Activity Review

North Carolina State Board of Certified Public Accountant Examiners

1101 Oberlin Road, Suite 104 • PO Box 12827 • Raleigh, NC 27605 • 919-733-4222 • No. 7-2008

Failure to Renew By Deadline May Result in Forfeiture

21 NCAC 08J .0101, *Annual Renewal of Certificate, Forfeiture, and Reapplication*, requires that all active CPAs renew their certificates annually by the first day of July.

NOTE: *Online license renewal will remain available through the end of July.*

If a CPA fails to renew his or her certificate by July 1, the Board will send a Letter of Demand to the CPA at the most recent mailing address the Board has on file.

Failure of an individual to submit the completed renewal within 30 days of the mailing of the Letter of Demand automatically results in forfeiture of the CPA's certificate, as required by NCGS 93-12(15).

Upon forfeiture of a certificate, the individual is no longer a CPA--he or she cannot use the CPA title in any way--and he or she must return his or her CPA certificate to the Board within 15 days of the notice of forfeiture.

A person who has forfeited his or her certificate pursuant to NCGS 93 12-(15) for failure to renew, may be eligible to apply for reissuance.

If you have questions about the certificate renewal process, please contact Buck Winslow by e-mail at **buckw@nccpaboard.gov**.

Should You Register Your Firm With the Board?

Although many North Carolina CPAs consider business, industry, government, or education as their primary employment, a significant number of these individuals also provide or offer to provide accounting services to the public.

A CPA who uses the CPA title in or with his or her business name or who offers to provide or provides attest or audit services, must register with the Board as a CPA firm pursuant to 21 NCAC 08J .0108 and 21 NCAC 08N .0302.

An individual may register with the Board as an individual practitioner, partnership, professional corporation, professional limited liability company, or registered limited liability partnership.

The Board considers attest services or assurance services to be

- any audit or engagement to be performed in accordance with the Statements on Auditing Standards, Statements on Generally Accepted Governmental Auditing Standards, and Public Company Accounting Oversight Board Auditing Standards;
- any review or engagement to be performed in accordance with the Statements on Standards for Accounting and Review Services;
- any compilation or engagement to be performed in accordance with the Statements on Standards for Accounting and Review Services; or
- any agreed-upon procedure or engagement to be performed in accordance with the Statements on Standards for Attestation Engagements.

Please note that a CPA or CPA firm that provides any audit services, reviews of financial statements, compilations of financial statements, or agreed-upon procedures must enroll in a peer review program pursuant to 21 NCAC 8M.

CPA firm registration information and firm registration forms are available from the Board's web site, **www.nccpaboard.gov**.

If you have questions regarding the registration of your CPA firm, please contact Cammie Emery by e-mail at **cemery@nccpaboard.gov**.

www.nccpaboard.gov

In This Issue...

Focus On: Uniform CPA Examination

What Is A Concentration in Accounting?

Important Information for Applicants and Educators

Over the past few months, the Board has received numerous phone calls, letters, and e-mails from Uniform CPA Exam applicants and educators who have questions regarding the education requirements for Exam applicants.

Pursuant to 21 NCAC 08F .0302, *Education and Work Experience Required Prior to CPA Exam,* applicants for the Exam must possess a bachelor's degree in any subject, from a regionally accredited college or university, that either includes or is supplemented by a concentration in accounting as defined in 21 NCAC 08A .0309**.**

21 NCAC 08A .0309 states, in part, that a concentration in accounting must include at least 30 semester hours, or the equivalent in quarter hours, of undergraduate accountancy courses which shall include no more than six (6) semester hours of accounting principles and no more than three (3) semester hours of business law.

One of the most frequently asked questions refers to the stipulation that no more than six (6) semester hours of accounting principle coursework may be counted toward the 30 semester hour requirement.

Few colleges and universities still call introductory accounting courses "Accounting Principles I and II;" such courses are now named "Introduction to Financial Accounting," "Introduction to Managerial Accounting," or similar names. Regardless of the course titles, these courses are, in fact, introductory level accounting courses.

As such, even if the college or university considers these courses to be four (4) semester hours each, these introductory accounting courses may be claimed as no more than six (6) hours of the 30 semester hour requirement.

A similar question concerns "pre-accounting" courses offered by some schools. These courses are generally one (1) or two (2) semester hours and serve as introductory courses to the accounting program and are completed before courses such as "Accounting Principles I and II," "Financial Accounting," or "Managerial Accounting," etc.

Again, these courses are at the introductory or principle level and can only be counted toward the six (6) semester hours of accounting principles portion of the 30 semester hour requirement—any additional hours of principle-level coursework cannot be used to meet the concentration in accounting requirement.

Unfortunately, a number of Exam applications have been denied because the individuals incorrectly included more than six (6) semester hours of accounting principles when calculating their compliance with the 30 semester hour requirement.

These applicants must take additional courses to fulfill the concentration in accounting requirement to become eligible to sit for the Exam.

Duplicate coursework is also a problem for many Exam applicants. For example, some colleges and universities offer a single tax course that covers both individual and business tax return preparation. A student completes that course, but chooses to take a business tax tax return preparation course at another school.

Because the coursework is duplicative (the business-only tax preparation course supersedes the combined individual/business tax preparation course), only one of the courses may be counted toward the 30 semester hour requirement.

Applicants who include the credit hours for both courses may be ineligible to sit for the Exam because they, in fact, do not have a concentration in accounting.

Applicants must consider the content of courses, not just the course names, when calculating compliance with 21 NCAC 08A .0309 and 21 NCAC 08F .0302.

While finance, management, marketing, computer, economics and writing classes may be essential components of a school's degree program, such classes are not acceptable for the concentration in accounting.

In addition, accounting internships and Exam preparation courses, while highly beneficial to the student, are not eligible for credit toward the 30 semester hour requirement.

Exam applicants and educators are encouraged to review the Board's rules regarding the education requirement for the Uniform CPA Exam.

If you have questions regarding the concentration in accounting or other Exam requirements, please contact the Board's Deputy Director, J. Michael Barham, CPA, by e-mail at **mbarham@nccpaboard.gov**, or contact the Board's Executive Director, Robert N. Brooks, by e-mail at **rbrooks@nccpaboard.gov**.

2008 Board Meetings

August 18

September 22

October 20

November 17

December 17

Meetings of the Board are open to the public except when under State law some portions may be closed to the public.

Meetings are held at the Board office at 1101 Oberlin Road, Raleigh, and begin at 10:00 a.m.

Are You Using the Firm Name As Registered With the Board?

21 NCAC 08N .0306(c), *Advertising or Other Forms of Solicitation*, states that a "CPA firm shall offer to perform or advertise professional services only in the exact name of the CPA firm as registered with the Board."

This rule applies to stationery, envelopes, reports, business cards, brochures, banners, office signs, telephone directories, newspaper or magazine ads, web sites, engagement letters, and business proposals, as well as any other form of advertisement or solicitation.

For example, if your firm is registered with the Board as "James Joseph Blue, CPA," you must always use "James Joseph Blue, CPA, "as the firm name—you may not omit or abbreviate any portion of the firm name.

For example, by referring to the firm as "JJ Blue, CPA," or "Joey Blue, CPA," you are in violation of 21 NCAC 08N .0306(c).

If your firm is registered with the Board as "Able, Baker, Charlie, Dog, and Easy Company," the firm must always use the firm's full name--the firm cannot be referred to as "ABCDE Company" or "Able Baker Company"

Suffixes such as "Professional Association," "PA," "P.A.," "Professional Corporation," "P.C.," "PC," "Limited Liability Partnership," "LLP," "L.L.P.," "Professional Limited Liability Company," "P.L.L.C.," "PLLC," "Company," "Co.," etc., which are part of the firm name as registered with the Board must be used each time the firm name is used.

For example, if your firm is registered as "Arm & Legg, LLP," the firm must always be referred to as "Arm & Legg, LLP." It is not acceptable to refer to the firm as "Arm & Legg, " or "Arm."

In addition, if your registered firm name includes "Certified Public Accountants," "CPA," or "CPAs," this language must be included each time your firm name is referenced.

NOTE: ***The plural form of CPA is CPAs, not CPA's.***

To modify your firm name as registered with the Board, you must request a name change from the Board.

To modify your firm name as registered with the Board and the Secretary of State's office, you must not only request a name change from the Board, but also complete *Articles of Amendment* or *Certificate of Amendment* from the Secretary of State's Office.

For additional information on firm names, please contact Buck Winslow by e-mail at **buckw@nccpaboard.gov**, or Cammie Emery by e-mail at **cemery@nccpaboard.gov**.

Exam Fees Effective August 1, 2008

Administrative Fees	
Initial Applicant	$230.00
Re-exam Applicant	$75.00
Exam Section Fees	
Auditing & Attestation (AUDIT)	$226.28
Financial Accounting & Reporting (FAR)	$214.35
Regulation (REG)	$190.50
Business Environments & Concepts (BEC)	$178.58

IRS Increases Mileage Rates

On June 23, 2008, the Internal Revenue Service announced an increase in the optional standard mileage rates for the final six months of 2008.

Taxpayers may use the optional standard rates to calculate the deductible costs of operating an automobile for business, charitable, medical or moving purposes.

The rate will increase to 58.5 cents a mile for all business miles driven from July 1, 2008, through December 31, 2008.

This is an increase of eight (8) cents from the 50.5 cent rate in effect for the first six months of 2008, as set forth in Rev. Proc. 2007-70.

In recognition of recent gasoline price increases, the IRS made this special adjustment for the final months of 2008.

The IRS normally updates the mileage rates once a year in the fall for the next calendar year.

"Rising gas prices are having a major impact on individual Americans. Given the increase in prices, the IRS is adjusting the standard mileage rates to better reflect the real cost of operating an automobile," said IRS Commissioner Doug Shulman. "We want the reimbursement rate to be fair to taxpayers."

While gasoline is a significant factor in the mileage figure, other items enter into the calculation of mileage rates, such as depreciation and insurance and other fixed and variable costs.

The optional business standard mileage rate is used to compute the deductible costs of operating an automobile for business use in lieu of tracking actual costs.

This rate is also used as a benchmark by the federal government and many businesses to reimburse their employees for mileage.

For additional information on mileage rates, please visit the Internal Revenue Service web site, **www.irs.gov**.

Your Laptop Computer: Physical Security, Data Protection and Tracking/Recovery

The theft of laptop computers and the sensitive data they contain is a growing problem for North Carolina CPAs—in one week, three CPAs contacted the Board regarding the theft of laptops from their firms.

There are three major aspects to laptop security—physical security, data protection, and tracking/recovery.

One of the first things to do after purchasing a laptop is to make a copy of the purchase receipt, serial number, and description of the laptop and keep that information in a location separate from the laptop. This information will be invaluable if the laptop is lost or stolen.

In addition, asset tag or engrave the laptop. Engraving your firm name and phone number or address may increase the likelihood of getting the laptop returned if it is stolen and recovered. Tamper-proof asset tags may serve as a deterrent to a thief who must choose between stealing an unmarked laptop or a marked laptop. Why? Asset tags are difficult to remove and may hamper the thief's ability to sell the laptop on the open market.

Industry experts estimate that one in eight laptops is at risk of theft. With such a daunting statistic, laptop users may feel resigned to being the victim of theft. However, one of the cheapest and most cost-effective solutions to deter the theft of a laptop is to attach a security cable (similar to the locks used on bicycles) to the laptop.

With cable locks, a steel clip provided by the manufacturer is installed in a security slot on the back or side of the laptop and a steel cable is threaded through the clip and wrapped around a heavy object such as a desk leg or support pole. The two ends of the cable are then secured with a locking device.

If the laptop does not contain a security slot or if the desk does not provide a location for suitable anchorage, special adhesive pads containing an anchorage slot are available. Although cable locks are not infallible, they will at least make the thief work a little harder to get the laptop.

Another effective method of protecting a laptop is to use a laptop safe. An advantage of a laptop safe is that when the laptop is locked in a safe, the PC cards and peripherals are secure, a protection that is not available with cable locks.

The two main types of safe available are portable safes that can safely attach to most work surfaces and car safes which are designed to protect valuables while they are stored in the trunk of a vehicle.

NOTE: Never leave a laptop in plain sight in a vehicle; doing so is inviting a thief to break in the vehicle and take the laptop.

Whereas cable locks and safes are designed to stop (or at least slow down) an opportunistic thief, alarms and motion detectors are intended to make the potential robber so conspicuous that he or she aborts the crime.

Products range from simple motion detectors to sensors that detect the unplugging of cables. Some products are designed to lock down the laptop if it is moved out of a designated range. Other products rely on nothing more than movement of the object to which it is attached; if the laptop to which the sensor is attached is moved, an alarm will sound.

Let's assume that, despite taking the appropriate physical security measures, your laptop has been stolen. How worried would you be about the security of the data on the machine?

Safeguarding data when it is in unauthorized hands is a matter of controlling access and encrypting data.

If the first thing a thief sees when turning on a laptop is, "please enter boot password," he or she knows that it will take some effort to access the information on the machine.

Many machines allow the owner to set a boot password; a user will be prompted three times to enter the correct password. If there are three password failures, the machine will refuse to boot. However, if the machine is restarted, the user will have three more chances to enter the right password.

Removing a password-protected BIOS (basic input output system) and boot sequence typically involves physically opening the computer and removing the CMOS (complementary metal oxide semiconductor) battery (which may clear the BIOS information) or shorting some jumpers to reset the BIOS to a default state.

If you are running an operating system that supports proper logins (such as Windows XP/Vista or Linux), setting a password is not only a good idea, it is required. To successfully login to the computer, the user must provide a login name and password. If the information entered is incorrect, the operating system will refuse to allow the user to become an active user.

When creating a password, make sure you create a strong password. For a password to be considered strong, it must be eight or more characters (14 characters or longer is ideal); it must combine letters, numbers, and symbols; it must use a mix of uppercase letters and lowercase letters; and it should use words and phrases that are easy for you to remember, but difficult for others to guess.

NOTE: Avoid using your login name, your name, your birthday, anniversary, social security number, telephone number, etc., as part of your password. Don't forget to change your passwords on a regular basis.

Although applying strong passwords to your laptop will make it more difficult for a casual thief to log in as "you," and therefore gain access to the information on your machine, passwords should not be relied upon as the sole piece of security on a laptop.

Even if an unauthorized user gains access to your laptop, encryption will

continued

protect the information stored on your machine. When you encrypt a file or folder, you are converting it to a format that can't be read by another user. When a file or folder is encrypted, an encryption key is added to the files or folder that you selected to encrypt and the key is needed to read the file.

Although Microsoft provides a form of encryption through Windows Encrypted File Service (EFS), that encryption is keyed to your user login. If the intruder is able to login as "you," he or she has access to your data even if it is encrypted with EFS.

Therefore, most firms who go this route will seek a third-party product which relies on encryption techniques above and beyond the Windows operating system.

CPAs using encryption technology need assurances that application databases such as tax, audit automation, and time and billing will operate correctly from encrypted disks or folders. The major software vendors test their products under a variety of scenarios and will be able to advise their customers of encryption solutions which are fully compatible with their products.

While encryption will protect the sensitive information on your laptop, it does nothing to retrieve the data on a lost or stolen machine. To do that, you must back up your files and store them in a secure location. Ideally, files should be backed up on a network server, but if that is not possible, there are other options.

External drives, flash drives, zip drives, and CDs are excellent choices for backing up your files. You can even use your digital music player to back up your data; these players don't just copy music files, they can copy any data. Players are easily hooked up to a laptop through the USB port and have up to 20-gigabyte hard drives.

While encryption strategies will help safeguard the data on a lost or stolen notebook computer, they do nothing to help recover the missing machine--the FBI estimates that just 3% of stolen or lost laptops are recovered.

Until recently, luck was the determining factor in recovering a lost or stolen machine, but new technology is providing users with the ability to track stolen or lost laptops.

With tracking programs, once a computer is reported lost or stolen, the tracking company will wait for the laptop to send a location signal (sent whenever the machine is connected to the Internet). When a signal is retrieved, the program will be instructed to broadcast as much information as it can about the current connection (originating phone number, IP address, service provider, etc.). When enough information has been collected, the tracking company will notify the appropriate law enforcement agency which may be able to recover the machine.

Other programs provide the user with the ability to execute commands remotely to the missing machine (if connected to the Internet), theoretically allowing the user to delete all of the important information on the hard drive.

If you haven't yet experienced the loss of a computer full of sensitive and confidential data, you are living on borrowed time. Plan ahead now to minimize the risk, reduce your exposure, and enhance your chances of recovery. Manage your risks through proactive strategies. Develop a security policy and implement it.

This is not an issue you can address once and have solved forever. Threats will change, risks will change, and requirements will change. Be sure your plans, your people, and your processes change along with them. Conduct periodic training updates, ensure software is kept up to date with the latest versions, and keep your emergency reaction checklists current.

Have a Question or Comment?

E-mail your questions or comments about the *Activity Review* to Lisa R. Hearne, the Board's Communications Manager, at **lisahearne@nccpaboard.gov**.

Board Office Closed

In accordance with the holiday schedule adopted by the State of North Carolina, the Board office will be closed on the following date:

Monday, September 1, 2008
Labor Day

Need a Form or an Application?

The Board has made most of its forms and applications available on its web site, **www.nccpaboard.gov**.

To access the forms, click on the "Forms" link on the left side of the home page.

Many of the forms and applications are interactive; the user types in his or her information and then prints the form and submits it to the Board.

If you do not have Internet access, you may request a form or an application by calling the Board office at (919) 733-4222 .

Address Changed?

21 NCAC 08J .0107 requires all licensees and firms to notify the Board in writing within 30 days of any change in address or business location.

Licensees and firms can make address changes online by clicking on the "Address Update" link on the Board's web site, **www.nccpaboard.gov**.

Address changes may also be submitted by fax, e-mail, or US mail.

Exam candidates must submit address changes by fax, e-mail, or US mail.

Please note that all address changes must be in writing; Board staff is prohibited from accepting oral changes of address.

www.nccpaboard.gov

Security Breach Notification

The following information is published as a courtesy to the North Carolina Department of Justice and the Consumer Protection Division of the North Carolina Attorney General's Office.

The Identity Theft Act of 2005 (NCGS 75-60, *et seq.*) requires businesses to notify **each** individual when there has been a security breach involving his or her personal identifying information. Notification waivers are void and unenforceable. A violation of this provision constitutes an unfair trade practice.

Who Must Notify?

A business that owns or licenses records or data that contain personal information, and that personal information has been subject to a security breach, must notify the affected parties.

A business includes sole proprietorships, partnerships, corporations, associations, charities, or any group, however organized. The business must be located in North Carolina or own/license the personal information (in any form) of North Carolina residents.

Businesses that maintain records/data that contain the personal information of North Carolina residents on behalf of an owner/licensee must notify the owner/licensee of a security breach.

What Is A Security Breach?

A "security breach" is defined as the unauthorized access and acquisition of unencrypted or unredacted records/data containing personal information with corresponding names, such as a first initial and last name.

The acquisition of encrypted data only constitutes a breach if a confidential process or key is also acquired.

"Personal information" includes an individual's social security number (SSN), employer taxpayer identification number (TIN), driver's license or state identification number, passport number, checking/savings account number, credit/debit card number, PIN, digital signature, biometric data, fingerprints, or any number that can be used to access his or her financial resources.

In addition, the access and acquisition of an individual's e-mail name or address, Internet account number, Internet username, or password may be considered a breach if it would permit access to his or her financial accounts or resources.

Personal information does not include publicly available directories that an individual has consented to have made available to the general public, including name, address, and telephone number.

Notification Requirements

Once a business discovers or is informed of a security breach, the business must notify those individuals affected, regardless of number. The notice must be clear and conspicuous and given without unreasonable delay.

Notice may be delayed if law enforcement informs the business that disclosure of the breach would impede a criminal investigation or jeopardize national security.

The notice must include a general description of the security breach incident; the type of personal information that was the subject of the breach; the business' general efforts to protect personal information from further unauthorized access; a telephone number for further information and assistance; and the advice that the affected individuals should remain vigilant by reviewing financial accounts and monitoring their credit reports.

If a security breach involves more than 1,000 persons, the business must provide written notice of the timing, distribution, and content of the notice to the Consumer Protection Division (CPD) of the Attorney General's Office, as well as the three major credit reporting agencies.

The CPD will need a copy of the notice itself, the date of the security breach, the date the notice goes out, and the manner of distribution. The CPD will also need the number of North Carolina residents affected and the total number of persons affected.

For more information on protecting yourself or your business from identity theft or security breaches, visit **www.noscamnc.gov**.

Facts About Identity Theft

- Nearly 10 million people in the United States are victims of identity theft each year. In North Carolina, approximately 300,000 people are victimized annually.
- The number of North Carolinians reporting identity theft to the Federal Trade Commission (FTC) jumped from 1,656 cases in 2001 to 5,830 cases in 2005.
- The Social Security Administration reported a 490% increase in allegations of Social Security number misuse between 1998 and 2001.
- Business loses nearly $50 billion to identity theft each year.
- Consumer victims lose $5 billion in out of pocket expenses as they try to restore their good names and credit, an average of $500 per victim. Victims of what the FTC considers the most serious kind of identity theft – such as those involving opening new accounts in the victim's name – spend $1,180 and 60 hours on average to try to undo the damage.
- Another study showed that a typical identity theft victim spends $800 and 175 hours over 23 months to clean up his or her reputation and erase $18,000 in fraudulent charges.

Inactive Status

"Inactive," when used to refer to the status of a person, describes one who has requested inactive status and been approved by the Board and who does not use the title "certified public accountant" nor does he or she allow anyone to refer to him or her as a "certified public accountant," and neither he nor she nor anyone else refers to him or her in any representation as described in 21 NCAC 08A .0308(b) [21 NCAC 08A .0301(b)(21)].

05/28/08		
Kimberly Bennett Bushnell	#30779	Durham, NC
Jesse Erik O'Shea	#29828	Matthews, NC
Barbara Mills Poole	#13769	Marietta, GA
Laura L. Seery	#28765	Maryville, TN
05/29/08		
Donna Goldstein Waga	#18089	North Charleston, SC
06/02/08		
Renee A. Ashe	#24766	York, SC
Peter Henry Bozetarnik	#25142	West Palm Beach, FL
Keli Michelle Decker	#29969	Horsham, PA
Kelly Adair Poteat	#20422	Matthews, NC
Robin Mendina Tenney	#29161	Raleigh, NC
06/03/08		
Olivia Jahnsen Jones	#19240	Katy, TX
06/03/08		
Heather Oakes Popadak	#26140	Bowdoinham, ME
Robert Glenn Ray	#4094	Fayetteville, NC
Deborah Gaile Watkins	#13918	Lancaster, SC
06/05/08		
Pamela Rowlings Geiger	#17161	Asheboro, NC
Linda Stowe Greer	#15265	Cornelius, NC
Daniel W. Mirabito	#25831	Ringoes, NJ
Murray Melvin Monosoff	#19565	Charlotte, NC
Thomas Hamilton White, II	#24846	Atlanta, GA
David Earl Williams	#2543	Greensboro, NC
06/09/08		
Robyn B. Beck	#20680	Charlotte, NC
Tina Marie Pittman	#26959	Chambersburg, PA
06/10/08		
Robert Hayden Crandall	#27331	Boone, NC
Janice Janette Martin Gearheart	#17710	Charlotte, NC
Wilbert Lyerly	#2535	Charlotte, NC
Zahayia Kannon Partin	#12644	Wrightsville Beach, NC
Ram Kumar Sangal	#20235	Durham, NC
06/11/08		
Jean R. Broadway	#31831	Wilmington NC
Mark Alan Cox	#19129	Southlake, TX
William Edward Johnson	#31689	New York, NY
Thomas Andrew Lewis	#6842	Atlantic Beach, NC
Junling Yang	#29744	Austin, TX
06/13/08		
Robert L. Fleshman	#25944	Marietta, GA
Julius C. Forhecz	#28049	McLean, VA
Walker James Grossell	#33029	Washington, DC
Stewart Clayton Hare	#32027	Mount Holly, NC
Olga Ivanova	#32224	Castle Rock, CO
E. Johnston LeDuke	#21733	Jacksonville, FL
06/13/08		
Jerry Allen Little	#3277	Asheboro, NC
Michelle Susan Moser	#24170	Wilmington, NC
06/16/08		
Barry Dale Church	#18848	Summerfield, NC
Diana Kriegsman Davis	#27774	Greensboro, NC
Phillip A. Hammond	#30150	Findlay, OH
W. Kelly Jones	#29863	Columbia, SC
Michael John Mas	#28908	Jacksonville, FL
Kathryn Noxon	#15642	Winston-Salem, NC
Danny Robert Parker	#6110	Greensboro, NC
Susan Alma Riddle	#18758	Greensboro, NC
Nina P. Saravia	#26360	Greensboro, NC
John Lawrence Schwarz	#22069	Charlotte, NC
Susan Walsh Stankavage	#17354	Durham, NC
06/17/08		
Walter Vaughan Davidson, Jr.	#8623	Charleston, SC
Penny L. Dierickx	#28748	Clayton, NC
06/18/08		
Wilhelm F. Dendorfer	#22249	Atlanta, GA
Bernarda Jackson	#32268	Wheaton, MD
Lori Young Masielle	#20756	Peachtree City, GA
Karl Newton Priedeman	#24657	Westerville, OH
Tomas C. Siaton	#27213	Clemmons, NC
Richard Worsley	#988	Greenville, NC
06/19/08		
Elizabeth Caroline Digirolamo	#29018	Mooresville, NC
Betty Jean Powell	#15595	Garner, NC
06/20/08		
Paulus Irwan Asali	#31711	San Jose, CA
Samuel Alfred Floyd	#16727	Raleigh, NC
Robert Jutzi Howell	#32953	Evanston, IL
Rebecca Lynn Neeriemer	#29826	Palm Beach Gardens, FL
Susan Raney Roach	#25599	Greensboro, NC
Susan Elizabeth Spain	#15713	Plano, TX
06/23/08		
Susan Carter Ferguson	#15065	Dallas, NC
Karen Downey Lightfoot	#20101	Gainesville, GA
Dawn York Morrison	#26694	Statesville, NC
John Quincy Shelton, IV	#30456	Charlotte, NC
Traci Taylor Welch	#18797	Bermuda Run, NC
Robert Leon Wellons, Jr.	#17374	Dallas, TX
06/24/08		
Melinda Jayne Crouse	#18390	Cary, NC
Amy Crary Erwin	#31630	Charlotte, NC
Lisa L. Koebrich	#31915	Atlanta, GA
Stuart Perinchief Rogers	#15318	Raleigh, NC
Alicia N. Thrasher	#33552	Charlotte, NC

New Exam Fees Effective August 1. See Page 3.

State Board of CPA Examiners

Board Members

Arthur M. Winstead, Jr., CPA
President, Greensboro

Michael C. Jordan, CPA
Vice President, Goldsboro

Jordan C. Harris, Jr.
Secretary-Treasurer, Statesville

Jeffrey T. Barber, CPA
Member, Raleigh

Norwood G. Clark, Jr., CPA
Member, Raleigh

Tyrone Y. Cox, CPA
Member, Durham

Maria M. Lynch, Esq.
Member, Raleigh

Staff

Executive Director
Robert N. Brooks

Deputy Director
J. Michael Barham, CPA

Legal Counsel
Noel L. Allen, Esq.

Administrative Services
Felecia F. Ashe
Vanessia L. Willett

Communications
Lisa R. Hearne, Manager

Examinations
Phyllis W. Elliott

Licensing
Buck Winslow, Manager
Alice G. Steckenrider
Cammie Emery

Professional Standards
Ann J. Hinkle, Manager
Mary Beth Britt
Paulette Martin

North Carolina State Board of
Certified Public Accountant Examiners
PO Box 12827
Raleigh NC 27605-2827

PRSRT STD
US Postage PAID
Greensboro, NC
Permit No. 393

21,500 copies of this document were printed for this agency at a cost of $3,054.46 or approximately $.142 per copy in July 2008.

Notice of Address Change

Certificate Holder _____
Last Name Jr./III First Middle

Certificate No. _____ Send Mail to ___ Home ___ Business

New Home Address _____

City _____ State _____ Zip _____

CPA Firm/Business Name _____

New Bus. Address _____

City _____ State _____ Zip _____

Telephone: Bus. ( ) _____ Home ( ) _____

Bus. Fax ( ) _____ E-mail Address _____

Signature _____ Date _____

Mail to: NC State Board of CPA Examiners PO Box 12827 Raleigh, NC 27605-2827

Fax to: 919-733-4209

Pursuant to 21 NCAC 08J .0107, all certificate holders and CPA firms must notify the Board in writing within 30 days of any change in address or business location.