COMMUNICATE
COLLABORATE
CO-EXIST
COMPLIANCE

THEFOURTHC

A monthly publication of the compliance department of WFG National Title Insurance Company

Volume 3 | Issue 5 | August 2015

Welcome to TheFourthC

WFG's Monthly Compliance Newsletter

Lenders are reminding us almost every day that "just saying it doesn't make it so". In other words lenders seeking to find the truth about a service provider's compliance efforts are no longer relying on representations from the provider that they are doing what they say they are doing. Long gone is a time when a title agent or settlement services provider could get away with merely making assurances that they are protecting consumer non-public private information and that emails are encrypted and secure. The days of "*trust me, we're doing everything the way we're supposed to"* are gone. Lenders and the audit firms they hire are asking initial questions, followed by what seems like a never-ending barrage of follow-up questions demanding unassailable proof in the form of written documentation, audit reports, results from self-imposed stress tests, attestations and notarized affidavits.

Not only will lenders require audits of our data centers, but they will also want copies of our policies and procedures, flowcharts, trust account reconciliations, data security plans, and much more. In addition, lenders and even the CFPB may ask for permission to visit our facilities. CFPB supervises and examines settlement service providers who provide services for banks and non-banks to determine if the organization is complying with consumer financial protection laws.

Lee Ann Fenske recently interviewed Bob Lohr, SVP of Systems Implementation for WFG Lender Services for this month's feature article entitled, "How Do I Know if I'm in Compliance and Ready for a Lender's Audit?" We hope you find this article provides valuable insight into what lenders and regulators are expecting in an ever increasing regulatory and compliance-oriented world. The article provides valuable information and timely reminders about what we need to be doing. When we excel at being compliant on a daily basis, we increase our chances of passing

any type of audit with or without notice.

Also in this month's issue, you will read about our new Compliance Hotline for anonymous reporting. We encourage you to continue turning to your manager, HR, Legal or Compliance Departments with questions or suspected breaches in policies and procedures. However, if you feel that you can't go to these sources, then please utilize the new anonymous reporting services.

This month's publication also updates you on *"What's New in WFG Scholar?"* This publication provides answers to frequent questions about navigating in the system, and what is required for our annual training program.

Interested in a particular compliance or audit topic? Or, writing an article for *TheFourthC*? We are always looking for ideas for new articles and new contributors. If you have an idea for a future article or want to write an article, please contact us at compliance@wfgnationaltitle.com.

Donald A. O'Neill
Executive Vice President & Chief Compliance Officer
WFG National Title Insurance Company

How do I Know if I'm in Compliance and Ready for a Lender's Audit?

We've heard managers ask, "How can I be assured that I am in full compliance and ready for a lender's or CFPB audit at a moment's notice?" As you can imagine, that isn't an easy five-minute conversation. By understanding and following our corporate policies and procedures and the new CFPB Rule is an excellent start, but there is more to it.

The CFPB Bulletin 2012-03, states that "lenders may be held legally responsible for the actions or inactions of their service providers where consumers are harmed as a result of the service provider failing to comply with consumer financial law." Due to the lender being held responsible for our actions, or lack thereof, they will conduct audits on top of the due-diligence requests that we receive by way of their Lender Questionnaires.

I interviewed Bob Lohr, SVP of Systems Implementation for WFG Lender Services and asked him the following question. "What helpful hints could you give our FourthC audience on being prepared for an audit from a Lender?"

Bob had some good insight that I thought I would share. "Spend quality time with a team of experts to be prepared. Lenders will send pre-work to your organization ahead of their audit. You will need to provide answers on the spreadsheets they send and gather the supporting documentation to send to the lender by their requested date. This takes a considerable amount of time to coordinate with other individuals and teams, such as the WFG Corporate IT, HR, Compliance and Legal Departments; supervisors within your organization and any outsourced vendors or vendor suppliers. Plan on two to three weeks for the preparation. Also, review all Master Service Agreements (MSAs) and the lender's Statement of Work (SOW) that may have been signed to re-familiarize yourself with the terms and conditions. Check with management to see if any attestations were signed with the lender. Make sure that all of your corporate Policies and Procedures (P&Ps) are within a year old, and review any business unit Standard Operating Procedures (SOPs)."

Bob went on to discuss the business unit's SOPs, "the lender will want your local practices documented for recording documents, completing final policies, entering orders into your production system, flow-charts for how the work and NPI moves throughout your office and within your systems, how your office interacts with business process outsource (BPO) vendors, standard disbursement process for your state and any other states that you do business in, among others which are outside the scope of a corporate P&Ps that only your business unit can develop and maintain."

He went onto say, "the local office has control over a small portion of the audit, however, your local team that is managing the audit process, needs to stay engaged and make sure that all of the other corporate departments are kept advised. Review all logs prior to the audit, and don't wait until the last minute to do your due-diligence. As an example, the physical security log showed some false door propped open messages for the door that leads into the

computer room. The bottom hinge was a little loose, so it kept bringing up a false reading. They fixed the hinge, documented the repair and watched the logs to make sure that it wasn't reporting any further errors. Don't wait until the last minute, in fact, make sure that you always follow your P&Ps, SOPs, review and audit your logs, and document your reviews. My experience has been that most times, the auditors are very helpful and want a collaborative working relationship through the review process. They want you to succeed as much as you do. Contact them ahead of time if the lead team has any questions, or ask if your responses are sufficient. Being prepared and sending them the correct information ahead of time will reduce what easily could be a three to four-day audit meeting down to a day and a half. You are in the audit meeting for the entire time that they are there, answering all of their questions and showing proof that you do what you say you do. It is also very rare to have no remediation items, but you will usually know what they are before the auditors leave your facility. If you can, complete the remediation items while the auditors are still there. Remediation of the different risk levels is given to the operation with due dates. The higher the risk level will result in a shorter time-period that you are required to remediate the issue. If you don't remediate, you may not receive any further business."

One of the recent audits focused on the following areas that they evaluated:

- Access Control
- Asset Maintenance
- Insider Threat
- Compliance
- Communication and Operations
- Information Systems Acquisition, Development, and Maintenance
- Incident Management
- Physical and Environmental Security
- Security Policy
- Vendor Management and HR
- Consumer Complaint
- Training

Access Control

Review of all Security Policies on Access Control – how the organization creates and maintains access to: applications, network components, operating systems, routers, databases, firewalls, voice communication servers, tokens, smartcards, VPN, and encryption methods. How the accounts are created, disabled and documented; does management review logs; how do guests log-in, how are non-permanent employees handled, and explain cloud services, if applicable.

Asset Maintenance

Review of all policies on the handling of hardware and software. Is inventory required and reviewed annually on all hardware and software assets that are tracked by serial numbers or asset control tag? Verify that no one can load unauthorized hardware or software. Review the

policy and logs on the disposal of all electronic media. Review prior audits of all logs documenting the deletion, physical moves, repair, etc. of electronic media (tapes, disk, drives, multifunction devices, copiers, and end user devices).

Insider Threat

Review of all policies, logs and audits surrounding: Encryption; no removable media (no CD/DVD burners, hard drives, back-up tapes) – exceptions have to be documented and approved by upper management; outbound internet activity logged and monitored, write data from scanners/printers to removable media is disabled, access to social media sites disabled, and review of the Asset and Data Classification Policy.

Compliance

Review of all policies, procedures and audits that involve: acceptable use and protection of company email, internet, social media, company assets and the handling of NPI; how do we ensure compliance with local, state and national information security and privacy regulations; how do we ensure that consumer's data is retained and disposed of in accordance with regulatory requirements; and process to identify and assign a risk ranking to discovered security vulnerabilities.

Communications and Operations

Review all policies and procedures that involve: IT security risk assessment; network diagrams, data flow diagrams and physical/facility security.

- Security-related products such as anti-virus and personal firewall software are managed to ensure that unauthorized modifications cannot go undetected.
- Capacity planning
- Formal change management/change control process that requires documentation and management approval of all changes to applications, systems, databases and networks.
- Disaster Recovery and Business Continuity review and audit of testing procedures.
- Where is data stored, and what are the procedures for safekeeping?
- What are the back-up procedures or alternate data centers to ensure Service Level Agreements (SLAs) can be met?
- When files or data are transferred from site-to-site, are there inventory logs for checking-in and checking-out of the files/data?
- All laptops, mobile devices or removable media needs to be encrypted.
- If NPI is printed, copied, faxed or scanned, it has to be done in secure locations with restricted access.
- How are security event logs reviewed and monitored for operating systems, firewalls, IDS, routers and other network infrastructure?
- How are updates and patches being put into production?
- How do changes to hardware, software, patches, and updates get communicated, and are all patches and updates implemented within 30 days of release dates?
- Email servers are required to have active anti-virus/anti-malware software installed that includes scanning email attachments for malware. All devices are required to have the

most current version of anti-virus/anti-malware software installed.
- What are the protocols of all inbound and outbound network traffic?
- Review of all wireless technologies including encryptions controls.
- Review of voice over internet (VoIP) protocols.
- Review of annual internal and external vulnerability scanning process that encompasses all networks and hosts associated with the lender's data.
- Penetrations tests of critical applications or networks with internet connectivity must be conducted every 12 months and after any significant changes in systems.
- Disposal rules and procedures around paper shredding – must be locked and requires cross-cut shredding.
- Are devices in place to detect and prevent non-authorized software and hardware?
- How do we notify consumer and lender in the event of a breach in data/NPI?
- Review of all current licenses and insurance policies; and
- Review of all internal and external audits.

Information Systems Acquisition, Development, and Maintenance

Review of policies, procedures and program applications for: the security requirements for all internal and external developed applications that are used for the lender's services and products. How are changes authorized and tested before implementing? Is there a mirrored production level in place before going into the new program? Are logs in place that monitor changes to production and are there separate development/test and production environments?

Incident Management

Review of policies, procedure and logs for: incident response procedures for information security incidents defined and documented – which can be network outages, abuse of access privileges, lost cell phones or laptops, lost closing packages, and compromised NPI. Are all incidents reported to the appropriate information security, business continuity staff, and management? Are reviews conducted after the incident to document what happened and what can be done to prevent future incidents? Are staff members trained on what to do in the event of incidents and how to report them?

Physical and Environmental Security

Review of policies, procedures for: the physical security of the facilities and equipment assigned to an individual; and

- Is access to buildings where the lender's data is stored, transmitted, or processed restricted to authorized personnel only?
- Are visitors required to log-in, wear badges and are escorted at all times through production areas that contain NPI (logs must be retained for at least six months)?
- Is access to sensitive areas restricted to authorized personnel (computer rooms, network and communication rooms)?
- Are the access entryways where sensitive information is handled controlled by a physical access control process that identifies each person entering and leaving the area such as key cards?

- Are logs reviewed for unusual activity?
- Is there video surveillance equipment monitoring doorways that lead to sensitive data (including computer rooms)? They will require a time/date stamp of the video surveillance on a specific date that they will give during the audit. The cameras and equipment must be protected from someone being able to tamper or disable the devices.
- Does the surveillance equipment monitor and sound an alarm if the door is propped open?
- Is there sufficient lighting to ensure video images are clear and useful?
- Do video surveillance of computer room and perimeter entrances exist and is it aligned to see clearly people's faces with acceptable video quality?
- Computer room walls must go all the way from floor to ceiling with locked key card controls.
- Are emergency exits equipped with an audible or monitored alarm and locked to prohibit access from outside?
- Are sensitive areas where data is stored, transmitted or processed protected by a fire detection and suppression system?
- Does the computer room have environmental controls to detect the presence of water?
- What is the process to ensure the temperature and humidity of sensitive areas where data is stored, transmitted or processed?
- Is access to the badge system limited to authorized personnel?
- All shredding bins must be locked, and no shredding/recycling containers can be under desks; and
- Verify that computer monitors and open files containing NPI are not visible from hallways or outside windows.

Security Policy

Are information security policies defined and documented? Have all policies and procedures been updated in the last 12 months, and are policies and procedures approved by senior management. If a new vulnerability is detected, does it trigger a policy review? Are all policy exception processes approved by senior management, and do employees formally acknowledge the receipt and understanding of all corporate policies and procedures. Is the completion of annual security awareness training required, and are all part-time, contract, temporary and offshore employees required to comply with company policies? Are vendors and employees required to sign a confidentiality or non-disclosure agreement? What is the access rights policy of staff whose roles have changed or been terminated (facility, network, and systems)? Is the usage of external social media products for a business purpose approved and monitored by a senior risk manager, and are the content and postings to social media by employees who are subject to more restrictive legal and regulatory requirements reviewed to ensure compliance with relevant regulation? Describe and show proof of background check policy for all new-hires (some lenders require a ten-year background check upon hire with a renewal check run every two years). Does the background check processes comply with any additional country or region requirements, and are background checks

reviewed to ensure employees are meeting FDIC-defined prohibitions (dishonest acts, breach of trust or money laundering)? What is the organizations drug-testing policy? Visit with random employees about information security and training policies.

Vendor Management

Review of policies, procedures and documentation of: contracting due diligence (including financials, performance history, anti-money laundering, information security reviews, risk score/tiered classification, audit and testing, roster or abstract of all vendors that shows what access they have to NPI and/or production sites and programs). Do our vendor's background check their employees and do we obtain our vendors policies and procedures regarding NPI, data security, and their background check policy?

Consumer Complaint

Review of policies, procedures and documentation of: consumer complaint intake methods, logging, monitoring, tracking the time from opening to closing of the complaint; escalation of complaint and was the conclusion documented in a tracking program.

Training

Review of policies, procedures and logs for: mandatory training for employees, subcontractors, and vendors that have access to consumer's NPI for specific training courses. They will ask for logs on certain employees chosen by the auditor that reflects the date training was completed, if it contained an assessment quiz, and the final score.

CFPB Supervision and Examination Manual

http://www.consumerfinance.gov/guidance/supervision/manual/
http://solutions.allregs.com/article/525/what-to-expect-from-a-cfpb-audit
http://www.consumerfinance.gov/guidance/
http://files.consumerfinance.gov/f/201409_cfpb_readiness-guide_mortgage-implementation.pdf
http://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf
http://files.consumerfinance.gov/f/201306_cfpb_bulletin_responsible-conduct.pdf

Lee Ann Fenske
SVP Compliance/National Training Manager
WFG National Title Insurance Company

NEW WFG Compliance Hotline for Anonymous Reporting

What if you see behavior that you feel may be a violation, but you are afraid to report it? If you feel that you can't go to your supervisor, HR Department or Compliance Department and wish to remain anonymous, please do so! Anonymous hotlines are effective in preventing and identifying unethical or potentially unlawful activity, including corporate fraud, regulatory violations, employment discrimination, and harassment or bullying. If you are afraid that you will be punished, or you are not sure it is a violation, you can now report your concerns anonymously. Here is how you can report anonymously:

Toll-Free Telephone:

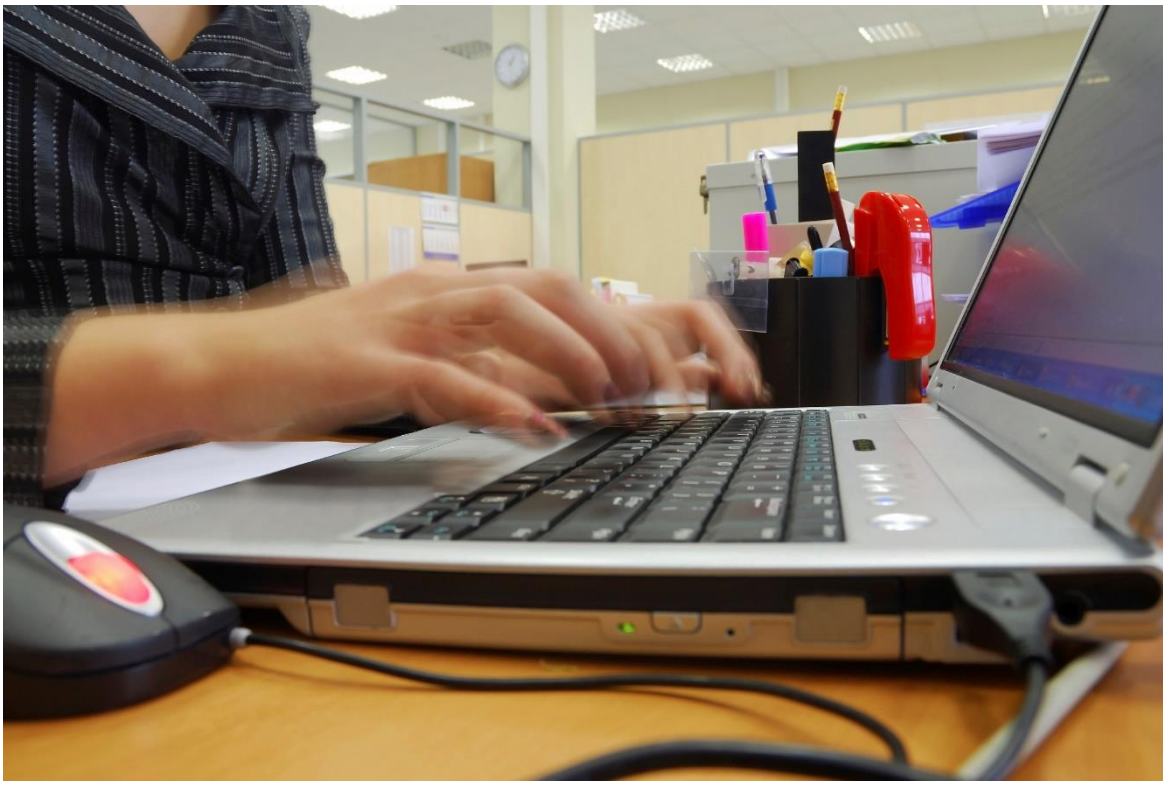
- **English speaking USA and Canada: 844-470-0003**
- Spanish-speaking USA and Canada: **800-216-1288**
- Spanish-speaking Mexico: **01-800-681-5340**
- French-speaking Canada: **855-725-0002**

Website: www.lighthouse-services.com/wfgnationaltitle[lighthouse-services.com]

E-mail: reports@lighthouse-services.com (must include company name with report)

Fax: (215) 689-3885 (must include company name with report)

Deborah Everett
Senior Vice President/Compliance Counsel
WFG National Title Insurance Company



Why Personal Email Can't Be Used for Business Purposes

It is a prohibited practice for WFG employees to use their personal email accounts for business purposes pursuant to Section 10.8.4.1.4 in our WFG Information Security Policy. If an employee uses their personal email account to conduct company business it puts us at risk in several ways:

- We have agreements with several of our national lenders to use a secure protocol to deliver emails that cannot be met with personal email.
- None of our anti-virus, anti-spam, or anti-phishing controls protect personal email.
- Our outbound anti-virus that protects our customers from receiving infected email sent or forwarded by us cannot protect against infected personal emails.
- Our Data Leakage Protection controls that prevent us from sending sensitive data via email cannot inspect and protect personal emails.
- In the event of an investigation or subpoena we cannot review or produce company emails sent using personal email accounts.

What's New in WFG Scholar

There are courses that are due on an **annual** basis. The user receives an email reminder that they need to go in and retake the courses. We now have the reminders set for a 30-day notice before the course expires and becomes delinquent. The user can go to the "achievements" tab and it will show dates in red that each **course is compliant until**. If the date is close or come and gone, then the user needs to go into the "Course Library" tab, find the course and retake it and the assessment quiz. It will extend that specific course out another year. Many people think that once they do a course, that it is good forever. This is not the case with most of them, as we are required to take them on an annual basis if they have anything to do with the new federal regulations. Lenders require annual training in their due-diligence questionnaires, along with verification.

Supervisors receive a report that shows the status of their employee's progress in the system. On the reports, column G shows the date that the user took the course, but then column E may show a "no" which means they never took the annual update and it is now delinquent. Column H shows if there has been any change to the course since the last time the user took it.

Another helpful hint for those that are taking courses on a wireless internet connection, is to make sure the connectivity is good. If there is any dip in the connectivity, the system will continue to allow the user to take the course, but it won't register that they completed it. Limit interruptions if taking courses from the office. If there is a large gap of time in going from screen-to-screen it will think that the user left the system, and again it won't show the completion.

After the user is done with the assessment quiz, there is a white "exit" button in the upper right hand corner of the screen. Once this is clicked, the system will reflect that it is loading the information. This may take a couple of minutes and if the user exits the system too quickly, or goes back to the home page, the system will not recognize that they completed the quiz and course.

There are two modules to all Policy and Procedure Acknowledgements. The first module is the P&P, and at the bottom of the P&P there is a blue "next" button. Once the user has finished reading the P&P, click this button that will then take the user to the next module. If this step is missed, then the system will show that only fifty percent of the Acknowledgement is complete.

If you have any questions or concerns regarding your account, please contact training@wfgnationaltitle.com.

WFG Compliance Program

The WFG Compliance Program incorporates the latest industry best practices, as well as CFPB's most recent guidance for third party settlement services providers.
Check out all the new information on our website