a la mode, inc.
The leader in real estate technology

Complying with the Gramm-Leach-Bliley ("GLB") Act

What is the GLB Act?

The Gramm-Leach-Bliley Act, passed in 1999 and fully effective in July, 2001, addressed overall financial industry reforms as well as emerging consumer privacy and security issues. Officially called the "Financial Modernization Act of 1999", it affects the technology and information system policies used by anyone engaged in providing financial services either directly or indirectly to consumers.

Under GLB, both the security and the privacy of a consumer's **non-public personal information ("NPI")** are protected. Charged with implementing the act, the Federal Trade Commission addressed the security and privacy components separately by issuing two distinct rules, the **"Safeguards Rule",** and the **"Privacy Rule".**
Appraisers are subject to the rules. All appraisers are required to implement at least the following:

- Under the Safeguards Rule, secure the transmission, receipt, and storage of data relating to any consumer's NPI at all times, via passwords, encryption, and physical protection, backed by a written information security plan
- Under the Privacy Rule, provide easily understood privacy statements to any consumers who engage the appraiser directly, disclosing the gathering, sharing, and security of NPI data, as well as the methods the consumer may use to opt-out of sharing of the data with third parties

Compliance is not terribly difficult, but it does require understanding of the rules and the methods available. This Best Practices document will hopefully provide appraisers with information and ideas useful in implementing GLB compliance as part of their overall regulatory compliance strategy.

Note: For a la mode clients, we've provided specific details at the end of this document regarding how to be in GLB compliance and protect the NPI you send and receive using our tools. Clients of other software vendors should contact their own vendors directly.

What non-public personal information ("NPI") am I receiving?

NPI includes loan terms, lender or mortgage broker name, sales concessions, co-borrower, unpublished phone numbers, other contact information, and of course more sensitive information as well. Even the fact that a particular consumer is engaged with a particular lender, at the time of the appraisal, is considered to be NPI if it has not been recorded in the public record yet or disclosed in some other way.

Whether or not some of the data might eventually be disclosed post-closing through recording of deeds and mortgages is irrelevant. At the time it is provided, it must be treated as NPI and accorded all of the security and privacy controls under the law.

Perhaps more importantly, the burden is on the appraiser to determine whether the data provided is public information or not. The institution – the appraiser – is required to have a "reasonable basis to believe" that the data is publicly available. In other words, research must have been done to determine its public availability first. One could

not assume that a phone number or an email address is publicly listed without verifying it. To be safe, anything about a particular borrower or individual, which is not absolutely known to be public at the specific moment the appraiser receives the information, should be strictly treated as NPI, and subjected to the appraiser's implementation of both the Safeguards and Privacy Rules.

Best Practices: It's safest to simply assume that an appraiser receives NPI on every assignment, and therefore, the Safeguards Rule precautions must be taken on every assignment. The Privacy Rule also applies at all times, but the actions the appraiser must take vary depending on whether the appraiser was directly engaged by the individual.

It's also important to note that the appraiser may not fall back on any state regulations which are less protective than the federal regulations. Only those state laws offering greater protection of the consumer's NPI, in the eyes of the FTC, are considered to apply.

Does it really apply to me?

GLB applies to financial institutions of all sizes. While appraisers may not think of themselves as a "financial institution", the Code of Federal Regulations [§ 4(k)(4)(F); 12 C.F.R. § 225.28] specifically defines appraisers as such: "*A personal property or real estate appraiser is a financial institution because real and personal property appraisal is a financial activity listed in 12 CFR 225.28(b)(2)(i) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act*."

Like all laws, opinions differ as to the level of applicability in particular circumstances (lawyers are, after all, paid to argue both sides). When evaluating whether or not a law applies, it's valuable to look at the intent of the legislators and regulators implementing it. In the case of GLB, the rules were submitted for industry comment by the FTC prior to adoption. The commission noted specifically that lenders requested specific waivers for the hundreds of thousands of appraisers, attorneys, and accountants in the settlement services chain.

The commission rejected the request, replying that the security of NPI must be maintained at every link in the chain and that lenders could not abdicate the responsibility of the Safeguards Rule at any point. The FTC considered the case of appraisal transactions specifically, and clarified in the public record that the rules do indeed apply to appraisers. Throughout the FTC's official business guides to the two rules, posted on its website, appraisers are specifically listed up front as being covered by each particular rule.

The FTC guidance is also very clear that size of the company is not an exception. A one-person appraisal shop is an "institution" under GLB and is bound by the law exactly to the same extent as any other institution.

It's important to note that the GLB rules apply to the institution, not the transaction, since the consumer's NPI is held by the institution and unrelated to a transaction's "federally related" status. A transaction also does not have to be successfully completed for the rules to apply. The consumer information merely has to be provided to any "financial institution" in the performance of financial services, such as appraising.

Just as FIRREA resulted in the creation of USPAP, the GLB act resulted in the creation of the Safeguards Rule and the Privacy Rule. Both are sets of rules created by federal agencies as a direct implementation of federal law, and both are non-optional in any appraisal firm's overall regulatory compliance obligations.

The practical application of the two rules in any size appraisal shop can be summarized this way:

The Safeguards Rule always applies to appraisers. A consumer's NPI must be securely handled at all times, regardless of where it originated, how it is held, or what type of transaction prompted it. The Privacy Rule only applies when the appraiser is directly engaged by an individual consumer.

Best Practices: GLB is just as applicable as USPAP to every appraiser. Appraisers handle NPI on virtually every appraisal, and should implement GLB compliance using simple, unbending rules. At the bare minimum, all transmissions with NPI, including the order and the final appraisal, must be via secure methods.

Realize that USPAP is talked about frequently among appraisers because it guides numerous individual valuation decisions, on a daily basis. But GLB similarly guides numerous individual data handling decisions, especially as related to emails to and from clients, on orders and final reports. It must become part of the appraiser's daily regimen.

As an analogy, most appraisers have encountered privacy hurdles attached to medical information under HIPAA. Medical providers, from dentists to insurance companies, are now required to provide additional disclosures to patients, cannot provide information even to other family members, and must provide checks and balances even in person to ensure only authorized access is granted to information. It changed everything related to how privacy of medical information is implemented. It affected virtually every aspect of any medical provider's daily interaction with the public, from phone calls to emails to paper storage.

GLB is effectively the financial counterpart to HIPAA, and its impact on even the most low-level tasks conducted in the completion of an appraisal should be considered no less sweeping.

What's the risk if I ignore it?

This is an era of substantial litigation with respect to privacy and security of data, in all industries. There are also increasingly broad state and federal investigations of specific mortgage-related fraud activity, with appraisers being fairly or unfairly caught in the middle of thousands of cases. The FBI lists mortgage-related fraud as its single fastest growing area of concern.

Perhaps most worrisome of all, action against an appraiser for violating GLB rules can also come from individuals, and could be used as settlement leverage by plaintiffs filing lawsuits over valuation disputes. The environment becomes rich for these types of suits as markets slow down, foreclosures go up, and lawyers for both consumers and lenders get involved.

Best Practices: GLB-related liability is always present. Don't increase legal exposure by ignoring it any more than ignoring USPAP. Compliance is much easier than it appears on the surface, much easier than USPAP, and much easier than responding to an investigation or lawsuit after the fact.

It's by no means necessary to panic, but it would be unwise for appraisers to treat compliance with these rules lightly. There's been little discussion to date in the appraisal community, but they do apply and they are clearly an issue.

As always, appraisers should consult their own legal advisors. This document is not intended to provide legal advice of any kind. It is merely our opinion of selected technological best practices for GLB compliance. Simply put, if we were in an appraiser's shoes, this is what we would do.

Why is this just now coming up?

GLB has been in force since mid-2001, so it isn't new. But with the combination of the mortgage boom and the post-9/11 focus on other areas of banking, GLB compliance took a back seat at most institutions, large and small. Recently however, with identity theft and mortgage fraud both capturing headlines, GLB is now squarely in the spotlight. As a provider of technology products directly to mortgage lenders and brokers, we were naturally asked by our customers in that market segment to carefully research GLB and ensure that our mortgage products were fully compliant.

In the process, we were surprised to find the clear references to appraisers and the lack of exceptions to the rules. Like most in the appraisal industry, we were not aware of the applicability to appraisers, nor the scope of the changes needed to comply.

Since we are now aware that most appraisers are not in compliance, and we are a service provider ourselves to appraisers who operate as financial institutions under the law, we feel we are obligated to notify appraisers of the relevant issues and to help them transition their businesses to practices consistent with the law.

GLB compliance is therefore now an integral part of our overall compliance support for appraisers, and part of our Best Practices series of documents.

How do the two rules affect me?

Safeguards Rule: Security and custody of consumer data

The Safeguards Rule requires that appraisers and all other financial institutions implement *written* security procedures to prevent NPI from falling into the wrong hands. The complexity and scope of the written protocols may be appropriate to the size of the institution, but core security of the NPI may not be abdicated. NPI must be secured using passwords and encryption during any sort of transmission, as well as during storage (and physically secured even when stored in paper form).

All institutions are required to respect the sensitivity of the NPI data in all phases of a transaction, and interact with service providers appropriately, according to their written information security plan. This written information security plan and the relevant protocols in it must be referenced in the privacy policy provided to the consumer (if the consumer directly engages the appraiser).

In the appraiser's role in the transaction, NPI data is potentially received electronically under many scenarios:

- Receiving an appraisal order via email
- Receiving sales contracts and other financial documents
- Transmitting final appraisal reports to the client
- Ad hoc emails with other service providers – agent, mortgage broker, loan officer, etc.

In addition to unauthorized access, the data must be secured from loss due to environmental hazards such as floods, as well as from technological hazards such as system failures.

Obviously, the appraiser must implement secure means of sending and receiving documents containing NPI. Utilizing regular emails with NPI data in the message body or attachments, and even with password protected PDFs, is not sufficient. (Appraisers of course normally send a final report PDF with a password preventing a client from editing the PDF, to prevent fraud. But that still does not prevent anyone else from reading the PDF with the NPI in it. Access to the data is undeterred by preventing the editing of the report.)

Best Practices: Adopt a "custodial" mindset on all NPI data received, thinking in terms of security as well as preservation. Develop a written information security plan and have it on file at all times, and review it regularly. The plan must specify steps used to secure any communications containing NPI. The easiest method is by using password-protected website delivery over SSL (Secure Sockets Layer).

Obviously, each appraisal firm will adopt different levels of implementation. But at its core, NPI data must be secured at all times.

There may be cases of course where the appraiser receives no NPI, and therefore, in hindsight, encryption would not have been necessary. It would be tempting for an appraiser to decide therefore that security overall is not needed until the presence of NPI is certain. However, the appraiser would not be aware of the scope of NPI until the data had already been received, which would already be a security breach if NPI was indeed present. The only safe route is to assume that NPI is present and secure all communications appropriately.

Note that encrypted email may also be used, but is more difficult to implement, since encryption keys must be exchanged manually with multiple providers. It's unlikely that the people dealing with an appraiser on a transaction will have encryption enabled in their email at all. But all recipients and transmitters of NPI in the transaction are likely to be able to click a link to an SSL-enabled website in an automated email, and to be able to set up password protected accounts on that site. There are many options available, both tailored to appraisers' needs and generic "off the shelf" secure delivery sites.

Regardless of the scope and type of encryption methods and processes used, developing a written security plan describing them is not optional. The law specifically requires that it be written and regularly reviewed. The appraiser must have it on file, and the privacy statement must refer to its presence.

Privacy Rule: Policy statements and opt-out provisions

Under the Privacy Rule, individuals fall into two categories: “consumers”, and “customers”. Consumers are any individuals who engage the institution at least once. Customers are simply consumers who have an ongoing relationship with the company. Both must be given privacy statements regarding the use of their NPI, and opt out notices at specific times and circumstances, by the institution they engaged.

That last phrase is essential. When a lender or other business client provides the appraiser with NPI on an individual as part of a transaction, the appraiser is not required to provide another privacy policy disclosure to the individual. The appraiser’s client must ensure that the suppliers it engages are in compliance with the privacy disclosures and opt-out notices it already provides to the individual.

Best Practices: Do not send privacy notices to consumers brought to you by a business client. The obligation is on the institution whom the consumer directly engages.

Appraisers who are indeed directly engaged by individuals must do the following:

- Provide a conspicuous and understandable initial notice of the privacy policy, covering handling of NPI, opt-out methods, and security safeguards
- Provide opt-out notices of sharing of NPI, with a "reasonable opportunity" to respond (weeks or months)
- Provide new revised privacy and opt-out notices if policies change
- For “customers” only, provide an annual privacy statement reminder for the duration of the relationship

Typically, an appraiser does not share the NPI with any non-affiliated third parties except where required to process the report. Appraisers don’t usually sell or otherwise distribute their databases for marketing purposes. Most appraisers should be able to invoke the exceptions to opt-out notification as provided in sections 313.13, 313.14, and 313.15 of the act.

Under section 313.14 in particular, appraisers would not be required to send an opt-out notification nor even provide notice that sharing of the NPI has been undertaken, when the party to whom the data is disclosed is a nonfinancial service provider used in processing the transaction. Likewise, in cases where the appraiser was not directly engaged by the consumer, the act of providing the data to the appraiser’s service providers would not be a violation of the original client’s privacy obligations to the consumer under section 313 of the law.

However, when directly engaged by the consumer and even when claiming exemption under any provision of section 313, the appraiser must provide the privacy policy statement up front in order to be granted the exception.

However, when directly engaged by the consumer and even when claiming exemption under any provision of section 313, the appraiser must provide the privacy policy statement up front in order to be granted the exception. Unless the consumer is aware of the policy overall, there can be no exceptions granted.

Also, note that the security provisions still apply. The appraiser must be sure that the service provider provides security controls, and that they are commensurate with the appraiser’s written security and safeguards policy.

Best Practices: Do not share NPI data with anyone other than service providers who meet your security standards, and you can generally use the opt-out exceptions in section 313. Treat all consumers and customer clients the same,

by providing the "initial," "revised," and "annual" privacy policy disclosures to every individual who has engaged you. Annual disclosures should be sent within the calendar year (i.e., by December of the year).

Remember that unless the privacy policy disclosures are provided in all three conditions (initial, revised, and annual), the exceptions under section 313 cannot be invoked.

The privacy statement itself needs to address how the NPI will be handled and disclosed (if at all), how the consumer may opt out, and how the appraiser safeguards the data.

The latter is why the company's individual safeguards policy must be in writing. The privacy statement does not need to include the full text of it, but it does need to state that the procedures are in place and are in writing.

Specific guidance for a la mode clients

Choosing an overall approach

The important thing when evaluating your options is to scale them to your needs, and remember that it's not "all or nothing". Improving security and compliance is a path, not a destination. It will never be "done" because the risks and methods constantly change. Don't feel like you have to have it all done tomorrow. You don't. You do need to start, and be educated, however. Security and privacy issues are not going away, ever.

If you're a smaller firm, you can keep it simpler. If you're larger, the risk and the expected standards for privacy communications, security, and employee training are probably higher.

Knock out the highest risk elements first. Generally, in the Safeguards Rule, you're most likely to get valuable NPI in the original order and in the documents sent to you as follow-ups (contracts and such).

Any time you receive or handle a document with a credit card number, an electronic bank account number, a loan account number, or an SSN on it, you're handling the most sensitive data in the consumer's NPI, and the security and privacy standards go up accordingly. Since you don't know when you'll receive an order that already contains something sensitive, it's usually a good idea to employ the strictest security all the time, up front, so that it's not "too late" by the time you see it.

That being said, you can apply different standards of security based on your beliefs of the risk. If, for example, you don't believe that digital faxes inside unencrypted emails pose a risk, approach that aspect last, or not at all. (But even eFax recognizes the non-compliance of unsecured faxes in email and has a system designed specifically for GLB requirements: http://www.efaxcorporate.com/corp/twa/page/glb).

It's your decision as to what level of compliance you think is "reasonable", given your environment.

Don't forget that some state privacy laws are stricter than GLB's own Privacy Rule. The privacy statements and the opt-out provisions of GLB should be implemented no matter what when dealing with consumers.

Finally, remember that top-level privacy and security are good business, and appealing to your clients. If you decide to "lead the pack", tell them. Market yourself as being in full GLB compliance. Turn your efforts into profit instead of just an expense.

Complying with the Safeguards Rule using our products

To comply with the Safeguards Rule, security and safety of the data is necessary – inbound, outbound, and stored on your systems – and you must have a written security plan. The following are suggestions for using our products and others for compliance.

- **Develop a plan.** Keep it simple at first – anything is better than nothing. For ideas in a "checklist" format, see http://bit.ly/2dFEIT2 or http://bit.ly/2eFMpfo.

- **Receive orders securely.** Avoid orders sent via email, as they can be intercepted and read easily (even attachments).

  If you don't have an XSite, use some sort of website which is SSL encrypted, and do not allow orders from it to be forwarded to you via unencrypted email. Likewise, faxed orders received via an online email fax service are not secure if they are delivered to you as attachments to unprotected email. Use a fax service with a desktop component which downloads the orders securely without email.

  If you have an XSite, use TOTAL Connect to pull down orders placed on your site, and those from plugin-capable clients, as it uses a secure connection.

- **Receive documents securely.** If you have others send you documents which are confidential, such as sales contracts, do not receive them as attachments to emails.

  If the document can be received as a secure fax (not as an attachment to an unencrypted email), use that technique.

  If you have an XSite, clients (or you on their behalf) can log into the site, click on an existing order, and electronically upload documents. You can also manually add these documents to TOTAL's Digital Workfile.

- **Transmit appraisals securely.** Sending a final PDF should also be done securely. Password protecting a PDF to prevent a client from changing it does not make it secure from viewing. Others can easily snoop on an unencrypted email in transit.

  If you have an XSite, use it to deliver final reports even if the order came in via phone or fax. When the client receives the delivery notification, they will be logging in and receiving the PDF over a secure connection.

  If you do not have an XSite, deliver the final report using DataCourier's secure email option in TOTAL. It avoids the PDF being attached to the unencrypted email, it notifies you that the client opened the actual PDF, and it is downloaded to the client via an SSL secure connection.

Complying with the Privacy Rule using our products

To comply with the Privacy Rule, you have to deliver and display privacy statements as well as provide opt out mechanisms to any consumer who engages you directly. Providing the privacy statements and opt out methods is not optional. There are exceptions to the opt-out conditions when sharing that data with third parties, but not to the provision of the privacy statements up front.

Remember, the opt-out clauses only have an impact when sharing data with certain types of third parties. Most appraisers will be unaffected since no sharing takes place. (But you still have to provide the opt-out mechanism and the privacy statement.)

Opt-out provisions may be stricter and more mandatory in some states (California, for example) than under GLB alone, so be sure you understand what other opt-out restrictions may be placed on you and try to incorporate those into your site as well. In any case, it's good business to have a strong, client-friendly opt-out policy.

- **Develop a privacy policy and opt-out mechanism.** Privacy policy examples are all over the web, on nearly every site you visit. Check out the GLB policies of your clients, posted on their sites, for examples too. Like the security plan, keep it simple at first – anything is better than nothing.

  If you have an XSite, there will be sample privacy policies available within it. (We will be adding opt-out flagging in your contacts database as well; if they opt out, it will tag their record in your database.)

  If you do not have an XSite, you can use your own sample policy, and add a mailbox for monitoring opt-out requests via your ISP or other mail carrier. Be sure to keep track of clients who opt out.

- **Post the policy conspicuously on your website.** It should be on the footer of every page, as well as in the main navigation. It should visually stand out. The law specifically requires that it be conspicuous.

  If you have an XSite, you can quickly add our template Privacy Policy page to your site's footer and navigation using the XSite Wizard. Simply check the boxes to add the page.

  If you do not have an XSite, use whatever method you currently follow to add pages, or consult your web designer.

- **Send the policy immediately any time you get a new consumer order.** As soon as you receive an order from a consumer, you must provide the policy. You do not have to make it a mandatory "click through" before accepting an order. You only have to provide it quickly enough after the order that the consumer would be able to opt-out before his or her NPI is shared with anyone. Generally speaking, you should send the notice as soon as the order is received.

- **Send your annual privacy policy statements en masse to all consumers you handled, as well as any time you change it.** By sending an annual statement to every consumer, you don't have to distinguish between "consumers" and the longer-term "customers". Also, send changed policies to everyone as soon as the change is made.

  End of year is a great chance to thank them for their business, and then also remind them of the policy and your high standards in handling their NPI. Use it as a marketing opportunity – not a sales pitch. It's a subtle opportunity to position yourself as a serious professional entity.

  If you have an XSite with XSellerate, use an XSellerate campaign set to trigger in December of each year, with your consumers selected automatically using the "groups" function. From then on it will be automatic. If you make a change to your policy at any time, simply trigger the same campaign to be sent immediately.

  If you do not have an XSite with XSellerate, use an email program to manually send your privacy notice every year. Be sure to set a reminder so that it doesn't fall off your list of end-of-year tasks. Likewise, be sure you send the policy again any time it's changed.

References

"Safeguards Rule" on the FTC's web site:
https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying
http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

"Privacy Rule", from the same FTC site: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/financial-privacy-rule.htm https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm

Code of Federal Regulations, from the Government Printing Office:
https://www.gpo.gov/fdsys/browse/collectionCfr.action?collectionCode=CFR

Developing an information security program:
http://www.federalreserve.gov/boarddocs/SRLETTERS/2001/sr0115a1.pdf