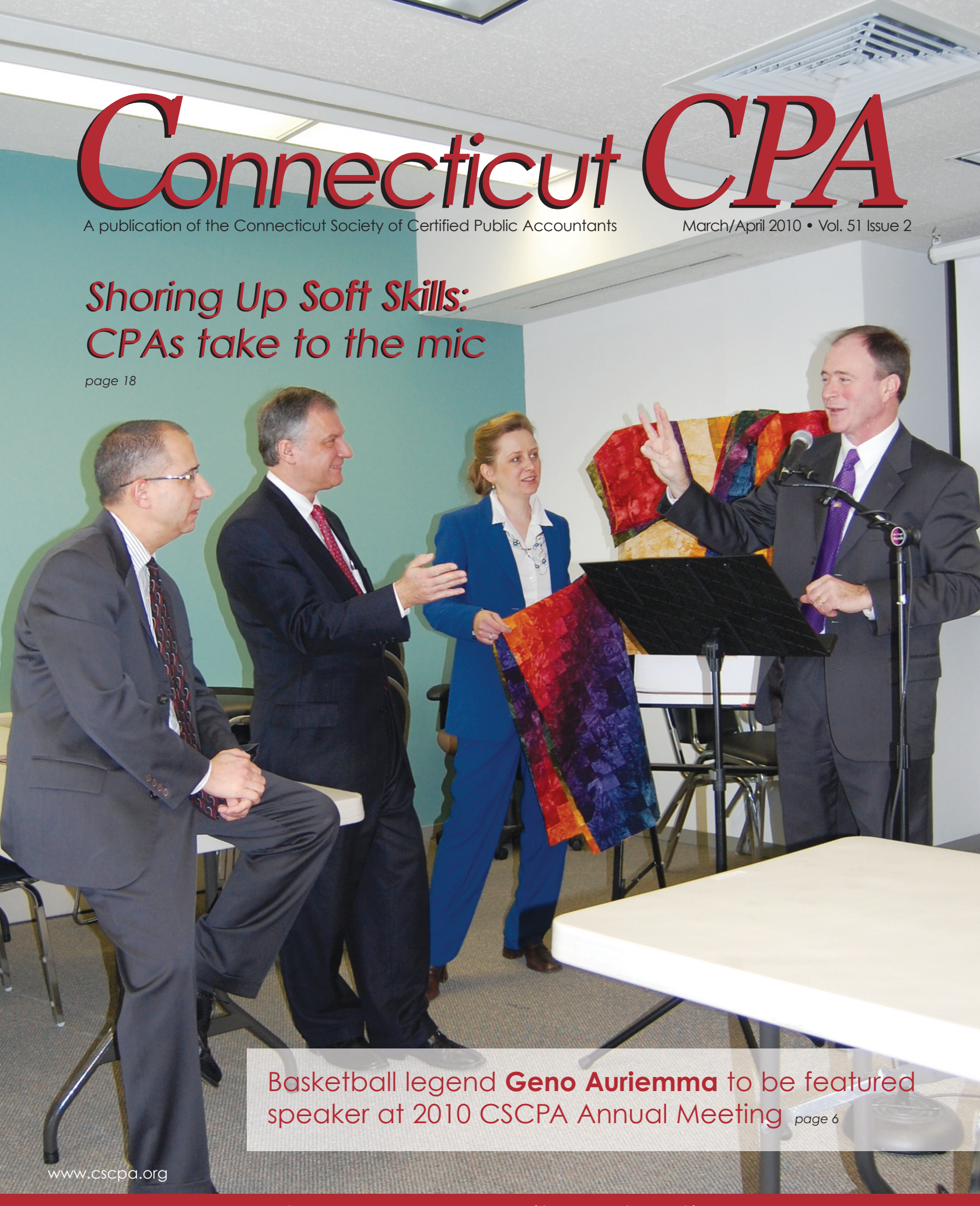
Connecticut CPA

A publication of the Connecticut Society of Certified Public Accountants

March/April 2010 • Vol. 51 Issue 2

Shoring Up Soft Skills: CPAs take to the mic

page 18



Basketball legend **Geno Auriemma** to be featured speaker at 2010 CSCPA Annual Meeting page 6

www.cscpa.org

advocacy • community • education

Just When You Thought It Was Safe To Buy Gas

By Stephen Pedneault, CPA, CFE, CFF, FCPA

The quantity of fraud and identity theft has become alarming. Thieves continue to develop new schemes to steal individuals' financial information and, ultimately, steal their funds.

To compound this issue, the financial institutions have begun to shift the burden for finding and funding fraudulent activity back to their customers, or at least are requiring notification of a potential problem in a more timely fashion to avoid bearing the risk of the loss.

Just as technology changes rapidly, so do the schemes being utilized to commit these crimes. In order to minimize the risk of becoming a victim – and detect a problem as quickly as possible once you have been victimized – it is incumbent upon you and your clients to keep up with the latest schemes and techniques.

Credit Card and Debit Card Skimming

Simply having and using a credit or debit card puts you at risk for a financial crime. Hopefully by now most cardholders understand the risks associated with using their cards, and that unscrupulous employees working at merchants like restaurants and stores can easily swipe your information after the card has been provided to them.

However, I suspect most cardholders are less aware that the schemes utilized by thieves have evolved, taking advantage of state-of-the-art technology. Skimming devices now utilize wireless communications, and the latest devices have the ability to communicate the swiped card's information in real time to an accomplice's cell phone.

Once captured, the card's information is sent to another involved party who uses the information to generate a fictitious card. The theft can be accomplished before an unsuspecting person's credit card has been returned.

A trend that started on the West Coast has now made its way into Connecticut. Skimming devices in the shape of card insert slots have been regularly used as attachments to ATM machines, along with a small camera to capture your pin number. Worse, thieves have been replacing the devices used to allow ATM users access into the ATM's secured room with their own devices, capturing the card information as the cardholder simply swipes his or her card just to gain access to use the ATM.

These devices are typically installed after the banks close and retrieved before the banks open in the morning. Based on the timing, the victim banks don't know the skimming devices were even installed until customer complaints are received and camera images are reviewed.

Now that these devices have been found installed at Connecticut ATMs, it is imperative that you observe your surroundings when using any ATM. If there is anything suspicious, out of the ordinary, or looks as though it is not part of the actual ATM, it would be wise not to use that ATM and to contact the police.

Adding Fuel to the Fire

The latest round of skimming involves thieves opening gas pumps and installing skimming devices within the gas pumps. It turns out many of the fuel pumps common to most stations utilize similar keys. Once a thief obtains a key, even the station's owners may be unaware the devices have been installed in their pumps.

I have advocated for years for individuals to shred their debit cards and strictly use credit cards for their spending activity.

These internally installed devices, hidden from the consumer's view, copy the information of every cardholder who uses the manipulated pump to purchase gas using their credit or debit card. The stolen information is then transmitted via cellular service to a nearby co-conspirator's cell phone.

What can you, the consumer, do about it? As far as prevention – nothing! Detection is the key. Cardholders need to review their statements and account activity on a very regular basis in order to identify fraudulent activity as quickly as possible.

Credit Cards vs. Debit Cards

Having been a victim of fraudulent activity three times with my debit card and several times with credit card transactions, I have advocated for years for individuals to shred their debit cards and strictly use credit cards for their spending activity. I also advocate returning to a simple ATM card to allow you access to your funds whenever needed. I did several years ago.

Here's the difference and why it matters. Credit cards provide a credit limit and require payments to be made against the borrowed balance, similar to a loan. If fraudulent activity occurs within your credit card account, you simply alert the card's issuer (bank), have the card shut off, dispute the fraudulent transactions, and obtain a new card. The issuer will require you to complete a financial affidavit, but in the end the fraudulent transactions shouldn't cost you anything.

Conversely, a debit card is linked directly to your bank account, with each purchase automatically withdrawn from your account. When your debit card is fraudulently used, your funds are withdrawn from your account. Your money is gone. Once detected, you have to work with the card issuer to get your money back.

While that usually occurs, two things highlight the risks to you. First, with the shifting of the shared fraud exposure, the issuer may decide not to put the funds back into your account, leaving the loss with you. Second, if your mortgage or other bills are due during the period between the theft and the return of the funds, you will have to determine how those bills will be paid on time, as your funds are gone from your account.

(continued on next page)

Just When You Thought it Was Safe to Buy Gas *(continued from previous page)*

The short answer is easy – discontinue using a debit card linked to your bank account and return to a traditional credit card. If you manage your cash flows to enable you to pay the credit card balance on a monthly basis, you should end up exactly where you would have been when the funds were withdrawn from your bank account each time you used your debit card.

Financial Institutions Responses to Fraud

Have you been reading the notices accompanying your monthly statements? The notices I've been receiving with my bank statements, loan statements, and investment accounts have been identifying my new role and responsibilities regarding fraudulent activity within my accounts. Most recently, the notices I have been receiving indicate I have a very limited time period to identify and notify the affected bank of a potential problem within my account. While some of my accounts offer up to 30 days notice, more recently I have been receiving notice with periods significantly reduced (as little as days), and they now also include financial consequences for not providing notice within the identified time period.

One notice I just received indicated I had four days to notify the bank of a potential problem, or I would be assessed the cost of the loss up to the first $500 of the fraudulent activity. Four days is not much time – what should I do if I'm away for a week without Internet access? The trend I am seeing will require the customer to monitor his or her account activity daily and provide notice within days in order to ensure the return of their funds.

What this means is that every customer now needs to develop a daily habit of monitoring his or her bank, investment, and loan accounts in order to avoid having fraud activity result in a financial consequence previously covered by the financial institution. Failing to identify and notify the financial institution in a timely manner could cost the customer his or her funds. In some of the accounts I maintain, that could be up to $500 presently. I predict as fraud increases, this threshold will only increase as well, raising the customer's exposure higher and higher.

Remain Vigilant

Every account holder must remain vigilant over the activity within his or her accounts. Based on ever-changing technology and the adoption of the technological innovations by individuals committing crimes, customers will be able to do less and less to prevent themselves from becoming victims.

Regardless of how fraud evolves, the three-tier approach to fraud risks will remain your most effective means. The first element is prevention. By limiting where you use your cards and being observant at ATMs, you won't use your cards at places that may increase your risks. But, as illustrated by the skimming within gas pumps, there may be no way for the customer to know his or her card was skimmed, and therefore no way to prevent this from occurring.

The second element is detection. This is where each customer has the greatest impact, which is consistent with the direction the financial institutions are moving toward. Detect a potential problem or issue as early as possible – allowing the bank's fraud units to respond as quickly as possible, increasing their ability to stop the crimes, catch the responsible parties, and recover the funds.

The third and final element is to obtain and maintain adequate insurance coverage. If both prevention and detection have failed, typically the only means available for recovery is through insurance. While not common and often not available for individuals, this coverage is certainly available for businesses in the event their employees steal from the company, which is another growing problem.

Stephen Pedneault, CPA, CFE, CFF, FCPA is the principal of Forensic Accounting Services, LLC in Glastonbury, specializing only in forensic accounting, employee fraud and litigation support matters. Pedneault is a Certified Fraud Examiner (CFE) and Certified in Financial Forensics (CFF). He is the author of Fraud 101: Techniques and Strategies for Understanding Fraud *(Wiley) and the recently released* Anatomy of a Fraud Investigation *(Wiley). Pedneault is also a member of the CSCPA Board of Directors. He can be reached at Steve@forensicaccountingservices.com. To find more information about Forensic Accounting Services, visit www.forensicaccountingservices.com.*

Want to hear more from Steve Pedneault?

He'll be a featured speaker at the 2010 CSCPA Accounting and Auditing Conference!

CSCPA Accounting and Auditing Conference
June 8, 2010, Aqua Turf Club, Plantsville

Find out more and register at www.cscpa.org/register.