate with you, and change as quickly as the landscape is changing. By preparing together for risks on the horizon, we can secure a brighter future beyond the horizon.

I'm grateful for your work this past year. I look forward to an even more successful 2014, and beyond. Thank you.

