



Headline News

Senate conferees accept House option on interchange

The Credit Union National Association (CUNA) on Tuesday repeated its call for credit unions to oppose Congress's final financial regulatory reform bill, as the House Senate lawmakers voted to accept a House proposal that retained portions of that bill that would modify current interchange practices.

Following the late afternoon decision by the Senators, CUNA Senior Vice President of Legislative Affairs said that CUNA "opposes the big bill with interchange in it, not the concept of financial regulatory reform."

The agreed-to version of interchange legislation would allow the federal government to impose controls on the fees paid to use electronic payment networks. While the proposal does currently exempt financial institutions with under \$10 billion in assets from the terms of the legislation, CUNA and others have said that that carve out is unlikely to matter, as smaller issuers will likely be pushed aside by favorable deals between merchants and big issuers.

CUNA has repeatedly stated that, among other things, altering the current interchange rules would result in an artificially low debit interchange rate that would force small issuers to recoup losses through other means. The interchange provisions as written would hurt consumers by driving up debit card fees, with no compensatory advantages to consumers, CUNA has said.

CUNA and various state credit union leagues continued to make their case to legislators during Hill visits on Tuesday, and hundreds of credit union representatives, along with over 650,000 credit union backers, have contacted their legislators to voice their opposition to the interchange fee changes in recent weeks.

Legislators are aiming to wrap up the financial regulatory reform conference committee by the end of this week. House Financial Services Chairman Barney Frank (D-Mass.) and Senate Banking Committee Chairman Chris Dodd (D-Conn.) on Tuesday disclosed that the committee will discuss prudential regulation on Wednesday, with limited debate on derivatives set to take place on Thursday. Legislative offers, counter-offers, as well as votes, will take place on those days as well.

The committee this week agreed to legislation addressing thrifts, deposit insurance reforms, hedge funds, credit rating agencies, executive compensation, and investor protections, among other items.
(source: CUNA's NewsNow 6/23/2010)

First quarter 2010 Louisiana rate comparison available on LCUL website

The Louisiana Credit Union League is pleased to provide member credit unions with quarterly rate comparisons. These reports are compiled from Louisiana credit union data reported to NCUA, as provided by cudata.com and prepared by the Louisiana Credit Union League's Research & Compliance Department. The quarterly comparison for March 2010 was recently posted to the website. Should you have any questions, please contact Jennifer Green at jgreen@lcul.com.

ATM & debit card safety tips for members

Keeping your personal identification number (PIN) a secret is among safety tips released by PULSE, an ATM/debit network. Credit unions can pass the tips on to members.

June is ATM & Debit Card Safety Awareness Month, which is why PULSE released the tips.

The recession has prompted consumers to use their debit cards more than other forms of payment, but with the increased use comes an increased risk of fraud, according to Jim Cichy, PULSE vice president of fraud management.

"To keep money safe and secure, consumers need to better understand how to work with their financial institution to combat security compromises and fraudulent use of financial information," he said.

Along with keeping PIN numbers a secret, PULSE noted that consumers should memorize their PINs and never write it on a card or store the number with the card. Also, never let someone else enter a PIN number.

"No company or individual should ever ask for your PIN," PULSE said.

PULSE also suggested that consumers:

- Never provide a debit or credit card number or any personal information through an unsolicited e-mail or request;
- Look for secure transaction symbols when shopping online to ensure the account information is protected;
- Call the financial institution if a card is lost or stolen;
- Review all account statements promptly and report any errors;
- Do not expose a card's magnetic stripe to magnetic objects because they can damage cards;
- Block the view of others when using an ATM or PIN debit terminal;
- Observe surroundings before using an outdoor ATM or debit terminal;
- Do not use ATMs that appear to be tampered with and report tampering to the ATM owner immediately.

CUNA releases FTC, Fed final rule analyses

The Credit Union National Association (CUNA) addressed the Federal Trade Commission's (FTC) final rule that requires disclosures for financial institutions that do not have federal deposit or share insurance in a recently published final rule analysis.

The FTC's final rule, which will become effective on July 6, requires institutions to inform their members or customers that the institution is not federally backed and that the federal government does not guarantee the depositor will receive money if the institution fails.

While a proposal released in 2005 would have required financial institutions to provide this notice to each member or customer in writing, financial institutions may now comply with the rule by posting a disclosure of their insurance situation, in some instances.

Those publicly placed disclosures must be visible at each station or window place where deposits are received, at each principal place of business, in all branches where the institution accepts deposits or opens accounts. The disclosures must also be visible on the financial institutions home page.

The final rule does not apply to financial institutions that do not receive deposits in amounts less than the maximum insurance level of \$250,000.

CUNA also addressed recent Federal Reserve Board clarifications to Regulation E, the Electronic Fund Transfer Act, and Regulation DD, the Truth in Savings Act (TISA) in a separate final rule analysis.

One item noted by the Fed changes, which were released late last month, was a clarification that institutions may not assess fees for the payment of ATM and one-time debit card overdrafts if consumers do not opt-in to their overdraft programs. The Fed at that time also clarified that Reg DD does not require financial institutions "to exclude from the consumer's balance funds that may be transferred from another account" under retail sweep programs.

(source: CUNA's NewsNow 6/22/2010)

NCUA assess 13-bp charge to repay corporate CU coverage

NCUA assesses 13-bp charge to repay corporate CU coverage

Credit unions will soon be charged an assessment of 0.134% of insured shares as the National Credit Union Administration (NCUA) collects a portion of the funds necessary to pay for the costs of the corporate stabilization.

Invoices for the assessment will go to credit unions in July with the assessment due in August.

In accordance with the stabilization fund established by Congress last year, the agency may collect the funds necessary to cover the costs of corporate stabilization over a period of as long as seven years. The NCUA assessment of the likely amount of those costs is in the neighborhood of \$6 billion, but the actual amount of the losses will not be known for some time, Credit Union National Association (CUNA) Chief Economist Bill Hampel said.

This year's assessment will provide \$1 billion toward the eventual losses, he added.

Credit unions should expense their assessment in June and report the expense on their June 2010 call reports, according to NCUA.

CUNA President/CEO Dan Mica said that while the NCUA's assessment is close to CUNA's prior predictions, it "is still a burden on the nation's credit unions coping with a recovering economy.

"Given that, and looking forward, we are hopeful that the agency will take the necessary actions to keep future assessments to cover corporate credit unions costs and for the National Credit Union Share Insurance Fund (NCUSIF) at the lowest level possible," Mica added.

NCUA Chairman Debbie Matz said that the agency would discuss a separate assessment to replenish the NCUSIF later this year.

Hampel predicted that the pending NCUSIF assessment would be somewhere between 5 and 10 basis points (bp), bringing the total amount assessed by the NCUA this year to between 18 and 23 bp. In its monthly report on the status of the NCUSIF, which was delivered later in the NCUA's monthly board meeting, the NCUA staff noted that the fund's equity ratio was at 1.22% as of the end of May 2010, adding that the fund increased its reserves for both specific and non-specific natural-person credit union (NPCU) losses by \$132 million, bringing the total amount of its reserves to \$1.1 billion.

The NCUA's \$1.1 billion "provision" for natural person credit union insurance losses "is not this year's expense," but is "what the NCUSIF has expensed over the past couple of years in anticipation of future losses," Hampel added.

"The language NCUSIF uses can be confusing compared to credit union terminology. The 'Provision for CU Losses' is analogous to a credit union's allowance for loan losses, and the NCUSIF's 'Insurance Loss Expense' is similar to a credit union's loan loss provision," Hampel said.

Overall, insurance loss expenses are "running at budget" this year, and "expenses for the rest of the year will likely depend primarily on changes in the number and size of troubled credit unions," Hampel added. *(source: CUNA's NewsNow 6/18/2010)*

You're invited to learn about the Sprint CU Member Discount program during free webinar

Would you like to learn more about Sprint's member discount program? Are you interested in hearing more about how your Credit Union can participate for FREE and receive an annual marketing incentive? Are you already participating and need a refresher?

Join our next FREE Webinar- NO reservation required! We will use this time to review how the program works and then follow up with a question and answer period.

Upcoming 2010 & 2011 Webinar dates @ 3:00 PM (central)

2010

Tuesday, Aug 10
Tuesday, Sept 14
Tuesday, Oct 12
Tuesday, Nov 9
Tuesday, Dec 14

2011

Tuesday, Jan 11
Tuesday, Feb 8
Tuesday, Mar 8

Tuesday, Apr 12
Tuesday, May 10
Tuesday, June 14
Tuesday, July 12
Tuesday, Aug 9
Tuesday, Sept 13

To join in, simply pick the date of your choice from the schedule above then follow the directions below to log in. It's FREE and it only takes about 15 minutes. We'd love for you to join us.

Meeting Link:

https://cuv.on.intercall.com/confmgr/public_unsched.jsp?confId=6072607

When prompted, select Light Version Installation
Meeting Phone #: 888.742.8686
Conference Code: 6072607

Moderator: Rhonda Peruski, Email rhonda.peruski@cucorp.com

If you have problems accessing either the phone or Web portion of the conference, please contact InterCall Tech Support at 877.549.2051. Be sure to let the Tech Support Representative know that you are attempting to connect to an InterCall Web Meeting.



Scam Alert

Latest phone scam targets your bank account

Imagine getting hundreds or thousands of calls on your home, business, or cell phone, tying up the lines. And when you answer, you hear anything from dead air to recorded messages, advertisements, or even phone sex menus.

It's annoying, no doubt. But it could be more than that-it could be a sign that you're being victimized by the latest scam making the rounds. This "telephone denial-of-service attack" could be the precursor to a crime targeting your bank accounts.

Denial-of-service attacks, by themselves, are nothing new-computer hackers use them to take down websites by flooding them with large amounts of traffic.

In a recent twist, criminals have transferred this activity to telephones, using automated dialing programs and multiple accounts to overwhelm the phone lines of unsuspecting citizens.

Why are they doing it? Turns out the calls are simply a diversionary tactic: while the lines are tied up, the criminals-masquerading as the victims themselves-are raiding the victims' bank accounts and online trading or other money management accounts.

Here, in a nutshell, is how the whole thing works:

- Weeks or months before the phone calls start, a criminal uses social engineering tactics or malware to elicit personal information from a victim that this person's bank or financial institution would have-like account numbers and passwords. Perhaps the victim responded to a bogus e-mail phishing for information, inadvertently gave out sensitive information during a phone call, or put too much personal information on social networking sites that are trolled by criminals.
- Using technology, the criminal ties up the victim's various phone lines.
- Then, the criminal either contacts the financial institution pretending to be the victim...or pilfers the victim's online bank accounts using fraudulent transactions. Normally, the institution calls to verify the transactions, but of course they can't get through to the victim over the phone.
- If the transactions aren't made, the criminals sometimes re-contact the financial institution as the victim and ask for it to be done. Or they add their own phone number to victims' accounts and just wait for the bank to call.

By the time the victim or the financial institution realizes what happens, it's too late.

The FBI first learned about this emerging scheme through one of its private industry partners, which told us how a Florida dentist lost \$400,000 from his retirement account after a denial-of-service attack on his phones.

And as of April of this year, there has definitely been a noticeable surge in telephone denial-of-service attacks, with numerous incidents having been reported in several Eastern states.

To help fight these schemes, the FBI has teamed up with the Communication Fraud Control Association- comprised of security professionals from communication providers-to analyze the patterns and trends of telephone denial-of-service attacks, educate the public, and identify the perpetrators and bring them to justice.

Ultimately, though, it's individual consumers and small- and medium-sized businesses on the front line of this battle. So take precautions: never give out personal information to an unsolicited phone caller or via e-mail; change online banking and automated telephone system passwords frequently; check your account balances often; and protect your computers with the latest virus protection and security software.

And if you think you may have been targeted by a telephone denial-of-service attack, contact your financial institution and your telephone provider, and file a complaint with the FBI's Internet Crime Complaint Center. *(source: www.fbi.gov)*

League News

CUNA announces LCUL winner in blockbuster, pro awards

State leagues and associations were honored for excellence in public relations, marketing and advertising during the American Association of Credit Union Leagues' (AACUL) 2010 Communicators/GAPS Conference, held this week in Washington, D.C.

LCUL won first place in two categories: 'Best Print Materials' for our 2009 Annual Convention Brochure and 'Best Website' (www.lcul.com). LCUL also received honorable mention in the 'Blow Your Own Horn' category for our 2010 Credit Union Planning Calendar.

Credit Union National Association's CUNA Blockbuster awards recognize two segments: advertising and marketing efforts for state level organizations, and advertising and marketing for credit unions. CUNA Pro awards recognize the best public relations, publications and online communication efforts.

In The News

Ronaldo Hardy wins vote to become regional finalist for the CUES Next Top CU Exec search

Ronaldo Hardy, Branch Coordinator with La Capitol Federal Credit Union, has been voted one of six Regional Finalists for the Credit Union Executives Society's Next Top Credit Union Exec challenge.

Next Top Credit Union Exec applicants needed to be age 35 or under, employed by a credit union, and had to create a 60-second video outlining the details of their credit union project. The online public voted for

their favorite in each of six geographical regions. Ronaldo Hardy, 26, submitted details of the credit union's Gen Y Task Force project and received more votes than the other five entrants in the Southeast Region.

Hardy wins a \$5,000 prize package, including registration, accommodation and airfare to CUES' CEO/Executive Team Network™ in Dallas, November 7-10, 2010. While in Dallas, Hardy will compete against the other five Regional Finalists who will face off for the grand prize - a CUES educational package valued at \$20,000 and the honor of being named the Next Top Credit Union Exec.

Over the next few months, Hardy and the other five Finalists will provide updates on their projects' progress at the website www.NextTopCreditUnionExec.com.

Educational Opportunities

Upcoming teleconference to discuss financial ratios you should know

Members are the most important element of every credit union though their relationships never appear on financial statements. Understanding just a few financial relationship ratios will tell you more about your credit union's strengths, weaknesses, and options to enhance them.

This session will cover:

- Review of Balance Sheet & Income Statement Structure
Capital: Supports Risks, Capital Ratio, also called Net Worth Ratio, Loan Delinquency & Loan Charge offs belong together
- Earnings: Where Capital Comes From Spread Analysis- Relationship between Asset Size and Income Statement, How Much Income is Needed to Support Your Growth
- Your Members - The Roots of Your CU: Member Usage of CU Services, Average Account Size Determines Your CUs Options

Join Carolyn Warden as she gives her expertise of operation analysis, training and coaching experience from all sides of the desk.

This program will take place on Wednesday, June 30, 2010, from 10:00 to 11:00 AM. The cost of this 1-hour teleconference is only \$129 and as a value-added feature for this session, we will be audio archiving it for 30 days following the seminar. You may access the archive by clicking on the following link beginning 48 hours after the session and using the same PIN you used to access the live call.