GUIDE TO ELECTRONIC CONFIRMATIONS

A BOOMER ADVANTAGE GUIDE

Confirmation.

BOOMER
CONSULTING, INC.

Contents

Introduction

When Brian Fox speaks at conferences, he likes to play a recorded session of messages received on their customer support hotline. Staff auditors mistakenly believe their company is a bank, and call them to follow up on the paper-based confirmations they mailed out weeks ago that were never returned.

“I’m calling to follow up … We faxed our third request last month … We really need this to finish up our audit. Could you please, PLEASE … sixth time I’ve called … ”

What comes through most vividly is the frustration. We’ve all been there. You’re a staff auditor, and it’s bad enough you have to spend time stuffing envelopes with confirmations. Now, to add insult to injury, you’re making frantic phone calls at the eleventh hour, leaving voice messages, trying to track down a single piece of paper.

There is a Better Way

Paper-based confirmations have been with us since the beginning of the audit profession 130 years ago. Through numerous changes in technology, business practices and auditing rules and regulations, the paper and mail system for making direct contact with third parties has endured. In the process, it has become increasingly outdated, less efficient and less secure every year.

But there is a better way!

In 2007, those who set auditing standards approved the use of electronic confirmations as a much-needed replacement to the traditional paper and mail-based process. In order to preserve the integrity of the confirmation process, they carefully defined what is and is not an electronic confirmation as well as the steps auditors must take to ensure a confirmation is reliable audit evidence.

Starting October 1, 2008, Bank of America required all of its customers’ external auditors to use electronic confirmations through Confirmation.com.

There’s good reason why stewards of the profession want to encourage the use of electronic confirmations. You can’t do a 21st century audit using 19th century technology.

The auditors of Parmalat and CF FOODs recently discovered this the hard way. The management of both companies concealed massive frauds by compromising the auditor's paper-based confirmation process. A properly designed, electronic confirmation would have prevented this cover-up.

Academic research shows that electronic confirmations produce a much lower error rate than the paper alternative. Similar research reveals that replacing paper-based confirmations with electronic confirmations leads to tremendous audit efficiencies. Some in the profession have declared the adoption of electronic confirmations to be a "foregone conclusion," and with leading banks now requiring auditors to use electronic confirmations, we expect the rate of adoption to continue its rapid increase.

In this publication you'll learn why and how to make the switch.

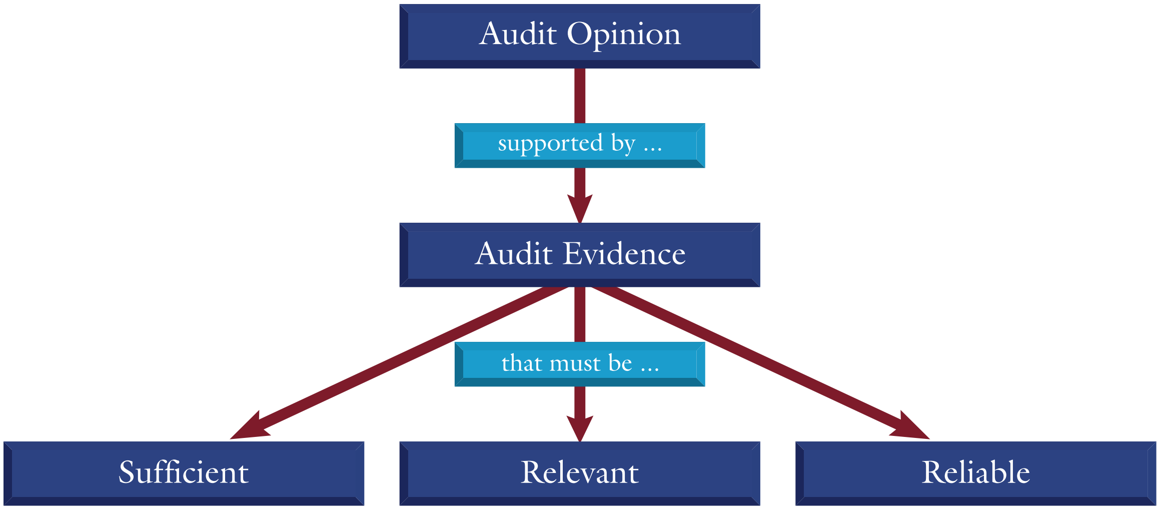
L. Gary Boomer, CPA.CITP
C. Brian Fox, CPA

The Confirmation Process

Independent auditors are required to obtain "sufficient appropriate audit evidence" to support their opinion on the financial statements.

"Sufficient" relates to the quantity of audit evidence obtained. Has the auditor gathered enough?

"Appropriate" relates to relevance and reliability.

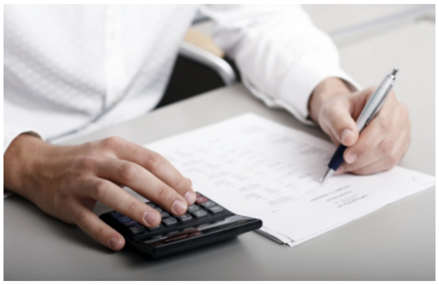


All three baseline elements must be in place for the auditor to fulfill his responsibilities. It doesn't matter how much audit evidence the auditor obtains; if that evidence isn't reliable, then the audit quality has been compromised.

Questions regarding the use of confirmations relate to reliability. Are electronic confirmations as reliable as paper confirmations? In fact, evidence suggests that electronic confirmations are more reliable than paper.

It doesn't matter how much evidence the auditor obtains; if that evidence isn't reliable, then the audit quality has been compromised.

Building a Reliable Confirmation Process



The stewardship of audit quality rests upon a variety of standards setting organizations. The rules for auditor performance are set by the AICPA (audits of non-public companies), the PCAOB (audits of public companies) and the IAASB (international audits).

Although the language of the three standards may vary, fundamentally they all agree on the four tenets of performing a proper confirmation.

- Communicate directly with and receive an active response from the third party
- Exercise professional skepticism
- Identify and validate a respondent who is free from bias and authorized to respond
- Maintain control of the confirmation process

Only by following these four tenets can the auditor ensure that the confirmation he or she receives is meaningful.

> ***"The auditor should consider whether there is sufficient basis for concluding that a confirmation request is being sent to a valid respondent from whom a response will be meaningful and provide competent evidential matter. If there is not a sufficient basis for that conclusion, the confirmation process is useless."***
>
> ***- Doug Carmichael Former Chief Auditor of the PCAOB***

How Reliable Are Paper-Based Confirmations?

Many auditors believe that simply receiving a signed response to a confirmation request provides the proper audit evidence. This is not so. Without a sufficient basis for concluding that the confirmation has been signed by a valid respondent, the confirmation lacks the high level of reliability necessary to constitute competent audit evidence.

The following fraud schemes identify the fallacy in this belief that a signed confirmation is all that is required. These examples serve as notice to auditors that, unless they apply the four tenets of a proper confirmation, they are not following the requirements of a Generally Accepted Auditing Standards (GAAS) audit.

Confirmation Fraud Schemes

Client provides false contact information

In a survey of over 150 accounting firms, researchers discovered that almost all of the mailing addresses for confirmations are provided to the auditor by the client or taken directly from client-provided bank statements.

To thwart the paper confirmation process, a dishonest client simply uses a scanning machine to manipulate or even create a false statement and provides incorrect contact information in an effort to defraud the auditor. This appears to be one of the techniques employed by Parmalat executives, who committed that company's almost $5 billion audit confirmation fraud.

What an auditor must be aware of is that using today's technology, a dishonest client can easily adjust the balance on a statement and change the contact information to be a friend's address, phone/fax number and email. Fraudsters do not have to use a friend's address as Mark Morze, the former CFO of ZZZZ Best Carpet Cleaning, did. Instead, they can use a UPS Store mail account, which is presented as a real street address and not a P.O. Box address. Phone numbers can be prepaid cell phone numbers or a FedEx Office store fax number. Email addresses can have extensions that closely resemble a legitimate client's email extension.

In an attempt to fool an auditor, a fraudster with $200 can easily establish three sources of legitimate contact information (address, fax and phone lines) at any executive office suite offering those services. In some cases they can establish an email account, and a receptionist will answer the phone using the name of whatever company the fraudster asks.

Ongoing improvements in scanning and printing capabilities will continue to make these types of activities that much more difficult to detect, even as today's regulatory scrutiny and public expectations demand that auditors catch such frauds.

Client provides the contact name

When auditors do spend the time and resources to independently validate the address, phone/fax number or email for a financial institution, they often do not independently know or validate an individual clerk within the confirming entity.

To circumvent the paper confirmation process when auditors validate contact information, a fraudster simply provides the correct mailing address along with phone and fax numbers, but has a co-conspirator within that organization. This dishonest associate may be a friend or relative who fraudulently fills out the paper confirmation and may even sign it with the name of another employee in order to hide involvement from the auditor.

> ***Maintaining control [of the confirmation process] includes performing procedures to verify that the confirmation is being directed to the intended recipient. ASB Auditing Interpretation (AU 9330.04)***

In one case, the Director of Apparel Sales for Adidas America intentionally provided auditors false information because of his motivation for future sales to his client. Just for Feet's auditors sent an accounts receivable confirmation directly to the Adidas Director of Sales, who confirmed $2.2 million in receivables due when in reality Adidas only owed Just for Feet approximately $40,000.

This one event exposed both companies, every individual involved in the audit and the audit firm itself to a huge liability.

Client influences the confirmation process

With a little effort, a dishonest client can create third-party credentials that closely resemble legitimate credentials. For example, an inexpensive fake website, displayed as if it were for a legitimate financial institution, can be quickly created to provide illegitimate contact information.

In two separate cases during 2004, thieves created fake U.S. Bank and Union Planters Bank websites to steal important online banking information from customers. These fraudsters were even able to highjack and use an email with the real bank email extension to direct customers to the fake websites. If the bank's own customers could not distinguish a real website from the fake, how can those of us who might see it once a year determine whether it is real or fake?

The fake signature of a legitimate employee from the bank was used by Parmalat executives to "verify" almost $5 billion.

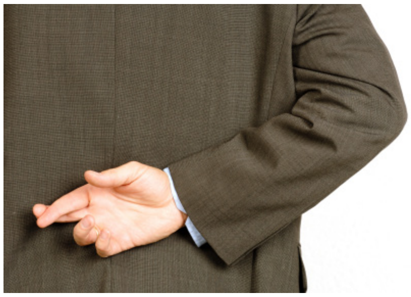
Signature verification is impracticable

Given all the possible loopholes to circumvent the paper confirmation process, it is not practical to think an auditor has the resources to validate the signature of the person who responded to a confirmation request.

In today's environment, unfortunately, a cursory review of a signature no longer provides a safeguard from liability when presented to a jury that does not understand why a signature was not validated and does not appreciate the challenges associated with checking the validity of a signature on a paper confirmation. Juries do not understand the tremendous resources that are required to accomplish such an ongoing task.

Fraudsters know that the type of effort required to validate the signature of the confirming entity is rarely used proactively to prevent fraud. Enormous costs are involved, and it is only used once a potential fraud is identified. At this stage it could be too late to eliminate the liability associated with the fraud exposure.

With this in mind, fraudsters falsely responding to a confirmation request simply scribble the signature of anyone, to include the signature of a legitimate signatory, to effectively validate a paper confirmation response.



A fake signature was used to perpetrate the Parmalat fraud. Believing that the auditors might attempt to validate the employment of the person who signed the confirmation, the fake signature of a legitimate employee from the bank was used by Parmalat executives to "verify" almost $5 billion.

Cracking Down on Fraud Schemes

In response to these and similar fraud schemes, the Auditing Standards Board issued an interpretation in 2008 that more clearly defined the auditor's responsibilities when using confirmations to obtain audit evidence.

On all audits, the auditor should consider the reliability of the information obtained through the confirmation process. To do that, he or she must assess the risks that:

- The information provided in the confirmation may not be from an authentic source
- The person responding to the confirmation may not be knowledgeable about the information being confirmed
- The integrity of the information may have been compromised

"The existing paper-based confirmation process has exposed auditors to substantial legal liability over the past two decades."

George Aldhizer and James Cashell "Automating the Confirmation Process" The CPA Journal ; April, 2006

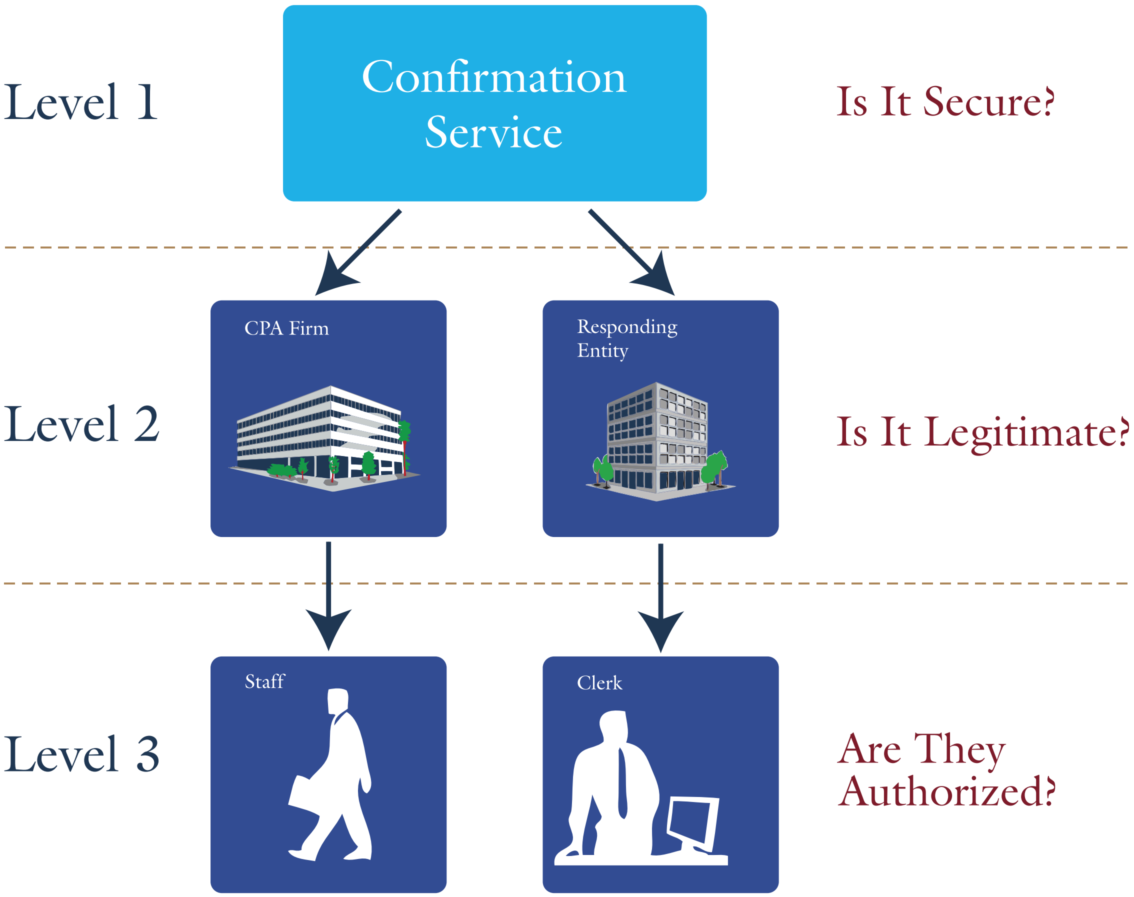
Requirements of an Electronic Confirmation

To ensure the reliability of electronic confirmations, the Auditing Standards Board states that electronic confirmations can be considered reliable audit evidence if the auditor is satisfied that:

- The electronic confirmation process is secure and properly controlled
- The information obtained is a direct communication in response to a request
- The information is obtained from a third party who is the intended respondent (See AU 9330.05)

Ensuring Reliability

The diagram below illustrates the relationship between the auditor and the responder to an electronic confirmation request. It indicates that authentication, validation and security are required at three different levels.



- **Individual audit staff and responders.** Authentication and validation are required to establish the identity of the auditor making the request and the person responding to it. Both parties will want to ask:
    - » Is the person I'm communicating with who he or she claims?
    - » Is that person authorized to communicate with me?
    - » Is the person responding to the confirmation qualified and authorized to respond?

- **Audit firm and responding entity.** Both parties will want assurance that the entity with which they are dealing is legitimate.
- **Communication channel.** Both parties need to know that they are communicating information through a secure service.

Authentication and Validation

A reliable electronic confirmation process means that the auditor has assurance he or she is sending the confirmation request to the intended recipient. At the entity level, the auditor should determine that the confirming entity is a legitimate enterprise by validating information like:

- Primary mailing address
- Physical address
- Website
- Telephone number

At the individual level, the auditor should verify the identity of the respondent, obtain some assurance that he or she is qualified and authorized to respond, and has access to the necessary data for a response.

The responding organization also needs assurance that the auditor is who he or she claims to be and has the client's permission to request the confirmation. For example, the responder will want to verify the audit firm's:

- Mailing address
- Website
- CPA license
- Telephone number

Some electronic confirmation providers will have a network of validated responders. Establishing such a network requires the provider to take steps to authenticate and authorize both the entity and the individual responders to the confirmation request.

Data Security

Confirmations contain highly sensitive information such as the audit client's bank account number, loan number and bank balances. For that reason, an electronic confirmation process must have controls that create a secure communication channel between the auditor and the confirmation responder. Such controls typically include elements such as:

- Passwords for individual participants
- Data encryption
- Firewalls that protect the system from unauthorized intrusion
- Intrusion detection and prevention systems

Ensuring the Security of the Electronic Confirmation Platform

Both responders and auditors demand a high level of security from any electronic confirmation platform. Responders such as banks rightly view the platform as an extension of their own IT system, and they want to make sure that the overall security of the system retains its integrity. It is common for banks that use an electronic confirmation process to perform periodic in-depth security reviews of the electronic confirmation provider's IT system.

> ***"An electronic confirmation process that creates a secure confirmation environment may mitigate the risks of human intervention and misdirection. The key lies in the process or mechanism used by the auditor and the respondent to minimize the possibility that the results will be compromised because of interception, alteration or fraud with respect to the confirmation."***
>
> ***AICPA Updated Practice Alert 03-1, Audit Confirmations***

Likewise, auditors should request a SAS 70 Type II and a SysTrust review as part of their required security assessment of the electronic confirmation provider.

These Techniques Fail the Test

While auditors are finding alternatives to traditional paper-based confirmations, they should ensure these methods meet the requirements of the auditing standards. The Auditing Standards Board has weighed in on the two most prevalent non-paper-based confirmation techniques and determined that they do NOT meet their requirements.

- Confirmations sent or received via e-mail are typically a less reliable form of audit evidence, because it is difficult if not impossible for the auditor to establish the origin of the email or determine whether the respondent is knowledgeable about the matters being confirmed. (See AU 9330.03)
- An online inquiry of a third party's database does not constitute a confirmation, but rather an alternative procedure. The reason is that a confirmation from a third party requires an active response from that third party, and an auditor looking up information on a database does not include the active involvement of the third party respondents. (AICPA Update Practice Alert 03-1)

In-Network Confirmation and an Out-of-Network Confirmation

Not all electronic confirmation processes are created equal. In order to select an appropriate solution, the auditor must understand the differences in functionality, the requirements of the auditor, and the response rates for the two main types of electronic confirmation processes, the "in-network" process and the "out-of-network" process.

Both processes should include security measures to ensure data integrity. Where they differ is in the authentication and verification of responders to the confirmation request.

In-Network – Some electronic confirmation providers have established a network of participating banks and other responding entities. Establishing such networks requires the provider to take steps to authenticate and authorize both the entity and the individual responders to the confirmation request. The auditor can rely on the in-network solution and is not required to perform additional authentication and authorization procedures.

Out-of-Network – An out-of-network electronic confirmation platform does not include authentication and authorization of the respondent. The provider of an out-of-network service has performed no procedures to validate either the entity or the individual responding to the confirmation. That responsibility falls to the auditor who is required to determine that the confirmation was sent to the proper source and that the respondent was authorized to respond.

In general, in-network confirmations are more secure and efficient than out-of-network confirmations. Expect to pay more for this added protection and convenience. The following table summarizes the differences between in-network and out-of-network confirmation processes.

Requirements for Audit Confirmations

		Requirements	Electronic Confirmations		Alternative Procedures* (Email & Direct Access)	Paper Confirmations
			In-Network	Out-of-Network		
SAS 67/AU 330		Control the process	Electronic confirmation provider	Electronic confirmation provider	Auditor	Auditor
		Knowledgeable and free from bias respondent	Electronic confirmation provider	Auditor	Auditor	Auditor
		Determine responding individual is authorized to respond	Electronic confirmation provider	Auditor	Auditor	Auditor
	Practice Alert 2003-01	Establish direct communication with respondent	Electronic confirmation provider	Electronic confirmation provider	Auditor	Auditor
Interpretation 9330		Maintain integrity of the data and data transmission	Electronic confirmation provider	Electronic confirmation provider	Auditor	Auditor
		Authenticate responding entity	Electronic confirmation provider	Auditor	Auditor	Auditor
		SAS 70 Type II and SysTrust certification	Electronic confirmation provider	Electronic confirmation provider	Auditor	Auditor
		Website authentication	Electronic confirmation provider	Electronic confirmation provider	Auditor	Auditor

Comparative Results

Efficiency Statistics	Electronic Confirmations		Electronic Alternative Procedures	Paper Confirmations
	In-Network	Out-of-Network		
Response rates	100%	50 - 60%	50-60%	71%
Average turnaround times	1.08 days	3 - 5 days	3-5 days	21 - 40 days
Reconfirmation rates	9.7%	20 - 25%	20-43%	43%

Pros and Cons

Pros and Cons	Electronic Confirmations		Electronic Alternative Procedures	Paper Confirmations
	In-Network	Out-of-Network		
Pros	Reduces auditor's exposure to fraud	Efficient	Faster than paper	Same results for the last 80 years
	Greatest efficiency			
Cons	Auditor must assess the design and operating effectiveness of controls. SysTrust and SAS 70 Type II may assist the auditor in performing their assessment.	Auditor must assess the design and operating effectiveness of controls. SysTrust and SAS 70 Type II may assist the auditor in performing their assessment.	Not a valid audit confirmation	Slowest turnaround time
		Auditor must perform procedures to authorize and authenticate responding entity and individual	Difficult to assess and validate the respondent	High error rate
			High exposure to fraud	High exposure to fraud

* Electronic alternative procedures like email and direct access to a database, while they may provide audit evidence, they are not a confirmation for audit and attest purposes.

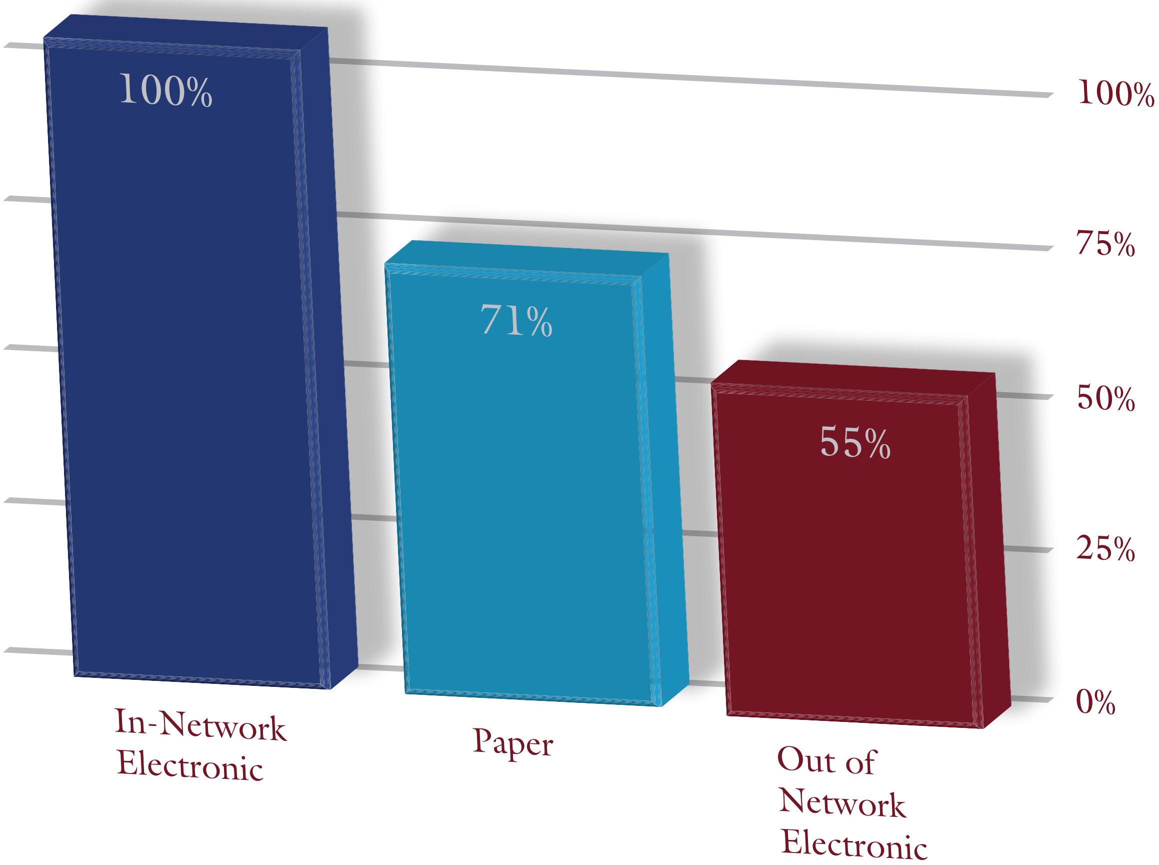
Driving Audit Efficiency

The use of electronic confirmations leads to a more efficient audit process. Research indicates that compared to paper-based confirmations, electronic confirmations result in dramatic improvements in three key audit efficiency metrics: response rates, turnaround times and reconfirmation rates.

Confirmation Response Rates

Non-responses to confirmation requests require the auditor to perform alternative procedures. Not only are alternative procedures time consuming, they are a less reliable form of audit evidence.

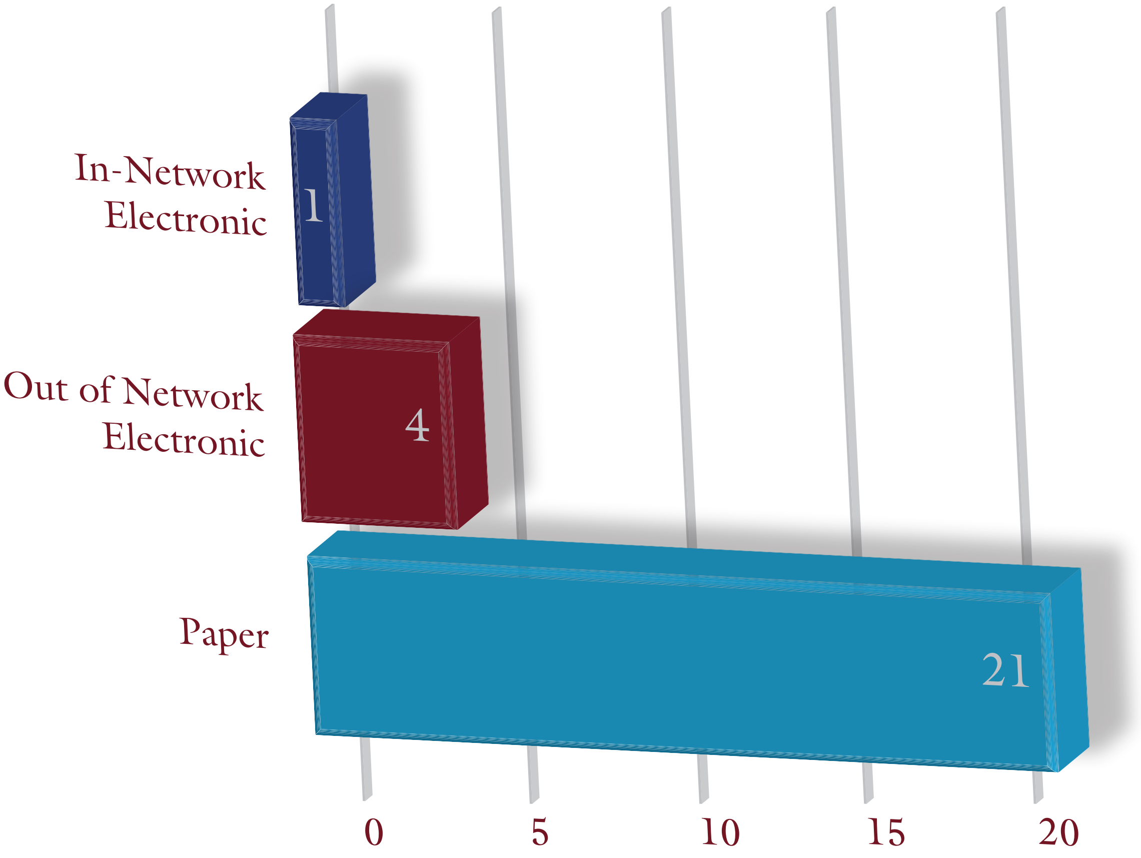
Response Rates



Turnaround Times

Slow turnaround times require the auditor to spend more time following up with third parties to get a response. Faster turnaround also gives the auditor more time to follow up on discrepancies and exceptions.

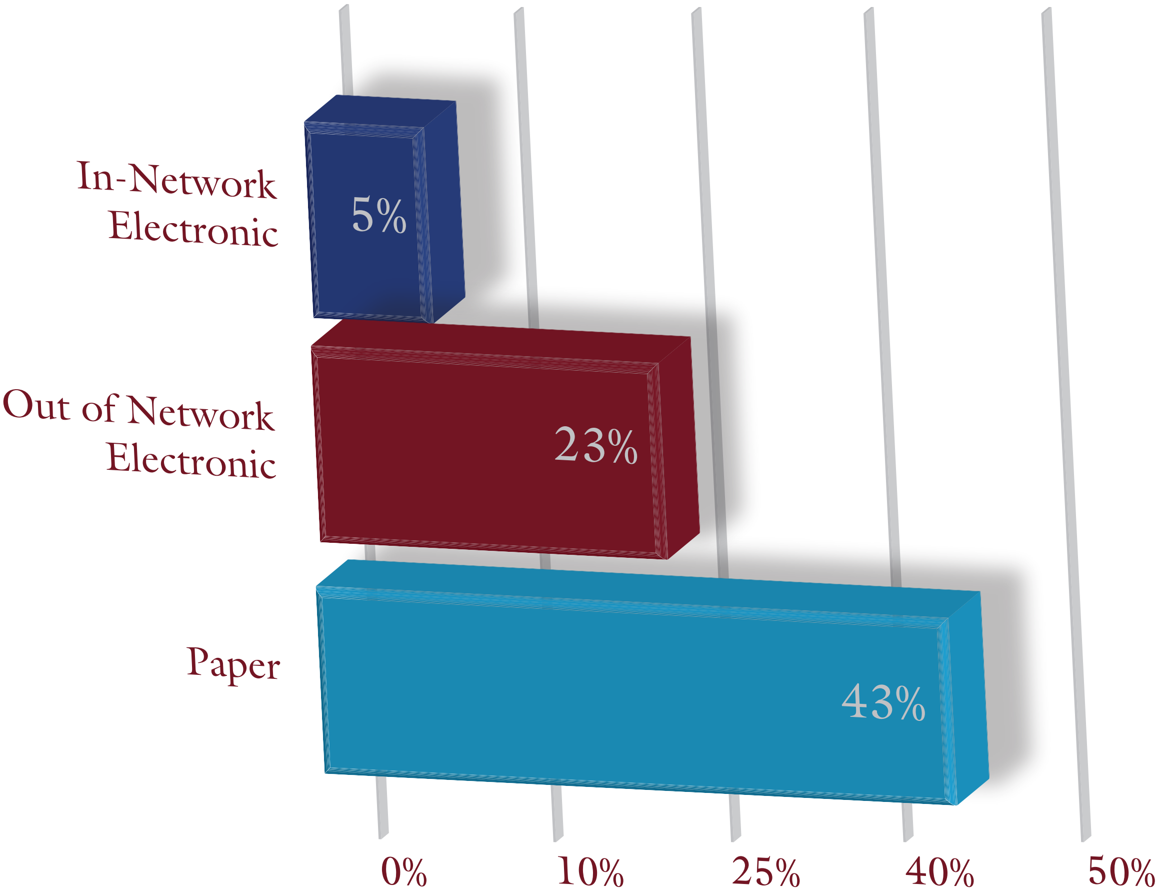
Average Turnaround Time (in Days)



Error Rates

It is not uncommon for responders to confirm incorrect information or otherwise make errors in the confirmations they return to the auditors. When the responder makes an error, the auditor must either reconfirm with the responder or perform additional procedures to gather the audit evidence originally sought through confirmation.

Reconfirmation Rates



Centralize the Confirmation Process

Many CPA firms have secured audit efficiencies by centralizing their confirmation efforts. They assign one person in the firm to coordinate the sending and receiving of confirmations for all audit engagements, and individual audit teams work directly with that one individual.

An electronic confirmation process is ideal for firms that use or are looking to implement a centralized confirmation process.

Paperless Audits

Many firms have adopted paperless auditing to increase efficiency. Most paperless audit solutions like CaseWare Working Papers, CCH's ProSystem fx® Engagement and Thomson Reuters Engagement CS™ now integrate directly with Confirmation.com, an electronic confirmation service. This integrated solution drives further efficiencies, because audits no longer require manual intervention to manage the confirmation process or to scan and upload paper-based confirmation responses.

The True Cost of Paper vs. Electronic

Consider one staff member at a typical CPA firm. Suppose over the course of her busy season she works on six different audits and audits a total of 40 bank accounts. How much time would she spend on a paper-based confirmation process, and what would it take her to do it electronically? Assume the following:

	In-Network Electronic		Out-of-Network Electronic		Paper-Based	
	Assumption	Total	Assumption	Total	Assumption	Total
Prepare and send confirmations, log-in results	10 mins per job; 6 jobs	1 hr.	20 mins per job; 6 jobs	2 hrs.	30 mins per job; 6 jobs	3 hrs.
Reconfirm non-responses	5% reconfirm rate; 40 original confirmations; 2 confirms to reconfirm	0.1 hr.	25% reconfirm rate; 40 original confirmations; 10 confirms to reconfirm	0.25 hr.	40% reconfirm rate; 40 original confirmations; 16 confirms to reconfirm	1 hr.

Alternative procedures for non-responses	0% non-responses	0 hrs.	40% non-responses;
			40 original confirmations;
			16 alternative procedures at 10 minutes per
				2.5 hrs.	29% non-responses;
					40 original confirmations;
					12 alternative procedures at 10 minutes per
						2 hrs.

General inefficiency caused by excessive delays in response	All responses received in one business day	0 hrs.	5 minutes per job; 6 jobs	0.5 hr.	20 minutes per job; 6 jobs	2 hrs.
Total Time		1.1 hrs.		5.25 hrs.		8 hrs.
Time Savings		**6.9 hrs.**		**2.75 hrs.**		**0 hrs.**

A paper-based, bank confirmation effort might take a day for just one staff person over the course of a busy season; an electronic confirmation process requires a little more than an hour. What would seven hours per staff person do for your firm's realization?

With over 500 auditors located in 10 offices, The Reznick Group is one of the largest accounting firms in the nation. As a way to drive audit efficiency and address fraud risk, several years ago the firm decided to make the switch to electronic confirmations. Rather than replace paper confirmations nationwide, the firm decided to pilot electronic confirmations starting in its Atlanta office.

Centralized Confirmation Effort Provides Even Greater Efficiency

Previously, each audit team had been responsible for sending and receiving the confirmations for its client. Together with the switch to electronic confirmations, the firm felt that even more efficiencies could be realized if it centralized its confirmation effort.

Responsibility for managing the confirmation process was transferred from individual audit teams to two paraprofessionals in the Atlanta office. The two of them received personalized training from Capital Confirmation on how to operate its system, and the electronic confirmation process was up and running.

Paraprofessional John Huynh estimates that each busy season he sends and receives thousands of bank confirmations. "Before, you never saw how much work it really took because confirmations weren't centralized in one place. Now I can see it all. It's a huge effort."

John Pushes a Button

The Confirmation.com system stores audit client and bank data in its system, which makes it easy to reprise each client's confirmation requests from year-to-year. Once the audit team begins its fieldwork they make any necessary changes to the previous year's data, John pushes a button, and the confirmations are sent.

"I can literally get a response within an hour," says John. "It goes right to the bank's queue, and they have to give me some kind of response. It doesn't get lost."

Before using electronic confirmations, each audit team would send out paper confirmations and wouldn't expect an answer back for several weeks. The time and aggravation spent following up on confirmation requests was significant.

Continuous Improvement

Like other Confirmation.com clients, The Reznick Group paraprofessionals provide valuable insight into future enhancements to the system. Clark Hudgins, Vice President Accounting Profession, routinely gathers input from clients on how to improve the user experience.

Says John, "Clark will call and ask 'hey, John, what do you think of this?' and I tell him." Many of these user suggestions eventually become system upgrades.

Nationwide Roll Out

Because of the success of the Atlanta office pilot, The Reznick Group now uses electronic confirmations on all audits nationwide. They've created even more efficiency by following the lead set by the Atlanta office to centralize all audit confirmations.

Greg Shelton, CPA is a sole practitioner in Bartlett, Tennessee. He has four audit clients and sends out about 20 confirmations each year. He has been an auditor for 25 years and was one of the first users of electronic confirmations.

When he first made the switch from paper, he was surprised that he was the only sole practitioner or small local firm in the list of users. But the advantages of using electronic confirmations can be realized by any firm, regardless of their size.

Just Get It Done

When he first learned of electronic confirmations, Greg immediately recognized the benefits of making the switch from paper. “I hate waiting three or four weeks to get a confirm from a bank. I like to just get it done. Now I can get a confirm returned from the bank before I even start fieldwork,” says Greg.

Once a company is set up on the Confirmation.com system, sending confirmations in subsequent years is a five minute task: change the date and the auditor is done with a single click of his mouse.

Confirming Liabilities

Greg is quick to point out that a standard bank confirmation does more than simply confirm bank balances, it also gathers information about loans, letters of credit and other liabilities. Obtaining this information is crucial especially when auditing a small business, where many times the liability may not appear on the books.

“You have situations where a loan was obtained to purchase equipment, and the cash never flowed through the company. Or the company got a line of credit and the owner took a draw directly that was never recorded on the company’s books.” Using electronic confirmations allows the auditor to identify those unrecorded liabilities immediately, rather than waiting several weeks (sometimes after the conclusion of fieldwork) to receive a paper confirmation.

Pass Through the Cost

Greg passes through the cost of the electronic confirmation service directly to his clients. Even though his clients are billed about $100 on each audit, overall they end up saving money because Greg spends essentially no time on the confirmation effort. “It’s a win-win situation because it saves money for the client and improves efficiency for my business,” says Greg.

A No-Brainer

Greg is sold on electronic confirmations. Like anything else, there’s a learning curve, but with electronic confirmations that curve isn’t too steep. “Once you get past your first one, it’s a breeze,” he says. “It’s really a no-brainer.”

There’s only one downside to his switch to electronic confirmations. Greg has a stack of paper bank confirmations he ordered eight years ago taking up space in his storage cabinet. If you see them show up on e-Bay, you’ll know why.

One Page Plan

Strategic Objective	Measurement	Strategy/Initiative	Due Date Time Frame	Assigned To
1. Research, analyze the available options.	• Develop a short list	• Complete the attached Electronic Confirmation Security Assessment for each option	2 weeks	Electronic Confirmation Task Force
2. Select a secure electronic confirmation service and determine implementation method - Centralized or Decentralized.	• Electronic confirmation service selected	• Centralized implementation is where an office centralizes the confirmation responsibility to a paraprofessional or administrative assistant within the firm • Decentralized implementation is where each engagement team manages their own confirmations	1 week	CEO/Electronic Confirmation Task Force
3. Implement a secure electronic confirmation service.	• Electronic confirmation service implemented	1. Communicate to Partners, Managers and Key Stake holders the decision to adopt electronic confirmations and ensure they will support the new direction 2. Provide an overview of the service to entire firm (can be done via newsletter, conference call, meeting) 3. Have the users go through the online narrated training tutorial 4. With Centralized implementations, include a short training on the roles and responsibilities of the engagement team (newsletter, conference call, staff meeting)	1 week	Electronic Confirmation Task Force
4. Improve customer relationships	• Communicate the improved process to your clients	• Communication to clients can be done at the beginning of each audit. Explain to them the new process, their role, and the improvements in security and efficiency with electronic audit confirmations.	Ongoing	All Engagement Teams
5. Monitor the process and adoption	1. Percentage of firm and audits adhering to the new process 2. Turnaround times 3. Response rates 4. Reconfirmation rates	• Develop deadline for firm wide adoption • Include online narrated training tutorial for electronic confirmations in new hire training	Ongoing	CIO/Electronic Confirmation Task Force

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 & Environmental 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)	√	√				

		Required for		Reviewed, Appropriate & In Place			
		In-Network	Out-of-Network	Yes	No	Notes	Reviewer
4. Website Authentication		√	√				
4.01	Extended Validation SSL Certification by recognized 3rd Party (e.g. VeriSign)	√	√				
5. Disaster 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	√	√				

		Required for		Reviewed, Appropriate & In Place			
		In-Network	Out-of-Network	Yes	No	Notes	Reviewer
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 Presentation 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	√	√				

About the Authors

L Gary Boomer is CEO of Boomer Consulting, Inc., an organization that provides planning and consulting services to leading firms in the accounting industry. Boomer strategies chart a transformation roadmap that results in increased revenue, goal-oriented personnel and business growth.

Gary is recognized in the accounting profession as the leading authority on technology and firm management. For the past twelve years, he has been named by *Accounting Today* as one of the 100 most influential people in accounting. He consults and speaks around the globe on management and technology related topics including strategic and technology planning, compensation and developing a training/learning culture. He acts as a planning facilitator, provides coaching and serves on many advisory boards.

As a member of The Advisory Board, Gary collaborates in a partnership of esteemed accounting firm consultants. He is the past chairman of the AICPA's Information Technology Executive Committee and a member of the AICPA Council. He has also served on the AICPA's Academic and Career Development Executive Committee and the ACUTE Board of Directors. Gary currently serves as the President of the Kansas Society of CPAs and on the accounting advisory board at Kansas State University.

About the Authors

As the founder of Capital Confirmation, Inc. (CCI), **Brian Fox** has been the driving force for CCI's effective response to rapidly evolving accounting industry standards. Brian previously worked in Audit for Ernst & Young LLP and Mergers and Acquisitions for PricewaterhouseCoopers LLP. Early on as a staff and senior accountant, Brian identified the inefficiencies and potential for fraud inherent in the current confirmation process. His vision resulted in the creation of a new, innovative and award-winning patented process, which today places CCI at the forefront of accounting industry service providers.

In 2006 Brian was named by *The CPA Technology Advisor* as one of the accounting profession's inaugural "40 Under 40". Brian is a member of the AICPA and The Tennessee Society of CPAs, where he sits on the Accounting and Auditing Symposium Committee for the Society. He has authored numerous articles on fraud, and his writing and quotes have appeared in *The CPA Journal*, *New York Times*, *The CPA Technology Advisor*, *AP Matters*, *The Auditor's Report*, *The International Herald Tribune* and many other professional publications. He also teaches continuing professional education classes on financial fraud and is often a guest lecturer at professional conferences and business schools.

Brian completed his MBA at Vanderbilt University with a dual concentration in Finance and Electronic Commerce and received a BBA in Accounting from Southern Methodist University's Cox Business School.

About Confirmation.com

Confirmation.

Capital Confirmation, Inc. provides secure electronic confirmation services for auditors, those responding to confirmation requests and their shared client. Capital Confirmation's patented Confirmation.com service minimizes fraud and brings efficiency to the audit confirmation process.

This easy to use, web-based service guarantees responses and has an average turnaround time of less than two business days. Using Confirmation.com, auditors will spend less time tracking down confirmations and have more time to spend on other critical engagement activities.

Confirmation.com provides both In-Network and Out-of-Network delivery options, allowing you to send confirmation requests to 100 percent of banks and other responding companies worldwide. For the greatest level of efficiency and security, Confirmation.com's In-Network application uses a unique Authentication and Authorization process to validate the authenticity and authorization of each user. Capital Confirmation also receives a SAS 70 Type II and SysTrust certification every six months to ensure that the highest level of security standards are used for privacy and data integrity.

As a result, Confirmation.com received the coveted *CPA Technology Advisor*'s Tax & Accounting Technology Innovation award for 2009 as well as the 2009 Reader's Choice Award. That's why several hundred responding companies and over 6,000 accounting firms in 52 countries trust Confirmation.com for their audit confirmation needs.

VeriSign Secured VERIFY

SAS70 Completed Type II Audit

SysTrust

TRUSTe EU SAFE HARBOR

The Boomer Advantage Guides™

GUIDE TO HUMAN CAPITAL ATTRACTION & RETENTION
GUIDE TO TRAINING & LEARNING
GUIDE TO SUCCESSION PLANNING
GUIDE TO STRATEGIC PLANNING
GUIDE TO OUTSOURCING
GUIDE TO PARTNER COMPENSATION
GUIDE TO SELECTING A MANAGING PARTNER
GUIDE TO PAPERLESS TRANSITION
GUIDE TO PERFORMANCE MANAGEMENT
GUIDE TO MOBILE DATA SECURITY & PRIVACY
GUIDE TO RISK MANAGEMENT IN THE DIGITAL WORLD
GUIDE TO CLIENT FILTERING
GUIDE TO DEVELOPING MANAGERS
GUIDE TO IMPLEMENTING CRM IN YOUR FIRM
GUIDE TO BUSINESS CONTINUATION
GUIDE TO ELECTRONIC CONFIRMATIONS
GUIDE TO PRICING FOR VALUE
A BOOMER ADVANTAGE GUIDE
Confirmation.
BOOMER CONSULTING, INC.

Order your copies today at www.boomer.com

BOOMER
CONSULTING, INC.

Think. Plan. Grow!

This publication is not a substitute for the advice of your advisors, personal and professional.

If you would like further information about The Boomer Technology Circles or other Boomer Consulting, Inc. services and products, please visit our website

www.boomer.com

© 2010 Boomer Consulting, Inc. All Rights Reserved. No part of this publication may be reproduced in any form, or by any means whatsoever, without the written permission from the publisher; except in the case of brief quotations embodied in critical articles and reviews.