May 29, 2009

Mr. J. Gordon Seymour
Secretary
Public Company Accounting Oversight Board
1666 K Street, NW
Washington, D.C. 20006
USA

By E-mail: comments@pcaobus.org

Re: Concept Release on Possible Revisions to the PCAOB's Standard on Audit Confirmations

Dear Mr. Seymour:

We would like to thank you for the opportunity to provide the Public Company Accounting Oversight Board (PCAOB) with our comments on the Concept Release on Possible Revisions to the PCAOB's Standard on Audit Confirmations (hereinafter referred to as "the Standard").

We believe that an updated Standard will provide a useful basis for improving the effectiveness and the efficiency of audits and more specifically will improve the audit confirmation process. We support revising the Standard.

The Concept Release asked for answers to specific questions and while we provide an answer to each question, we thought that it would be more beneficial to the PCAOB if we only took a position on the questions we felt we were best equipped to answer.

Questions raised by the PCAOB

1. Should the objective of the confirmation standard be for the auditor to design and perform confirmation procedures to obtain sufficient, competent evidence from knowledgeable third parties outside the company in response to identified risks?

Yes, the scope and focus of the confirmation standard should be to set the requirements that will improve auditor performance in designing and properly controlling the audit confirmation process.

Specifically, we believe the standard should start with the premise that the auditor's objective in performing audit confirmations is to properly control the process. Based on the high number of audit failures involving a compromised audit confirmation process, the standard should set the guidelines for what constitutes proper control over the confirmation process. Based on the collective guidance from the PCAOB, the IAASB and the ASB, as well as other non-authoritative research, we believe that proper control over the confirmation process requires the auditor to:

Properly control the process

1. Authenticate the identity and legitimacy of the responding source/entity;

2. Validate that the respondent is knowledgeable, free from bias, and authorized to respond on behalf of the responding source/entity;

3. Receive a direct, active response from the responding entity;

4. Ensure the integrity of the confirmation request and response throughout the process.

2. Should the definition of confirmation allow for responses other than traditional mailed responses, such as oral confirmation, facsimile, email, responses processed through third-party providers, and direct on-line access to information held by a third party?

We support an update to the definition by the PCAOB; however, we believe that this updated definition should take a forward looking approach since future technologies and processes will continue to improve the audit confirmation process. Therefore, we believe that instead of trying to identify within the standard all the approaches that exist today, and determining whether they meet the definition of a properly controlled confirmation process or not, that the new definition should allow for any confirmation process that adheres to the tenants of a properly controlled confirmation process. Through this approach the PCAOB ensures both adherence to the standard while crafting language that is prepared for each new advance in technology.

Specifically related to the question of which types of confirmations should or should not be allowed, we support the discussion from recent SAG meetings as well as ASB meetings that certain electronic processes such as email and direct access to a third-party database are unacceptable and not audit confirmations for assurance purposes but are instead alternative procedures.

Direct Access to Third-Party Database

Direct access to a third-party database is not a confirmation because there is not an active response and there is no ability for the auditor to assess the integrity of the data being pulled. It is also too easy for a client to create a fake website to circumvent the auditor's confirmation procedures.

Over the last several years, would-be thieves created fake Wells Fargo, U.S. Bank, Bank One, Citi Group and other banks' websites for their own gain, to steal important online banking information from customers. These fraudsters were even able to "highjack" and use an email with the real bank email extensions, a process called "phishing," and then direct bank customers to the fake websites. If the banks' own customers could not distinguish the real site from the fake site, auditors who might see this website only once a year may have trouble determining whether it is real or fake. Auditors may not be able to detect fake information unless they do more than a typical cursory review; they must take the time to validate a website's authenticity.

Validating the authenticity of a website, however, is extremely difficult and in some cases impossible. Fraudsters can purchase a website address, also known as a URL for $35 with a name similar to the legitimate company's website, and pay an Internet Service Provider (ISP) less than a hundred dollars to host the website. Then the fraudster simply copies the source code from a legitimate website to create the replica site. (Once on a website, click your right mouse button and then select View Source from the drop down. Then highlight and copy the source code, and paste it into any website building software to create a replica of the legitimate website.) The new site might well contain a fake auditor log in section where audit confirmations are falsely responded to or provide "direct access" to the third-party database containing falsified information. The fake site can even provide the auditor with incorrect contact information, including email addresses, telephone and FAX numbers, and fake mailing addresses just in case the auditor attempts to validate the legitimacy of the website through

contacting the responding party. Because the fraudulent website is almost an exact replica of the original and valid website, the fraudulent website and email extension appear to be legitimate to those who do not have a day-to-day working relationship with that specific financial institution or responding company.

One way to discover who owns a website is to use the DNS (Domain Name Server) lookup feature available on the internet; however, the DNS lookup information is subject to being manipulated to appear legitimate, even stating the real names of executives at a bona fide company. There is no regulatory or governing body that proactively ensures the DNS information is correct. It is basically a self-regulated service. As a quasi-self-regulated service, fraudulent information is often used with DNS lookup information to prevent people from identifying the true owner of a URL. When a complaint is filed questioning a URL's DNS information, the owner of the URL is simply given the opportunity to update the DNS information over the Internet, using possibly false data again, and the process starts over.

Until a URL has received numerous complaints over an extended period, often many months, an extensive assessment may never take place. Fraudsters understand this process and use it to manipulate the system. They know that the amount of time and energy required to identify the true owner of the URL would be significant.

Email is Unacceptable

Email does not and should not constitute a confirmation. First, is email's lack of security and how simple it is to "sniff" an email. Because email is delivered over the open Internet and it bounces around from computer to computer before arriving at its destination, those looking to intercept email now use a technique called "sniffing" where a person can seek out and capture specific emails from or to certain people. In fact, a search on the term in both Google and YouTube provide "How To" instructions.

One suggestion of note is to use secure email to communicate securely with the responder; however, that would not necessarily detect fraud. Secure email only ensures that the two-way communication was done in a secure manner; it does not serve to authenticate the identity of the responder. That is because it is too simple for someone to "spoof" an email to make it appear that the confirmation response sent via email came from a particular individual or department within a responding company when in fact that person or that department did not respond. Therefore, email cannot be considered a valid confirmation for assurance purposes because of the inability of the auditor to validate the authenticity of an email.

3. What direction should the standard include regarding the use of electronic confirmations and third-party service providers?

Confirmations using a properly controlled electronic process should be allowed within the standard. Like any confirmation process, confirmations sent through electronic means should be required to adhere to the tenants of a properly controlled confirmation process. Attachment 1 has been included as a sample evaluation form for assessing electronic confirmation processes.

4. What procedures should the auditor be required to perform to address the risk that the information is not from a proper source and the risk that the integrity of the data has been compromised?

The auditor should be required to authenticate that the confirmation is sent to and responded by the proper source, that the individual who responded is knowledgeable, free from bias and authorized to respond on behalf of that source.

Wayne Kolins, the National Director of Assurance for BDO Seidman stated at the PCAOB's June 2004 Standing Advisory Group[1] meeting that,

> "I think the biggest problem that I see with confirmations is 'who' on the other side is actually signing the confirmations? Are they sufficiently knowledgeable? And is the auditor even thinking about that when he or she receives the confirmation? This is one of the most significant pieces of evidentiary matter that the auditors have (an audit confirmation) and to the extent that that is diluted is a significant detriment to the audit process."

The auditor should also be required to provide assurance as to the integrity of the data throughout the entire confirmation process. Attachment 1 has been provided as a sample evaluation form to help the auditor assess the risk that the information is from the proper sources, and that the integrity of the data has not been compromised within an electronic confirmation process.

Looking at the definition of a properly controlled confirmation, as well as how audit confirmation frauds have happened or might happen, would be good ways to identify the proper suggested procedures as well. Examples might include:

Example 1 - Authenticate the Responding Source – Mark Morze, the CFO of ZZZZ Best Carpet Cleaning, used a friend's home address for where a confirmation was sent.

> Solution 1 - Independently look up the contact information (address, fax number, website, email, phone number) for every confirmation respondent before the confirmation is sent. The auditor should not rely on the client or client provided documentation or systems for the contact information of where to send a confirmation and to whom it should be addressed.

Example 2 - Validate the Respondent – during the Parmalat Fraud the bank that supposedly held the $4.9 billion in cash has claimed that, though the name of the person who signed the confirmation was employed by the bank, she was not authorized to respond and she did not complete that confirmation. Or the CF Foods fraud where the owner of CF foods inflated receivables at certain customers and once those customers were chosen in the random sample selection, the owner of CF Foods simply called those customers, said that a mistake had been made, and could the customer please return the audit confirmation letter to the owner directly. The owner then completed the confirmation with the false information, signed his customer's name and mailed it back to the auditor where the false balance matched exactly the fake documents that had been provided to the auditors.

> Suggestion 2 – The auditor should call the individual who responded to the confirmation to verify that they did in fact complete the confirmation. The auditor should not ask the client for the contact information of that individual, but should instead independently look up that person's contact information before contacting them.

[1] PCAOB Standing Advisory Group Meeting. June 21, 2004. Afternoon Session 1, timeslot 1:52:00/2:18:53. http://www.connectlive.com/events/pcaob/

Example 3 – Validate the Respondent is authorized to respond – during the Kmart, Ahold, and the Just for Feet audits where fraud occurred, the client directed the auditors to send the receivables confirmations to people like the National Director of Sales, the Corporate Account Managers, the Vice President of Business Development and other "relationship managers" instead of individuals within the Accounts Payable departments.

> Suggestion 3 – The auditor should call the supervisor of the individual who responded to the confirmation to verify that the respondent is authorized to respond to an audit confirmation on behalf of that entity and the auditor should document that conversation. The auditor should not ask the client for the contact information of the supervisor, but should instead independently look up that person's contact information before contacting them.

Example 4 – As part of their fraud, executives at HealthSouth manipulated the auditor's confirmation process to inflate revenue almost $400 million with the offsetting journal entry to Cash. It has been suggested that HealthSouth employees were familiar enough with the auditor's confirmation procedures to understand that with several thousand bank accounts to confirm that the auditors did not send bank confirmations on accounts with less than $10 million in the account. To conceal their fraud, HealthSouth allegedly created several hundred fake accounts that each contained less the $10 million knowing that individually these accounts would not be selected for confirmation.

> Suggestion 4 – It is understood that mailing confirmations is a tedious and time consuming process with 30-60 day turnaround times, however, the new secure electronic confirmation processes which reduce staff time and shorten turnaround times to 1-2 days can now be used in coordination with SAS No. 99's requirement to alter the nature, timing and extent of the auditor's procedures based on risk. In the confirmation area, auditors could now use electronic confirmations to increase their sample sizes and send confirmations more often throughout the year on a semi-annual or quarterly basis.

Additional guidance, like a Practice Alert or an addendum to the standard, might be used to more fully address many of these suggestions if there is not room within the body of the standard to provide complete guidance to the auditor.

5. Intentionally left blank.

6. Should the Board require that the auditor consider confirming other items? If so, which items should be included in this requirement?

The Board should require the auditor to also perform bank confirmations. Auditors must presume that there is a risk of fraud within Revenue during the mandatory brainstorming and planning session. To address the offsetting journal entry to Revenue within either Accounts Receivable or the Cash account, the auditor should be required to not only send receivable confirmations but also bank confirmations.

7. Should the Board require the auditor to perform specific procedures when evaluating whether confirmation of accounts receivable would be ineffective? If so, what should those procedures include?

May 29, 2009

Many auditors evaluate whether to send accounts receivable confirmations based on old confirmation processes and conclude that historically poor response rates and high error rates are indicative of the future and therefore conclude that accounts receivable confirmations are ineffective. However, auditors may inadvertently be drawing the wrong conclusion. Is it the accounts receivable confirmation that is broken, or the confirmation process they used that is broken? The PCAOB's research synthesis paper written by members of the American Accounting Association (AAA), as well as other more recent research, asserts that advances in new electronic confirmation processes are improving confirmation response rates while reducing the opportunity for fraudulent confirmations.

Additionally, it has been suggested that part of the motivating factor to label confirmations as ineffective has been the amount of time spent/wasted by auditors chasing confirmation responses.

While we do not support this approach to performing audits based solely on time and cost savings, we certainly understand the inefficiencies of outdated audit procedures. Therefore, we support the conclusion reached in the PCAOB commissioned research synthesis paper which states:

> *Technology offers the opportunity to authenticate confirmation responses and streamline the confirmation process.*[2]

Evidence of how electronic confirmations have improved response rates, lowered error rates, and improved turnaround time is shown below in Table 1:

Table 1

	Electronic Confirmations**				Mailed Paper
	2007	2008	2009	TOTAL	Confirmations
Response Rate*	100.00%	100.00%	100.00%	100.00%	71.55%
Reconfirmation Rate*	8.9%	8.3%	10.1%	9.9%	43.43%
Ave. Turnaround (days)	1.07	0.91	1.06	1.05	21.00
% Turned in 2 days	88.93%	92.47%	93.53%	93.05%	0%
% Turned in 3 days	94.15%	96.90%	95.94%	95.84%	0%
% Turned in 5 days	98.09%	98.57%	98.74%	98.67%	< 1%

***** For Mailed Paper Confirmations, the results are the combined results from research studies looking at response rates: Davis et al. 1967; Sauls 1970; Hubbard & Bullington 1972; Armitage 1990; Engle 1991; Engle & Hutton 2001; Allen & Elder 2001; Elder & Allen 2005.

** For Electronic Confirmations, the results are weighted based on the number of electronic confirmations within each period through www.confirmation.com.

8. Intentionally left blank.

9. Intentionally left blank.

[2] Caster, P., R. Elder, and D. Janvrin. 2006. A Summary of Research and Enforcement Release: Evidence on Confirmation Use and Effectiveness. (May): 23.

10. Should the standard include the requirement for the auditor to test some or all of the addresses of confirmation parties to determine whether confirmation requests are directed to the intended recipients? Why or why not?

In 1990 and 1991 when SAS No. 67 was being written, it was pointed out in an article titled Pitfalls in the Confirmation Process that the step of validating the mailing address was not written into the draft standard at the time. The response from those drafting the standard was that it was so obvious that validating the mailing address was a required part of performing the confirmation process correctly, that having to write this step into the standards would actually be an insult to the profession. However, today this step in the confirmation process is often not performed by auditors because of the time needed to perform this step correctly. We believe that the public, who relies on audit reports, would seriously question our audit approach if we as auditors chose not to do something as simple as validate a mailing address before we mailed a confirmation. Hindsight is 20/20, and while a jury may not understand off-balance sheet assets, they certainly understand not checking a mailing address. If our profession can't do what may seem simple to most, then how can we be trusted with the more complex aspects of the financial audit?

Yes, the auditor should be required to test all of the addresses (or other relevant contact information depending on the confirmation process used) for all of the auditor's confirmations. Independently validating all of the mailing addresses and contact information is part of performing the confirmation process correctly.

Take for example inventory counts. If there are a thousand SKUs and the statistical sample size selected is 126, the auditor is prohibited from counting just 63 of the SKUs and eyeballing the rest of the SKUs because it is too time consuming. The auditor must count all 126 SKUs selected as part of doing the inventory count correctly and for the sample to be a statistically valid representation of the entire population.

The same holds true for independently validating all of the mailing addresses for confirmations. Validating the mailing address is part of the auditor's responsibility to Control the confirmation process. If the auditor has a statement provided by the client, why send the confirmation at all if the auditor isn't going to validate the location for where the confirmation is sent? It is impossible for the auditor to place any reliance on the information provided in a confirmation response if the auditor can give no assurance as to the location of where the confirmation was sent.

P.O. Boxes

A P.O. Box as the mailing address for a confirmation is one of the "red flags" for auditors. Because places like The UPS Store, FedEx/Kinko's and other P.O. Box providers want to help small businesses look like larger business, they now offer "Real Street Addresses" as their #1 selling point in their marketing material (see Attachment 3) so that small businesses can appear bigger than they are. These providers also offer mail forwarding capabilities as well. While one of the providers has the tagline "It's our job to make your job easier," they might as well have told fraudsters "It's our job to make your *fraud* easier." Fraudsters can now provide the auditor with a real street address to limit suspicion. For a small cost, fraudsters can even set up multiple mail locations that appear to be legitimate customers or banks and simply have the store forward all the audit confirmations back to the fraudster. Then the fraudster can complete the confirmations with falsified information that matches the fake statements provided to the auditor.

11. What additional direction should the standard include with regard to maintaining control over confirmation requests and responses?

Maintaining control of the confirmation process used to mean that auditors simply had to put the envelope in a blue U.S. Postal Service mailbox and that the response had to come back to our office, not the client's office. However, we as auditors are really losing control from the start because a large percentage of auditors continue to rely on their clients, or client provided systems or documentation, to tell them where and to whom to send the confirmation.

Regardless of the confirmation process used – mail, electronic, etc. – auditors need to perform the following steps to properly control the confirmation process to reduce the opportunity for their confirmation procedures to be circumvented by the client:

Properly control the process

1. Authenticate the identity and legitimacy of the responding source/entity;
2. Validate that the respondent is knowledgeable, free from bias, and authorized to respond on behalf of the responding source/entity;
3. Receive a direct, active response from the responding entity;
4. Ensure the integrity of the confirmation request and response throughout the process.

12. What direction is necessary in the standard regarding maintaining control over confirmations in electronic form?

If the proper steps are followed to control the confirmation process then the type of process used – electronic, mail, etc. – should not matter. We do believe that the PCAOB could use additional guidance, such as practice alerts or an Electronic Confirmation Guide, to help the profession understand what procedures might be useful to ensure that the tenants of the confirmation process are adhered to.

One of the topics should cover the fact that each electronic confirmation service should have both a SAS 70 Type II and SysTrust certification because each is uniquely positioned to address different aspects of properly controlling an electronic confirmation process. For example, a SysTrust gives a higher level of assurance on security and data integrity than a SAS 70 Type II. A SAS 70 Type II is better than a SysTrust in evaluating the Authentication and Authorization procedures used by electronic confirmation services to authenticate the users and to define the access rights to the service. A SAS 70 Type II can also address items like insurances, service level agreements and background checks for those who oversee/manage the electronic confirmation service that are not addressed in a SysTrust.

A sample Electronic Confirmation Security Assessment is enclosed as Attachment 1 to this document.

13. What changes should be made to the standard regarding the auditor's responsibility for evaluating the reliability of confirmation responses and alternative procedures?

The guidance regarding the auditor's responsibility for evaluating the reliability of the confirmation response should be reinforced by the updated standard. The auditor has to be responsible for evaluating and determining that the confirmation response is reliable. That is what the public expects and requires, anything less would result in the profession being seen as underperforming. If the auditor's procedures and control of the confirmation process do not provide the auditor with a high level of assurance as to the reliability of the confirmation response, then there is no real purpose in performing audit confirmations.

14. When an auditor uses direct on-line access to a third-party database or a third-party service provider, what procedures should the auditor be required to perform to assess that the information included in the third-party database or provided by the third-party service provider is reliable?

Because direct online access to a third-party database does not involve an active response on the part of the responding party, according to the current guidance provided by the AICPA Updated Practice Alert 2003-01, direct online access to a third-party database does not constitute a confirmation for audit purposes.

We support the requirement that a valid confirmation process and response include an active response on the part of the responding third-party. Direct online access to a third-party database should continue to be defined as an alternative procedure.

When evaluating an electronic confirmation process, auditors should be required to ensure the electronic process adheres to the tenants of a properly controlled confirmation process.

Properly control the process

1. Authenticate the identity and legitimacy of the responding source/entity;
2. Validate that the respondent is knowledgeable, free from bias, and authorized to respond on behalf of the responding source/entity;
3. Receive a direct, active response from the responding entity;
4. Ensure the integrity of the confirmation request and response throughout the process.

We have provided a sample evaluation form as Attachment 1 that can be used by the auditor to address each of the tenants of a properly controlled confirmation process.

15. Are there factors other than those mentioned above that the auditor should consider when evaluation the reliability of electronic confirmations? If so, what are they?

Please see Attachment 1 which incorporates the factors the auditor should consider when evaluating the reliability of an electronic confirmation.

16. Intentionally left blank.

17. Should the standard require the auditor to investigate exceptions identified as a result of confirmation responses?

Yes, the auditor should be required to investigate exceptions identified as a result of confirmation responses. Not doing so will jeopardize the public's trust in the profession's audit procedures and will give opposing legal counsel room to criticize our professional judgment.

18. Should there be a requirement for the auditor to consider the possibility of previously unidentified risk of material misstatements including previously unidentified fraud risk factors when performing alternative procedures for non-responses and investigating exceptions on confirmation responses?

On September 22, 2004 Toby Bishop, a CPA and the then President and CEO of the Association of Fraud Examiners, said in a speech in Washington D.C. that:

> "*Fraudsters are the most reliable returners of auditors' confirmation letters, completed and signed without exception."*

Toby was addressing the long overlooked fact that fraudsters understand that in order to cover up a fraud they must fool the auditor into believing the falsified financial statements. For audit assertions that are addressed through the use of audit confirmations, fraudsters know that auditors think the "red flags" in the confirmation process are (1) when a confirmation goes to a P.O. Box, (2) goes to an invalid address, (3) doesn't come back at all, or (4) comes back with different information than the auditor was provided by their client. This is why "Fraudsters are the most reliable returners of auditors' confirmation letters, (which are) completed and signed without exception." Fraudsters know that auditors will follow up if the address provided to the auditor is a non-existent address. Fraudsters know that the auditor will ask questions if the confirmation response provides different information than what was provided on the falsified bank statement or invoice. Fraudsters make sure that they can interfere with and circumvent the auditor's confirmation procedures in order to provide the auditor with a "signed" and "matching" confirmation that provides comfort to the auditor so that there are no "red flags" that lead to additional questions by the auditor.

In truth, confirmations that go to a nonexistent address or that come back with conflicting information are most often just errors. The real risk of confirmation fraud lies within the confirmations that come back signed and with matching information. To address the risk of confirmation fraud auditors should call the supposed responder back (using a phone number that the auditor has independently validated) and ask if that person really completed the confirmation and if the response information is correct. The auditor should also call the responder's supervisor to verify that the person who responded was authorized to respond on behalf of that entity.

19. Intentionally left blank.

20. Should the standard include procedures for the auditor to perform to address situations in which management requests the auditor not confirm certain accounts, transactions, agreements, or other items? If so, are the procedures listed above the appropriate procedures for the auditor to perform? What other procedures should the auditor perform to address situations in which management requests that the auditor not confirm accounts, transactions, agreements, or other items?

By updating the confirmation process to be a properly controlled process, auditors should be extremely wary of a client who adamantly objects and refuses to allow the auditor to use the new confirmation procedures. Because the average fraud goes undetected for 18 months according to the Association of Certified Fraud examiners, in all likelihood, a client who has circumvented the auditor's confirmation procedures in the past will be extremely upset if the auditor incorporates an updated, more controlled process into their confirmation procedures.

21. Should the auditor be required to perform specific procedures to evaluate the effect of disclaimers and restrictive language on confirmation responses? If so, what specific procedures should an auditor be required to perform in evaluating such disclaimers or restrictive language?

Though some auditors don't realize it, the current Standard Bank Confirmation includes standard disclaimer language. Auditors should be encouraged to review such language and compare it to any additional disclaimers provided by the responding party.

Reviewing the current standard disclaimers may also reduce the chance that an auditor incorrectly relies on a confirmation response for more than the responder intended. For example, with bank confirmations, some auditors assume the bank is required to provide the auditor with information about additional accounts the client may have with the bank that the auditor did not list on the confirmation request. However, this is not true according to the agreed upon language between the accounting profession and the banking industry on the Standard Bank Confirmation form.

Standard Client Statement:

> *"Although we do not request nor expect you to conduct a comprehensive, detailed search of your records…"*

Standard Bank Response:

> *"Although we have not conducted a comprehensive, detailed search of our records…"*

Because of Sarbanes-Oxley and the enforcement of SEC Rule 13b2-2 which allows the SEC to bring charges against companies with employees who provide misleading confirmation responses to a public company's auditors, accounting firms should expect that the legal counsel for any company responding to an auditor's confirmation requests will contain new, additional disclaimer language. The recommended alternative to these disclaimers suggested by many law firms to their clients is to simply stop responding to audit confirmation requests because there is no law requiring them to respond to an audit confirmation request. A paper was written and published that was directed to those who respond

to audit confirmation letters encouraging them to participate in the audit confirmation process, and why "controlling the process" on their side was a better approach to reduce their risk of litigation than a "No Response." That paper is included as Attachment 2.

During the April 2, 2009 Standing Advisory Group (SAG) meeting several of the members stated that the SEC should require that public companies respond to audit confirmations. We support the approach to require public companies to respond to confirmation requests and that non-public companies should be required to respond to audit confirmation requests from the auditors of public companies.

22. Should auditors be allowed to use negative confirmations and, if so, in what circumstances?

Because there may be certain circumstances where negative confirmations might be preferred over positive confirmations, we support the idea that the PCAOB should seek to limit the use of negative confirmations and should provide guidance to auditors as to when negative confirmations may be used.

23. Intentionally left blank.

Thank you for the opportunity to provide input into the standard setting process and we hope that our views will be helpful to the PCAOB as it deliberates on the final version of this proposed standard. If you have any questions relating to our comments in this letter, we would be please to discuss them with you.

Sincerely,

Brian Fox

Brian Fox, CPA
Vice President

ATTACHMENT 1
Electronic Confirmation Security Assessment

May 29, 2009

		Required for		Reviewed, Appropriate & In Place			
		In-Network	Out-of-Network	Yes	No	Notes	Reviewer
1. SAS 70 Type II		√	√				
1.01	Performed every 6 months	√	√				
1.02	Controls for Organization & Administration	√	√				
1.03	Controls for Systems Development & Change Management	√	√				
1.04	Controls for Computer Operations	√	√				
1.05	Controls for Physical Access & Enviornmental Controls	√	√				
1.06	Controls for Authenticated Proper Source	√	N/A				
1.07	Controls for Authorized Users	√	N/A				
1.08	Controls for Proper Client Authorization	√	√				
1.09	Controls for Data Integrity & System Transmission Integrity	√	√				
1.10	Controls for Electronic Signatures	√	√				
1.11	Controls for Backup & Recovery/Data Retention	√	√				
2. SysTrust Certification		√	√				
2.01	Performed every 6 months	√	√				
2.02	Includes Principle of Availability	√	√				
2.03	Includes Principle of Confidentiality	√	√				
2.04	Includes Principle of Processing Integrity	√	√				
2.05	Includes Principle of Security	√	√				
2.06	Includes Principle of Privacy	√	√				
3. Privacy Policy		√	√				
3.01	Certified by recognized 3rd Party (e.g. TRUSTe)	√	√				
3.02	Includes EU Safe Harbor Certification (highest available)	√	√				
4. Website Authentication		√	√				
4.01	Extended Validation SSL Certification by recognized 3rd Party (e.g. VeriSign)	√	√				
5. Disater Recovery Plan		√	√				
5.01	Tested at least Quarterly	√	√				
6. Hosting Facilities		√	√				
6.01	Primary Hosting Facility with SAS 70 Type II or ISO Certification, minimum Tier 4 facility	√	√				
6.02	Separate Backup Hosting Facility with SAS 70 Type II or ISO Certification, minimum Tier 4 facility	√	√				
7. Insurances		√	√				
7.01	Rating A+ or better in the current Best's Insurance Reports published by A. M. Best Company	√	√				
7.02	E-commerce Technology Liability	√	√				
7.03	User Privacy Protection to cover 1 year worth of Consumer Credit Monitoring in the event of a Security Breach	√	√				
7.04	Commercial General Liability	√	√				
7.05	Professional Practice	√	√				
7.06	Umbrella Coverage	√	√				
8. Security		√	√				
8.01	Compliant with ISO 27001 Control Objectives						
8.02	All IT infrastructure & access limited to only company employees (e.g. including System Administration/Root Access)	√	√				
8.03	Physical and logical access control is a managed process (e.g. access control lists, change management, monitoring & logging)	√	√				
8.04	Only dedicated servers are utilized (e.g. no shared computing environments)	√	√				
8.05	All company employees have Federal & State background checks, annual drug testing, and are fingerprinted	√	√				
8.06	Sensitive confirmation data stored using cryptographic algorithms minimum key length 192-bit (e.g. Triple DES)	√	√				
8.07	Confirmation Data is transmitted with a minimum of 128-bit SSL using recognized 3rd Party encryption certificate (e.g. Verisign)	√	√				
8.08	Intrusion Presention System (IPS) and Intrusion Detection System (IDS) are both deployed for security	√	√				
8.09	Web Application Firewall for HTTPS traffic inspection	√	√				
8.10	Defense in Depth strategy deployed	√	√				
8.11	External Vulnerability & Penetration Testing performed by recognized 3rd Party (e.g. McAfee Secure)	√	√				
8.12	Internal Vulnerability & Penetration Testing performed using industry standard tools (e.g. AppScan, Webinspect)	√	√				
8.13	Virus protection runs on all servers	√	√				
9. Electronic Confirmation Process		√	√				
9.01	A user cannot electronically sign someone else's name on the confirmation	√	√				
9.02	User activity is logged	√	√				
10. Additional Items		√	√				
10.01	Defined Service Level Agreement with Escalation Procedures	√	√				
10.02	Review Service Agreement	√	√				
10.03	Review Privacy Policy	√	√				

In-Network – Electronic confirmation service where responding companies have proactively signed up for a confirmation service where the confirmation service guarantees the Authentication of the responding party and has verified the Authorization of the responding individual ensuring they are knowledgeable, free from bias and authorized to respond on behalf of the responding entity.

Out-of-Network – Electronic confirmation service where the auditor Authenticates the responding party and determines the Authorization of the responding individual ensuring they are knowledgeable, free from bias and authorized to respond on behalf of the responding entity.

ATTACHMENT 2

YOUR COMPANY COULD BE AT RISK… AND NOT EVEN KNOW IT

Chris Schellhorn, CEO of Capital Confirmation, Inc.

"Why, you may ask, would an employee falsely respond to an audit confirmation request?"

Being involved in a confirmation fraud will cost your company; and, the cost will be time and resources to defend your company and its name in a court of law – and in the court of public opinion. Just this year, several articles have been written warning companies about the risks of falsely responding to third-party audit confirmations.

Fraud incidents at Ahold, Kmart and Just for Feet are just some of the examples cited wherein employees at each of these companies persuaded employees at other companies to respond falsely to auditors' confirmation requests.

Motivation to Participate in Fraud

Why, you may ask, would an employee falsely respond to an audit confirmation request? Normally, external pressure leads someone to the point where they become involved in a fraud. A financial incentive has been identified as the cause in many confirmation response fraud cases reviewed by the authors of this article. The threat of losing a large business account or one's job has also been determined to play a role in this type of fraud.

For example, in the Kmart confirmation response fraud case, Kmart convinced employees (all sales and relationship managers) from at least four Fortune 1000 companies to respond falsely to an auditor's confirmation request. The key fraudsters from within Kmart threatened outside relationship managers with loss of a Kmart account if the relationship managers did not participate in the fraud. In two cases, Kmart employees threatened to transfer business to a customer's archrival if they chose not to participate in the confirmation fraud.

Historically, the primary individuals who have participated in confirmation fraud are key employees in the sales and marketing areas, or key relationship managers, for the audited company.

The SEC's Role

Companies continue to see that the SEC (Securities and Exchange Commission) files charges against the third-parties who participated in deceiving auditors with false confirmation responses, and point out the SEC's ability to pursue these participants under Rule 13b2-2. This rule gives the SEC authority to pursue anyone doing business with a public company who knew, or should have known, the information provided to the public auditors would be misleading or false. The SEC's trend in going after co-conspirators in a confirmation fraud is likely to continue.

In an attempt to control who has the ability to respond to confirmation requests, industry experts and law firms are advising companies to route the confirmations they receive to the accounting department, not through sales and marketing. Therefore, the responding company can be certain information provided to the auditors is accurate. This is a good step forward, but the question remains how to effectively accomplish this task.

Simply Centralizing the Response Won't Work

It seems obvious that a simple solution is to communicate a corporate policy to employees stating that all third-party audit confirmation requests are to be internally forwarded to a central response center. Normally, this would be the AP department, since that is where the knowledge resides regarding outstanding balances on accounts. While this is the correct department to respond, channeling the confirmation requests alone will not solve the problem.

Traditionally, auditors ask the audit client to provide a name and address to which the confirmation should be sent. And, audit clients normally provide their relationship manager's information. An employee at your company who is conspiring with the audited company to commit fraud will not forward the confirmation request to the AP department for response. The employee will, instead, sign the name of an AP staff member and send the fraudulent confirmation back to the public auditor. Instead of properly filing their fraudulent response, he/she will shred, burn, or throw away the copy of the response in an effort to hide his/her involvement.

While a central response center is a must, controlling how, and to whom, an auditor sends a confirmation is the key.

Errors, the Irrational Fear

Many authors and lawyers give stern warnings that you should consider a "No Response" policy to audit confirmations, for fear that an error will result in a legal liability for misleading a public auditor. This fear, however, is tenuous. When an auditor receives a confirmation response, the response is not simply taken at face value and booked to the audited company's financial statements. Instead, auditors compare the invoices and statements that were provided by the audited company to the confirmation response. The two documents must match before the auditor considers the confirmation response valid. If the invoice provided by the audit client and the confirmation response provided by your company do not match, the auditor will contact your company to ascertain why there is a difference. The difference could be the result of a timing issue with booked entries, an unapplied

credit, or it may simply be an error. Regardless of the cause, the auditor determines the correct number and moves on with the audit. (Note: Because of the frequency of inaccurate responses, auditors are accustomed to receiving confirmation responses that do not match the statement they have been given by the audited company.)

Fraud, the Rational Fear

Though it may seem counterintuitive, confirmation fraud occurs when the auditor compares the invoices provided by the audited company to the confirmation response and the two numbers match – because unknown to the auditor, the number on both the invoice statement and on the confirmation response is fraudulent. Auditors are thrilled when numbers agree, and this is where fraudsters take advantage of the audit confirmation process. That is why it is more important for your company to fear the rogue employee who intentionally responds falsely and why you should not be concerned about an error in the confirmation response.

Solution

Your company should consider a confirmation response solution that allows for the following:

1.) Receiving control over how, and to whom, the auditors send confirmation requests.

2.) Centralized response center, which is usually the AP department.

3.) Automatic signature of the employee who responds to the confirmation, eliminating the ability for a rogue employee to sign the name of someone else on the confirmation response.

4.) Review storage that allows you to review all responses sent out by your company (this feature in concert with the automatic signature feature serves as a deterrent to an employee who even considers falsely responding because they know the false response will be tracked back to them).

5.) Response control that ensures your confirmation response is sent back to the public auditor and not the audited client.

Capital Confirmation Inc., has created a solution, called CONFIRM™, that adheres to the above criteria. CONFIRM™, was launched in 2003 and has been used successfully by Fortune 1000 companies to control confirmation responses. The service is delivered over the Internet; so, there is no hardware to buy or software to install.

About the Authors: Chris Schellhorn, CEO of Capital Confirmation Inc. has over thirty years experience delivering technology solutions to businesses and is well equipped to work with companies in the rapidly changing regulatory environment created by Sarbanes Oxley. Brian Fox, CPA & Associate Member of the Association of Certified Fraud Examiners, is the founder of Capital Confirmation Inc. Dave Malone, Vice President of Capital Confirmation Inc., is an industry veteran in technology based process improvement services. IAPP

Every aspect of your business matters.
Including the address.

The UPS Store™

A number of advantages... all in one mailbox.

Your business address speaks volumes about who you are—and what your company is about. When you don't want to use your home address, but a P.O. box doesn't project the professional image you need, we have the solution.

Mailbox services from The UPS Store. We give you a real street address, not just a box number. And that's only the beginning. From convenient Call-in MailCheck™ to 24-hour access and much more, we invite you to discover the many services you'll receive as a mailbox holder with The UPS Store.

Mailbox services at The UPS Store offer convenience, professionalism, and an array of benefits to make your life easier.

- A real street address, not a P.O. box: A private mailing address gives your business the professional image you want.
- Package acceptance from all carriers: We'll hold your packages in a secure location for pickup at your convenience.
- Package notification: We'll let you know when a package arrives for you.
- Call-in MailCheck™: Save a trip... call to find out if you have new mail.
- Mail holding and forwarding: Just let us know when and where.*
- Receipt of oversized parcels: Large packages are no problem for The UPS Store.
- 24-hour access: Pick up your mail and postal deliveries any time, day or night.**
- Peace of mind: You no longer have to wait at home for a package delivery or risk having valuable shipments left on your doorstep.
- Convenience: The UPS Store also provides copying, binding, printing and a variety of document finishing services... so you can take care of business while you take care of the mail.

Mailbox services are provided at every one of our locations. You'll also find most of the postal products and services you need at your neighborhood The UPS Store. Ask us for details.

* Additional fees may apply.
** Available at participating locations.

The UPS Store centers are independently owned and operated by licensed franchisees of Mail Boxes Etc., Inc., an indirect subsidiary of United Parcel Service of America, Inc., a Delaware corporation. Services and hours of operation may vary by location.
©2004 United Parcel Service of America, Inc.