Confirmation.

September 13, 2010

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: PCAOB Rulemaking Docket Matter No. 028

To the PCAOB Board:

We would like to thank you for the opportunity to provide the Public Company Accounting Oversight Board (PCAOB) with our comments on the Proposed Auditing Standard Related to Confirmation and Related Amendments to PCAOB Standards (hereinafter referred to as "the Standard").

We believe that the 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 the revised Standard.

The Proposed Standard asked for answers to a list of questions and we have weighed in on all the questions we thought would be most beneficial to the PCAOB.

Questions raised by the PCAOB

1. Are the definitions included in the proposed standard sufficiently clear and appropriate?

Yes, the definitions in the proposed standard are clear and appropriate.

2. Is the objective of the proposed standard clear and appropriate?

Yes, the objective is clear and we agree with the objective as stated in the proposed standard as it is written.

5. Is the requirement in the proposed standard to confirmation cash and other relationships with financial institutions sufficiently clear and appropriate?

The requirement to confirm cash and other relationships with financial institutions is clear and appropriate. The Board should maintain this requirement in the final version. Auditors, in performing their risk evaluation, must assume a risk of fraud within the revenue recognition area. Because the

214 CENTERVIEW DRIVE • SUITE 265 • BRENTWOOD, TN 37027
PHONE: 615-844-6222 • WWW.CONFIRMATION.COM • FAX: 615-376-7971

offsetting journal entries to Revenue are either Accounts Receivable or Cash, it is appropriate to require confirmations of cash which complements the requirement to confirm accounts receivable. Doing so targets a fraud risk area that fraudsters might otherwise continue to take advantage of. Over the last several years there seems to have been more confirmation frauds involving cash, like Parmalat and HealthSouth, and it leaves one to ask if the fraudsters saw the lack of a requirement to send cash confirmations as an easier target for fraud as opposed to booking the offsetting journal entry to accounts receivable where confirmations are required and more scrutiny is therefore given.

10. Is the description with respect to the use of internal auditors in the confirmation process sufficiently clear and appropriate?

We agree with the Board that Internal auditors should not be used during the confirmation process to send or receive confirmations. In line with that, we also believe that Internal auditors should not be allowed to participate in the testing of confirmation addresses. There is a presumption that the Internal auditor can use their position to help management misdirect or circumvent the auditor's confirmation procedures which is why Internal auditors should not participate in either the sending or the receiving of confirmations. In line with that same reasoning, the auditor will also lose control of the confirmation process if the Internal auditor "validates" a falsified mailing address and the auditor in turn relies on the Internal auditor's work and sends the confirmation to the fraudulent address. Management in the ZZZZ Best fraud provided the auditors with a friend's residential mailing address and management told the auditors that the address was the address of a valid customer. Parmalat's auditors also sent a confirmation to an incorrect location at the direction of management. Had Internal auditors been been relied on by the auditors auditing either ZZZZ Best or Parmalat, the Internal auditors – with management's direction and/or coercion – could have simply "validated" the incorrect address as a valid address and the auditor's confirmation procedures would still have been circumvented no differently than if the Internal auditor had interfered with the sending or receiving of the confirmation letters. To strengthen the auditor's procedures and to reduce the opportunity for fraud, we recommend that Internal auditors be specifically excluded from testing the validity of addresses.

13. Are the procedures the auditor should perform to determine the validity of the addresses on confirmation requests sufficiently clear and appropriate?

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.

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

214 CENTERVIEW DRIVE • SUITE 265 • BRENTWOOD, TN 37027
PHONE: 615-844-6222 • WWW.CONFIRMATION.COM • FAX: 615-376-7971

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.

19. Is the requirement in the proposed standard for the auditor to investigate all exceptions in confirmation responses sufficiently clear and appropriate?

Yes, the proposed standard is clear and appropriate as to the auditor's need to investigate all exceptions in the confirmation process.

20 Are the requirements in the proposed standard related to addressing the reliability of confirmation responses sufficiently clear and appropriate?

Yes, the requirements related to addressing the reliability of confirmation responses is clear and appropriate.

21. Does the proposed standard include adequate requirements regarding electronic confirmation procedures?

Both the IAASB and the ASB state that auditors can use a service auditor's report and SysTrust reports to evaluate the three risks identified in Section 34 of the proposed standard and we believe that it would be helpful to auditors for the PCAOB's standard to provide that same level of guidance in assisting auditors in the evaluation of any electronic confirmation process.

Additionally, under Section 35 of the proposed standard, the third bullet point, we have two suggestions. The first suggestion has to do with the third sentence in that bullet point. That sentence reiterates the three risks auditors must consider when using electronic confirmations; however, these three risks are already appropriately including in Section 34 because these risks apply to all forms of electronic confirmations, intermediaries included. Because Section 34 already lists the three risks that are relisted in Section 35, and because the three risks apply to all forms of electronic confirmations and not just to intermediaries, we recommend that the third sentence in Section 35 be stricken.

The second suggestion related to Section 35 of the proposed standard under the third bullet point is that not all intermediary electronic confirmation services are the same. For example, at Confirmation.com we do not respond to the confirmation requests on behalf of the responding parties, instead, we provide the secure clearing-house for confirmations where the auditors still make the confirmation request and the companies that respond to those requests on paper are still the ones to respond electronically through Confirmation.com. We believe that what the Board is trying to address with the fourth sentence is that the auditors need to verify that the responding party has authorized the use of the intermediary for electronic confirmation and we agree with that intention. As such, we recommend that the fourth sentence read as follows:

214 CENTERVIEW DRIVE • SUITE 265 • BRENTWOOD, TN 37027
PHONE: 615-844-6222 • WWW.CONFIRMATION.COM • FAX: 615-376-7971

> "In addition, the auditor should determine whether the intermediary is an authorized service provider for the intended confirming party."

We also recommend that the Board consider providing auditors with additional supplementary material to help auditors effectively evaluate any electronic confirmation process. A sample Electronic Confirmation Security Assessment is enclosed as Attachment 1 to this document.

22. Are there risks related to the use of an intermediary that the proposed standard has not adequately addressed?

With the two changes to the third bullet point in Section 35 that we presented above in response to Question #21 we believe the risks related to intermediaries have been properly addressed.

23. The Board is interested in information about the services that an intermediary provides, specifically information about the responsibilities and obligations between the auditor and the intermediary and the intermediary and the confirming party?

Today there are over 7,000 CPA firms in more than 90 countries that use Confirmation.com for electronic confirmations and Confirmation.com is the only electronic confirmation service endorsed by the American Bankers Association (ABA) and the only one that has both a SAS 70 Type II and a SysTrust certification – which Confirmation.com has performed twice a year for both the SAS 70 Type II and SysTrust. While every third-party – other than the auditor, the client and the responder - that is involved in the confirmation process is defined as an intermediary in the confirmation process, at Confirmation.com we only have specific knowledge as to the responsibilities and obligations that we provide to both auditors and responding parties. We do have extensive knowledge about electronic confirmation risks and the fraud risks associated with various types of electronic confirmation processes from our research and sole focus on electronic audit confirmations for more than 10 years. We would be happy to meet with the Board and answer any questions that you may have regarding our patented Confirmation.com clearing-house or the research that we have on the risks related to various electronic confirmation methods.

Based on the *Guide to Electronic Confirmations* written by Gary Boomer and Brian Fox, there are principally two types of electronic confirmations provided by intermediaries: In-Network confirmations and Out-of-Network confirmations. Taken from the *Guide to Electronic Confirmations*, here are the definitions:

> **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

214 CENTERVIEW DRIVE • SUITE 265 • BRENTWOOD, TN 37027
PHONE: 615-844-6222 • WWW.CONFIRMATION.COM • FAX: 615-376-7971

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.

24. Are there risks related to the auditor's use of direct access that the proposed standard has not adequately addressed?

We agree with how the Board addressed the risks associated with direct access. In the numerous CPE classes we teach on confirmation fraud and electronic confirmations, we teach auditors how easy it is to set up a fake website and emails that look legitimate for under $500, and we believe that auditors should take extreme caution in using direct access and email for confirmations. Our research suggests that it will only be a matter of time – if it hasn't already happened – where a company being audited sets up a fake website and related fake email accounts to pose as a legitimate responding company in order to provide auditors with fraudulent confirmation responses. A website address and related emails are simply virtual real-estate that are easier and less expensive to fake and make to appear as legitimate businesses entities than doing so with real mailing addresses.

25. Should direct access be permitted as a confirmation response only if such response is received from a financial institution?

Because financial institutions have a greater fiduciary responsibility to their account holders and because it is so easy to set up fake websites and make them appear to be legitimate business entities, we do agree with the Board's suggestion that direct access be permitted as a confirmation response only for financial institutions.

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 pleased to discuss them with you.

Sincerely,

C. Brian Fox

C. Brian Fox, CPA
Founder & Chief Marketing Officer

214 CENTERVIEW DRIVE • SUITE 265 • BRENTWOOD, TN 37027
PHONE: 615-844-6222 • WWW.CONFIRMATION.COM • FAX: 615-376-7971

Confirmation.

September 13, 2010

ATTACHMENT 1
Electronic Confirmation Security Assessment

		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	√	√				

214 CENTERVIEW DRIVE • SUITE 265 • BRENTWOOD, TN 37027
PHONE: 615-844-6222 • WWW.CONFIRMATION.COM • FAX: 615-376-7971