



CONSTRUCTION INSPECTOR REVIEW

VOLUME 8, 1ST QUARTER 2008

WORD FROM THE HOME OFFICE

Happy New Year! Granite Construction Inspections (GCI) is realizing its forecast for a fruitful year. In spite of the downturn in the mortgage industry, GCI has been recognized as the "benchmark" for quality, efficiency and adherence to changing bank policies. As a result, we have seen both portfolio growth and increased interest in our services.

In keeping with this recognition, we have been expanding our web infrastructure in the area of security. A vendor's ability to provide secure data exchange has become one of the primary concerns with our banking clients. GCI continues to lead the way in this critical area.

You will be receiving a communication via our Email Blast System describing one of these security changes and instructions on what we need each inspector to do so that we are in compliance. Website logins must now meet compliance to bank level security protocols. The "Username" will be issued by GCI and you will simply create your own Password. Upon resetting your login, you will be asked to answer two questions, for example: "What is your dog's name? What is your mother's maiden name?" Please watch for this email communication in the coming weeks.

Review the article in this edition of the CIR; *Is it Safe? Data Security Concerns When Outsourcing Inspections*. It was authored by our Senior Vice President of Information Technology, Wes Hamil.

The GCI Inspection Team

Is it Safe?

Data Security Concerns When Outsourcing Inspections

by Wes Hamil

Financial institutions are constantly looking for creative ways to improve productivity, cut costs, and provide a higher quality service for their customers. The ability to do this can and does often determine an institution's market share and their ability to distinguish themselves to a prospective purchaser of their products. As a lender seeks to compete more effectively in the realm of construction lending, the ability to process draw disbursement requests efficiently becomes a key component in the Lender's ability to offer a cost effective product. They must be able to provide for the quick draw funding turnaround times that a borrower wants when building their home, while at the same time avoiding the pitfalls of over-funding a home and letting the contractor *get ahead* of the actual work that is in place.

One of the principal tools for managing this process is the construction draw inspection. The inspector is the lender's *eyes and ears* on a project. An accurate inspection, completed in a reasonably short time period, can enable a lender to make a funding decision that is expeditious and still preserves the level of risk

(cont'd page 2)

Wes Hamil is the Senior Vice President of Information Technology and has serviced as the principal architect in the development of Granite's proprietary software applications since 1999. Mr. Hamil manages the ongoing development of Granite's IT infrastructure, including the security environment. He may be contacted at 303.967.1702 or wes.hamilton@graniteloan.com.



New!

GCI DEVELOPMENTS

GCI is Rapidly Expanding into the Commercial Inspection Market!

GCI is currently seeking commercial qualified inspectors in all 50 states. Please submit your resume and/or Bio to Angie Kelley, Recruiting Department at angie.kelley@gcinspects.com.

(cont'd page 3)

Construction Inspector Review Volume 8, 1st Quarter 2008 In This Issue:

1. *Is it Safe? Data Security Concerns When Outsourcing Inspections*
2. GCI Developments
3. Outstanding Inspector

P: 800.919.8903

F: 888.647.4677

inspectorinfo@gcinspects.com

www.gcinspects.com



Is it Safe? (cont'd)

management required to properly control the risks associated with a construction loan portfolio.

There are numerous avenues a lender may utilize for construction draw inspections. Some lenders may choose to employ *in-house* inspectors. This approach may work when the lender's portfolio is highly centralized, predominantly local, and relatively small in number. However, once a lender starts to grow their portfolio and expand their market to include geographically diverse regions, for example, across state lines or to more than a hundred or so miles from their base of business, they often will employ a Vendor to provide construction draw inspections.

There are a number of construction inspection companies in the marketplace at present. The majority of these are regional companies that provide a varying degree of inspection services in a restricted area. There are additionally a handful of companies providing inspection services on a national basis. These companies work to provide a construction draw inspection to their clients with a degree of accuracy and a *turnaround time* that will satisfy that particular client's draw processing needs.

With that being said, all successful inspection companies must employ technology to serve the complex needs of a lender's draw processing. This may



range from simple telephone and fax based communication to much more complex web based technologies which allow a client to view inspection photos online, retrieve reports detailing the inspector's findings and

in some cases even interface with a third party processing software utilized by the lender.

In order to do this work the inspection company will have to be privy to some degree of the

lender's data. This data will at bare minimum need to include a property address, a borrower and contractor name and contact number, and some degree of understanding of the scope of the project being constructed. These basic elements allow the correct property to be located for the impending inspections and for communication lines to be available to the inspector and inspection companies if any issues arise. In addition, a construction budget may be provided to better define the scope of work on the project. This in turn means that the inspection company will now have knowledge of the money involved in the project. In many, if not all, cases it is also common practice for the vendor to have the loan number of the project as well, thus opening up a number of doors to information that must be kept secure.

How an inspection vendor manages data security is an extremely crucial

element to the success of the relationship. This is in effect an extension of the lender's information security systems. Under current statutes governing the Security and Privacy of Customer Information (Example: California Senate Bill 1386 [SB-1386]), as they apply to lenders, any breach of security or privacy that occurs at the vendor level will in all likelihood be

(cont'd page 4)

Granite is a member of:

THE NATIONAL ASSOCIATION OF
CERTIFIED HOME INSPECTORS (NACHI)



For more information about NACHI, visit them at www.nachi.org or explore their resources at www.inspectormall.com.

JOIN OUR NETWORK!

GCI is constantly recruiting qualified individuals for our nationwide Inspector Network.

If you are qualified to perform either residential or commercial construction inspections and are interested in applying, please email us at:

inspectorinfo@gcinspects.com

to learn more about what GCI can offer you!



INSPECTOR CENTRAL

New! *GCI DEVELOPMENTS* (cont'd)

Original Message to Inspector Contains Important Information

The Original Message to Inspector box displayed on the website contains information that is specific to that project. The information is often referred to as the "Special Instructions". These instructions communicate value and critical information regarding any special requirements associated with that order (i.e. contact numbers for directions or access, scheduling for access, wait to inspect next Monday, etc.). These instructions are located in three areas on the website/report; First, they are viewable on the project web screen under the heading "Original Message to Inspector." They are also displayed on both the inspection field report in the upper right section and on the email notification.

GCI Website Login Changes

As part of our new security policies, we will be requiring all inspectors to update their GCI website login. An instructional tutorial will be submitted to each of you in April 2008. This communication will be sent by email, please watch for it. ■

"OUTSTANDING... IN THE FIELD"

*Steven currently has a half day turn around time with us!
He is always ready to go at a moments notice.*

Way to go Steven!

Steven Zeito was in the business of buying and rehabbing houses when he realized that he was making a lot of costly mistakes. From there he decided to get a home inspectors license to help himself, home buyers and people doing rehabs avoid making the same costly mistakes. In 2002, he attended Kaplan Professional Schools and received a Professional Home Inspectors license (#8032) from the Texas Real Estate Commission. Steven is a Disaster Housing Inspector and performs inspections for FEMA when he is called on.

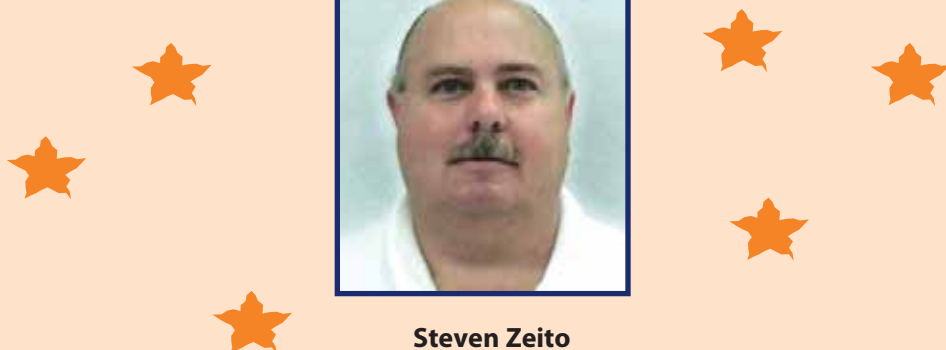
Steven started Advanced Home Inspections in 2003 and has been performing draw inspections for banks and home inspections for buyers and sellers.

He owes his success to two things. One is continuing his education by taking a minimum of 16 hours of classes every year and attending The ITALV inspection Expo that is held annually in Las Vegas. This has helped him to stay in touch with constant changes in the construction field. The other factor that has made him so successful is that he tries to get any and all of his inspections completed and submitted to the customer as soon as possible.

Everyone wants their results yesterday, so he went out and purchased a wireless card for his laptop so that no matter where he is, he can complete and e-mail the results of all inspections. "It works out great. I don't have to wait until I get back to the office to finish my days work."



Steven Zeito
Advanced Home Inspections
3463 Caracas Dr
Mesquite, TX 75150
972.310.0402
texasinspection@yahoo.com





Is it Safe? (cont'd)

construed as a violation by the lender as well. At last count, 38 states had data privacy laws that were more or less explicit in their disposition towards a perceived breach in security, and the remedial efforts imposed upon the holders of such breached data.

Recent changes in the laws of many states require that if a breach of privacy occurs concerning data that is deemed sensitive to the customer, then the lender must inform ALL customers that such a breach has taken place (Examples include, but are not limited to, Gramm-Leach-Bliley Act and Sarbanes-Oxley Act). In most cases these breaches have resulted in class action law suits on the part of the customers. Given the fact that industry standard practice for inspection service vendors is to obtain borrower names, property addresses, budget and loan amounts and loan numbers, it is clear that this information should be regarded as extremely sensitive by a client lender. A breach of this information is likely to invoke quite serious consequences and at a bare minimum, even if the courts were to find that a vendor had employed all recognized best practices and was nominally liable, the damage to both the inspection vendor and their



client lender's reputation in the market place could be considerable.

So what are some of the pitfalls to avoid in regard to processing inspections through an outsource vendor, and what are some best practices to look for when selecting such a service provider?

In the rush to secure potential technological vulnerabilities, many organizations overlook the obvious weak spots in an environment that could lead to data breaches.

First and foremost is onsite security at the vendor's facility. What is the nature of their physical security environment? Are servers easily accessed by any employee or are they located in a secured environment with cameras and monitored/restricted access?

What about access to their offices by the general public? Can anyone simply walk in, or must they sign in and be escorted? Is there more than one point of access to the offices, meaning are there multiple doors to the facility? If so, are they monitored in some way, and is access restricted? If someone can casually walk through a back or side entrance to a facility during work hours, it's not a difficult task to scan someone's computer screen or pick up a file left idling on a processors desk while they are away at the water fountain.

LOOKING FOR CONTRIBUTORS!

We are looking for contributors to the CIR newsletter. If you have an idea for an article or something you want us to review – let us know.

In addition, if you have authored industry-related articles and would like to submit something to the publication, contact our Marketing & Sales Department at 866.380.9504 or email us at sales@gcinspects.com.



Comments & Compliments

We are always looking for feedback from the field. If you have a suggestion to make your job more efficient or have something nice to say, let us know.

We appreciate your input and look forward to hearing your thoughts and ideas.

(cont'd page 5)



Is there a clean desk policy? How are paper files handled in the workplace and who gets access to them?

And then there is the question of employees. The largest banking data theft incident in history at that time, May 2005, occurred in New Jersey and according to authorities was executed through the manual construction of a database by employees while onsite in the workplace during business hours. The suspects manually built a database of the 676,000 accounts using names and Social Security numbers obtained by the bank employees while they were at work.²

So, does the vendor perform background checks on its prospective employees and do these checks include a search for criminal records? Employees have been known to do everything from pilfer hard copy files to attempting to print screen shots of sensitive data and carry them out with their personal possessions.

Is there a Customer Service Department? If so, are the Customer Service employees trained to cope with attempted *social engineering* tactics? Is it possible for an unknown caller to impersonate a real customer to a sufficient degree as to obtain sensitive information about that customer's account. As technological advances create a hopefully more difficult barrier to breach, there has been a rise in the *social phishing* techniques of attempting to obtain sensitive information not from solicitous emails but rather through exploiting overly helpful customer service representatives over the phone.

In a Visa Data Security Alert dated December 18, 2006³, Visa warned its consumers of this *voice phishing*, or *vishing* as it is now referred to as a rapidly escalating technique where an experienced visher will obtain a bare minimum of information on a customer and then make a customer service call, speaking with the authority of a few known facts and intimidate the customer service representative into disclosing enough additional details to enable the *visher* to potentially execute identity theft.

And how does such a person obtain that bare minimum of information required to exploit a hapless and perhaps under-trained customer service rep? It can be from internal data theft, from poorly designed network security practices that allow a user to copy data from a system and either email it to an external account or take it home on some form of portable storage such as a flash drive. It can be from a stolen laptop that had sensitive information on it and was never encrypted by the Vendor's Information Security (IS) team. It can be obtained from software that was not designed with the basic security premise of need to know in its baseline architecture, revealing too much sensitive information to employees whose job responsibilities did not entail access to such knowledge.

Data breaches can even come from the normal course of business practices that a vendor is engaged in to *make it easy*

for their clients. For example, does a vendor transmit potentially sensitive information in open, unencrypted emails or do they have a more secure method of communicating with their clients when sensitive data is involved? If they provide information via a website, does their website always, without exception, require strong authentication (username and password at the bare minimum) to be accessed?

Do they allow the client users to link directly to information on their site, bypassing the authentication requirements described above? This is an especially exploitable vulnerability, and depend-

(cont'd page 6)



PHOTO CORNER:

Spring Forward! Daylight Savings Time has arrived and the days are growing longer. That means there's more time to take your photos during daylight hours.

NOTE: Please remember that if you can't make out what's in the photo neither can we and neither can our clients!

Helpful Hints:

Remember to set your camera's resolution to the lowest possible level (300 dpi) or set the email setting to standard/email quality to ensure easier website upload.

²Todd Weiss, "Scope of Bank Data Theft Grows to 676,000 Customers," Computerworld, May 20, 2005, <http://www.computerworld.com/security/topics/security/cybercrime/story/0,10801,101903,00.html>.

³Security Vulnerability: New Social Engineering Schemes Detected* Data Security Alert #121806, December 18, 2006, Visa U.S.A. Inc., http://usa.visa.com/merchants/risk_management/cisp_alerts.html.



Is it Safe? (cont'd)

ing on how information is exchanged between the vendor and the client, it can be easily capitalized. It is very convenient to jump straight from an open email to a linked page on a website, however it is also very convenient for a hacker to intercept such an email, which may have traveled through half a dozen relay servers on its way to the client. If there is any information that aids in a potential ID exploit on that web page such as loan number, property address, etc., then the hacker has gained valuable insight and opportunity.

If the vendor uses web technology, has it ever been *ethically hacked* in the form of a formal penetration test? This is typically an expensive proposition, however it is one of the only ways a client can be comfortable that an independent outside expert has attempted to *break into* the vendor's technology and exploit it as would a malicious intruder. One example of such a company that performs the ethical hack of a penetration test is the Symantec Corporation. In such a test the *hacker*, in this case Symantec, would engage with the vendor's full knowledge in the process of attempting to exploit the web application and obtain access to sensitive data. Information gleaned from this process, if any, is shared with the vendor by Symantec so that remediation can be made.

Finally, where is the level of awareness within the vendor's organization as to the relevance and priority of data security? There are a myriad of

security measures and requirements in the banking industry, most notably Gramm-Leach-Bliley Act (GLBA) and the more recent Federal Financial Institutions Examination Council

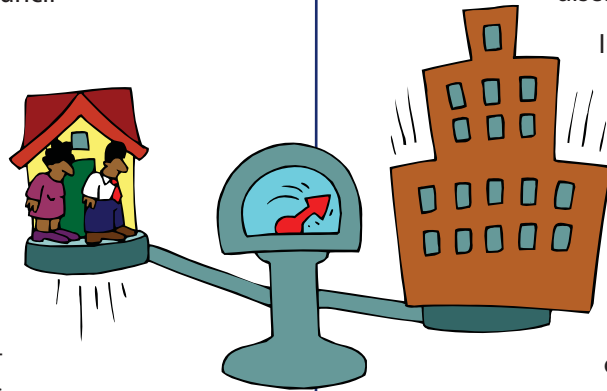
(FFIEC) guidance on strong authentication for web based transactions involving sensitive data, especially pertaining to financial transactions.

Does the vendor have a working knowledge of the ramifications of such regulations and are they compliant?

There are certifications from independent auditors that can be obtained that will validate for a financial institution that their vendor has a secure data environment. These audits are typically performed by an established accounting firm such as Ernst and Young. One such audit is a SAS 70 Compliance Audit, of which there are two types. Type 1 describes the design of controls in place at a specific point in time and Type 2 examines the design and effectiveness of controls in place over a specific timeframe, usually six months. A newer, emerging certification thought by many in the Data Security field to be even more comprehensive is the BITS certification. These audits are exhaustingly thorough and cover all of the topics mentioned in this article.

Some institutions annually audit their vendors with their own Information Security teams to establish a comfort

level with the degree of security in place within that vendor's infrastructure including the environmental, human resource, and technological channels discussed above.



In the current climate of construction lending, with an emphasis on a competitive product and the premium placed on the customer experience, there is

little question that an efficient draw process abetted by a quality inspection service will add tremendous value and efficiency to any program.

In this era of ever increasing awareness, the need for effective data security is equal to the potential impact from the failure to maintain that security. Lenders must view the vendors they employ as a direct extension of their own security. Ensuring that these vendors maintain their security environment to a high standard is insuring the integrity of the lenders own portfolios, valued customer base, and indeed their own reputation. ■

Construction Inspector Review
10770 Briarwood Avenue, Suite 280
Centennial, CO 80112
800-919-8903

Customer Service
800-919-8903
inspectorinfo@gcinspects.com

Sales & Marketing
866-380-9504
sales@gcinspects.com