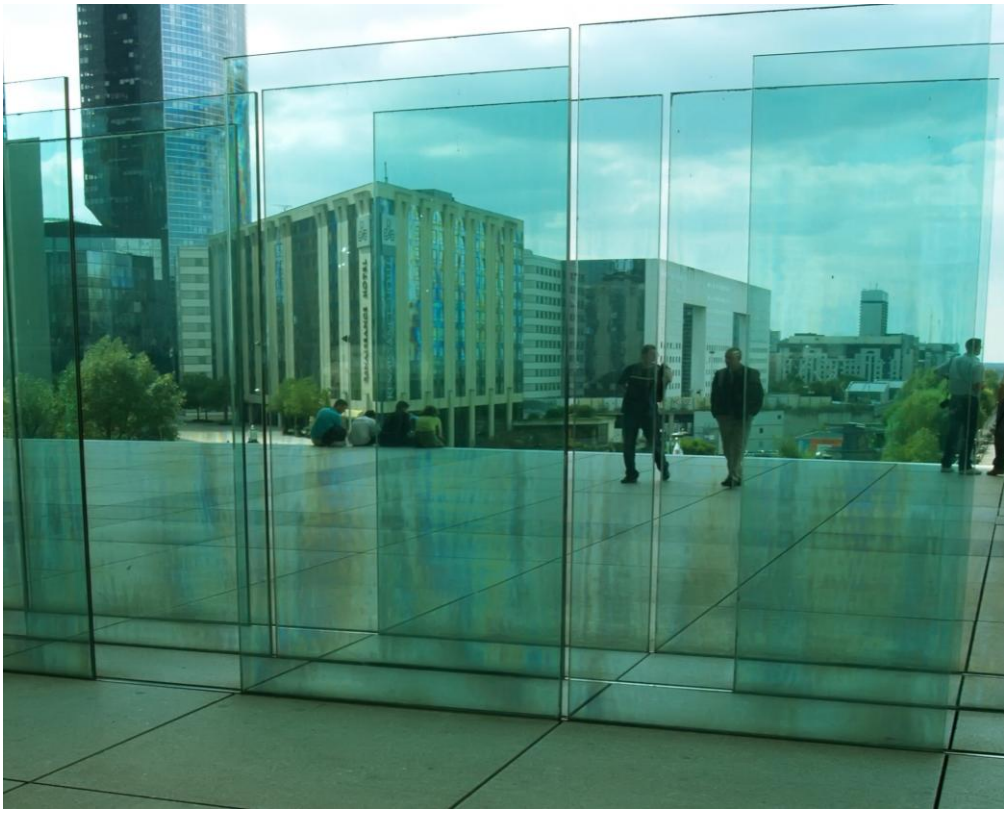
What Every Fraudster Knows…

What we need to know about confirmation fraud



Confirmation.

Table of Contents

Introduction

Whether you request them or respond to them, until recently very few people actually focused on confirmations. Confirmation fraud is now a very hot topic but was once considered a simple, relatively low risk procedure requiring little effort and even less thought. This oversight has been identified by fraudsters and is turning out to be a tremendous challenge for both the requestor and the responder, bringing with it a unique set of fraud schemes that need to be understood by all who participate in the process.

The Parmalat fraud is now the largest cash and investment confirmation fraud ever recorded, but this is not the first time this fraud scheme has been used to falsify financial reports. Nor are confirmation frauds unique to large or small clients. As the 2002 ACFE Report to the Nation highlights, fraud occurs in companies of all sizes and is perpetrated by the lowest employee to top executives. What is needed is opportunity. Confirmations are seen by fraudsters as that opportunity.

In the 1980's, a small company founded by a high school student grew into the highly glamorized story of ZZZZ Best Carpet Cleaning. It highlighted how a single executive could circumvent the paper confirmation process to provide auditors the paper evidence needed to take a company public and bilk banks and investors out of $100 million. In later discussions, Mark Morze, the company's CFO, detailed how he used white out and a copy machine to create over 10,000 false documents including false bank statements.

To complete the confirmation fraud, Mark paid a friend $10,000 for the use of the friend's name and address as the contact information for the audit confirmations. ZZZZ Best's accountants sent the audit confirmations to the friend's address and received back official looking confirmations that "verified" ZZZZ Best's accounts.

For a period of years ending in 2002, over 14 people at HealthSouth conspired to create 1,000's of false documents leading accountants to certify financial statements that included $300 million in false cash.

Confirmation Fraud Schemes

Providing false statements, though, is only the first step in the confirmation fraud scheme. The second step is accomplished by manipulating the responder to the audit confirmations.

By definition, third-party confirmations are sent to the client's financial institution, vendor or customer, and therefore, it is within the identity of the responder that the ultimate exposure to fraud exists.

In case after case, confirmation procedures are shown to be easily manipulated by fraudsters, especially when the process is so simple to circumvent. The liability in being associated with any part of a fraud includes:

- Criminal charges;
- Civil lawsuits;
- Loss of reputation and clients;
- Firm financial exposure;
- Personal criminal exposure; and
- Personal financial exposure.

Every fraud scheme is different and varies in its unique details. The schemes discussed here can be used individually or in combination by those trying to commit a fraud. Here are four primary ways that a fraudster can take advantage of the audit confirmation process:

Four Confirmation Fraud Threats

1. Client provides the account statement and contact information;
2. Client provides the contact name;
3. Client directs/influences the auditors authentication process; and
4. Impractical if not impossible to validate financial institutions signatures.

These four fraud schemes are used to circumvent the third-party confirmation process, but the list is not inclusive of all the fraud scheme possibilities or combinations. Let's discuss each one in more detail.

1. Client provides the account statement and contact information

Independent of the size of the accounting firm, a survey of over 150 accounting firms by Capital Confirmation, Inc., a company that provides confirmation authentication services, found that almost universally audit clients provide auditors with the contact information for confirmations and that rarely is any independent validation performed by the auditor to authenticate that contact information.

What the company found is that with the paper confirmation process, mailing addresses are provided directly by the client and/or taken directly off the client's statement which was in the client's possession. Audit standards require the auditor maintain control of the confirmation process—start to finish—which includes validating the contact information. Standards do not allow an auditor to take as audit evidence a statement or piece of paper provided by the client without the auditor independently validating that information. Therefore, asking the client for or taking that contact information off of a client-provided bank statement does not meet the standards requiring control and professional skepticism.

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 with today's technology the dishonest client can very 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 did, they can use a UPS Store mail account or a P.O. Box. Phone numbers can be prepaid cell phone numbers or a Kinko's 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, an address, fax line and phone line, at any executive office suite that offers those

services. In some cases an email account can be established and the phone will be answered by a receptionist using the name of whatever company the fraudster asked them to use.

Continuous 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.

2. 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, many times they 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, phone/fax number but a dishonest contact name. This dishonest associate can 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 not get caught when the confirmation is returned to the auditor.

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 Adidas' Director of Sales who confirmed $2.2 million in receivables due when in reality Adidas only owed Just of 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.

3. Client directs/influences the auditor's authentication process

Numerous examples illustrate how dishonest clients try and sometimes succeed in influencing an auditor's procedures, especially when it relates to third-party confirmations. If a client suspects that the auditor may try to authenticate the contact information for the confirmations, with a little effort and for very little money, fraudsters can create third-party credentials which closely resemble legitimate credentials.

Just last month, January of 2004, in two separate cases, thieves created a fake U.S. Bank website and a fake Union Planters Bank website to steal important online banking information from customers for their own gain. 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 banks' own customers could not distinguish the real site from the fake site, how can those of us who might see it once a year determine whether it is real or fake?

The answer is we are not able to tell the real information from the fake with only a cursory review. We must take time to validate a site's authenticity.

Here is how for less than $300, a false website for a legitimate financial institution can be created that displays incorrect contact information to include emails, phone/fax numbers and the mailing address. Fraudsters purchase a URL similar

to the legitimate company's URL, paying an ISP (Internet Service Provider) to host the website, and then simply copy and paste the source code from the original site to the fraudulent site while changing only the contact information. If an auditor sends confirmations to the false contact information, fraudulent confirmation responses will be returned. When compared, not only is the fraudulent site almost an exact replica of the original site, the URL and email extension appear to be legitimate to those who do not have a day-to-day working relationship with that specific financial institution.

One suggestion is to use secure email to authenticate the responder, however, that would not detect this fraud. Secure email only ensures that the fraudster and the auditor communicated in a secure manner, and does not serve to authenticate the responder to a confirmation request.

One way to determine who owns a website is to use the DNS lookup feature available on the internet. There is an issue with the DNS lookup though. DNS lookup information can be manipulated to appear correct, even stating the names of a legitimate company's executives. This is because no regulatory or governing body proactively ensures that 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 keep people from tracking down the 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 with new, and most likely, false information and the process begins again. It is not until a URL has received numerous complaints over an extended period of time, often many months, that a more extensive evaluation takes place. Fraudsters understand this process and use it to manipulate the system realizing that the amount of time and energy required to identify the true owner would be enormous.

4. Impractical if not impossible to validate financial institution's signatures

Given all the possible loopholes that exist to circumvent the paper confirmation process, it is not practical to think that 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 who 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 because of the enormous costs involved and is only used once a potential fraud is believed to have occurred—which could be too late to eliminate the liability associated with the fraud exposure.

Knowing this, 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. This occurred in 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.

Confirmation Fraud Schemes: The Responder's Risks

Companies and individuals that respond to confirmation requests face a different and unique set of issues.

By definition, third-party confirmations are returned to the requestor and not the client, therefore, it is within the identity of the requestor/recipient that the ultimate exposure to fraud exists.

In case after case, paper-based confirmation processes are shown to be easily penetrated by purported fraudsters, especially when the process is so simple to circumvent. The threats below highlight how a fraudster can take advantage of the paper confirmation process:

1. Return Address/Fax No. *Not* the Client's;
2. Return Envelopes *Not* Kept on File;
3. Incomplete Communication of Central Response Center;
4. No Penalty or Repercussions for Bad Requests;
5. Impractical if Not Impossible to Validate Signatures;
6. A Client's Employee Provides the Responder's Contact Address to the Requestor; and
7. A Client's Employee Provides the Responder's Contact Name to the Requestor.

The responder to a confirmation requests can vary but includes financial institutions, brokerage houses, public companies, private companies and government entities. Let's discuss each fraud threat in more detail.

1. Return Address/Fax No. *Not* the Client's

Third-party confirmations by definition are not returned to the client but to the requesting party. For the requestor, this eliminates the potential for the client to intercept and change the response information.

In combination with fraud schemes four and five below, to easily circumvent the confirmation process, a fraudster simply has to scribble an illegible signature of the company CFO or other signatory and request the response be sent back to a fraudster's address/fax, P.O. Box, a UPS Store account, a friend's address/fax, Kinko's fax number, etc.

2. Return Envelopes *Not* Kept on File

Most standard paper confirmation forms have a place for the requestor to write down the return address for the confirmation request; however, many requests come with a pre-addressed stamped return envelope in which to mail back the confirmation response. This saves the responder money and reduces the time required by a clerk to return the completed confirmation form; however, it also makes it easier to commit the fraud. With the current paper confirmation process, responders sometimes keep a copy the confirmation request for their own files, but rarely do they do they spend the time and energy or use the storage space to maintain copies of return envelopes.

To shield themselves from being caught, fraudsters use pre-addressed and stamped return envelopes knowing that copies of return envelopes are rarely made and stored with copies of the original confirmation response.

3. Incomplete Communication of Central Response Center

Many responders are transitioning to a central location or set of locations to respond to confirmation requests. This helps these responders maintain control over the process and provides for a central repository of all confirmations.

For responders that do not maintain a central response center and for those responders that do maintain a central response center but fail to communicate the location to the confirmation requesting entities such as auditors, the following fraud opportunity exists for all confirmations requests.

In interview after interview with employees from responding entities, Capital Confirmation found that paper confirmations are responded to by individual clerks, administrative personnel and account managers and are not forwarded on to the central response center. Many of these employees claim a lack of knowledge in regard to the central response center or a desire to satisfy a "client request" when a phone call is received requesting an expedited reply. Any number of other reasons is given as to why they respond to paper confirmations via the mail, fax or phone, but each time a confirmation is responded to in this manner the entire confirmation process is put in jeopardy.

Knowing this, fraudsters mail and fax requests to or just phone unsuspecting clerks, administrative staff and account managers and with just a few attempts acquire the information they seek.

4. *No* Penalty or Repercussions for Bad Requests

Paper requests that contain the wrong information such as wrong account number or wrong name of the signatory are not turned in to authorities but rather returned to the requestor stating the reason for denial.

In conjunction with fraud schemes three and five, with little to no chance for repercussions, fraudsters are free to make unlimited requests, correcting any inaccurate information until they receive the information they desire.

5. Impractical if Not Impossible to Validate Signatures

Because of the sheer volume of requests and the time it would take to validate a signature on a confirmation request, rarely are signatures validated. For security reasons some financial institutions do not provide access to signature cards to the confirmation response department or individual clerks and relationship managers and therefore it is impossible to validate the signatures on confirmation requests. Public and private companies almost never maintain signature cards on customers and vendors by which to compare the signature on a confirmation request.

Even in those financial institutions that do provide their employees access to signature cards, as is the case with paper checks it is almost impossible and completely impractical to individually validate every signature on the hundreds, thousands and even tens of thousands of paper confirmation requests.

Even if employees try to match the signatures on the confirmation requests to the signature cards, in today's environment, unfortunately a cursory review of a signature by an untrained employee no longer provides a safeguard from liability. The liability can be enormous when this fact is presented to a jury that does not understand why employees were not trained in signature recognition and that does not appreciate the challenges associated with exactly matching every signature on every piece of paper.

Juries do not have an appreciation for the tremendous resources required to hire, train and maintain specially trained staff to proactively compare and contrast each signature to a signature card on file. For practical reasons, today these types of specialists are not used to proactively prevent fraud because of the enormous costs involved but are only brought in once a potential fraud is believed to have occurred. However, this is too late to eliminate the liability associated with the exposure of not validating every signature.

Knowing this information, fraudsters simply scribble the signature of the signatory to gain access to private information.

6. A Client's Employee Provides the Responder's Contact Address to the Requestor

Because the confirmation requestors do not know where to send confirmations within the responding entity or to whom the confirmations should be directed, a client employee often provides that information. A dishonest client who is committing fraud can direct the requestor to send the confirmations to a fake address.

This was used by Parmalat executives who intercepted confirmation requests from their auditor and returned fraudulent account verifications. Even though the financial institution does not appear to be involved with the confirmation fraud, the mere fact that they were mentioned in the fraud has brought them tremendous scrutiny and has caused them to spend tremendous resources to defend themselves and their reputation.

7. A Client's Employee Provides the Responder's Contact Name to the Requestor

Again, because the confirmation requestors do not know where to send confirmations within the responding entity or to whom the confirmations should be directed, a client employee often provides that information. A dishonest client who is committing fraud can direct the requestor to send the confirmations to someone helping them from within the responding company.

Timothy McCool, Director of Apparel Sales for Adidas America, plead guilty to committing this type of confirmation fraud. McCool's client, Just for Feet, was a publicly traded company that had grown to be the

second largest retailer of athletic shoes in the country. Just for Feet's auditors sent an accounts receivable confirmation to Adidas asking Adidas to confirm the $2.2 million receivable due to Just for Feet. McCool was motivated by future sales to Just for Feet and confirmed to the auditors that Adidas owed the $2.2 million when in reality Adidas only owed Just for Feet approximately $40,000.

This one employee exposed Adidas, Just for Feet and every individual involved in the audit to a huge potential liability.

Preventing Confirmation Fraud

Preventing confirmation fraud requires proactive efforts to independently authenticate all parts of the confirmation. Relying on the unvalidated signatures and contact information does not limit your liability and may only serve to exacerbate your liability if it is shown that you had the information and chose not to authenticate it.

Here are a few ways to help eliminate confirmation fraud:

- Get independent verification of the contact information including addresses, phone numbers, fax numbers, email addresses and web site URLs;
- For requestors, validate that the responder to confirmations is authorized by their company to respond to confirmation requests and validate that the responder does not have a motive to provide false or misleading information;
- For responders, independently validate the receiver of the confirmation and their contact information; and
- Consider the use of specialized technologies that assist in providing independent authentication and validation to the confirmation process.

Conclusion

Just being mentioned as a party to a fraud can have a career damaging effect on your reputation, not to mention the consequences of being involved in a lawsuit or criminal investigation. Today's juries are not very forgiving when a fraud or even a potential fraud is missed, no matter how immaterial it is to the financial statements. Showing a jury a weakness in any area regardless of error, calls into question everything you do. Make sure that confirmations are one area that you can have confidence in.

For more information about secure electronic confirmations, contact us at:
1-888-716-3577 or visit www.confirmation.com.

Capital Confirmation, Inc.
214 Centerview Drive, Suite 265
Brentwood, TN 37027
Phone: 888-716-3577

