

# **THE HMDA INTERNAL ANALYSIS** **CONUNDRUM**

How to Avoid the Creation of Evidence to be Used  
Against You

By  
Wesley D. Few  
Matthew P. McGuire  
Frank A. Hirsch, Jr.  
Clark R. Abrahams

## **I. Introduction**

Virtually everyone knows the most basic of *Miranda* warnings to protect the rights of criminal defendants – “you have the right to remain silent; anything you say can and will be used against you in a court of law.” Lenders who must report data under HMDA do not have that option. Given both the financial and reputational risks at issue from HMDA reporting, it is more critical than ever that lenders understand the whys and wherefores of their HMDA data and vet the inferences that can be drawn.

The detailed internal analyses that must be performed to understand the data can generate documents and emails that could be discoverable in subsequent litigation. Given the overt litigation threats coming from the plaintiffs’ bar, that is not a pleasant option. Yet, reporting HMDA data without performing a fair lending analysis is corporate Russian roulette. This article examines recommended best practices to help avoid being caught on the horns of this dilemma.

## **II. Legal and Statutory Background for Potential Privilege Claims**

Lenders must understand the complex interplay between state and federal rules that can protect internal analyses of HMDA data from disclosure. Possible protections may be found in statutory and regulatory law, as well as the common law decisions of various courts. Because different jurisdictions vary in the way they construe and apply these protections, particularly where a common law privilege is asserted, a lender’s location (or the location of the dispute) may determine whether and to what extent it may protect internal analyses of HMDA data from disclosure.

**A. HMDA Self-Test Privilege**

When Congress amended HMDA, it authorized the Board of Governors of the Federal Reserve System to promulgate implementing regulations. 12 U.S.C. § 2804 (2000). These regulations create a limited privilege for self-tests conducted by lending institutions for the purpose of assessing HMDA compliance. 12 C.F.R. § 202.15 (2005). This limited self-test privilege expressly protects the use of surveys, fictitious mortgage applications, and similar techniques used to measure compliance, as long as they produce **new** data, as opposed to merely analyzing existing data.

However, reports generated by lending institutions that merely analyze existing HMDA data or existing loan files to assess compliance do not fall under this privilege, because they produce no **new** data. The self-test privilege specifically **excludes** “[l]oan and application files or other business records related to credit transactions, and information derived from such files and records, even if the information has been aggregated, summarized, or reorganized to facilitate analysis.” 12 C.F.R. § 202.15(b)(3)(ii). Furthermore, the official comments to 12 C.F.R. § 202.15(b)(1)(ii) further narrow the protection of this privilege:

The privilege does not protect a creditor’s analysis performed as part of processing or underwriting a credit application. A creditor’s analysis of its loan files, Home Mortgage Disclosure Act data, or similar types of records...does not produce new information about a creditor’s compliance and is not a self-test for purposes of this section. Similarly, a statistical analysis of data derived from existing loan files is not privileged.

Thus, the federal regulation itself provides limited comfort for the safeguarding of lender analytics.

## **B. Self-Critical Analysis Privilege**

The Self-Critical Analysis (SCA) privilege is a mostly common-law privilege of fairly recent origin that protects documents generated by institutions for purposes of critically analyzing some aspect of their business practices. This privilege is unevenly applied in reported cases. The SCA privilege typically is recognized only in the narrow fields of environmental litigation, litigation involving medical peer review, and Title VII discrimination cases. See, e.g., Reichhold Chem., Inc. v. Textron, Inc., 157 F.R.D. 522 (N.D. Fla. 1994) (environmental audits); Bredice v. Doctors Hospital, Inc., 50 F.R.D. 249 (D.D.C. 1970) (minutes of a hospital meeting evaluating the staff); Reid v. Lockheed Martin Aeronautics, 199 F.R.D. 379 (N.D. Ga. 2001) (Title VII discrimination case).

A few examples of the inconsistent application of this privilege by different jurisdictions shows the limited utility. Not all jurisdictions recognize the SCA privilege in the three contexts noted above. See, e.g., Aramburu v. Boeing Co., 885 F. Supp. 1434, 1440 (D. Kan. 1995) (refusing to apply the SCA privilege in Title VII cases). Other jurisdictions recognize a more expansive view of the SCA privilege. See, e.g., Reichhold, 157 F.R.D. at 525 (discussing cases applying the privilege in contexts different than those noted above). Some jurisdictions refuse to acknowledge the SCA privilege at all. Roman Catholic Diocese v. Morrison, 905 So. 2d 1213 (Miss. 2005) (refusing to recognize or create the SCA privilege); Payton v. New Jersey Turnpike Auth., 691 A.2d 321 (N.J. 1997) (declining “to adopt the privilege of self-critical analysis as a full privilege, either qualified or absolute”). Thus, lending institutions that wish to protect internal analyses of HMDA data under this common law privilege likely will face an uphill battle with an uncertain result.

The clear trend is a reluctance to expand the SCA privilege. This makes it unlikely that courts will utilize the SCA privilege to protect self-analysis performed by lending institutions. Such judicial abstention is typical. See, e.g., University of Pennsylvania v. EEOC, 493 U.S. 182 (1990) (stating, “although Rule [Fed. R. Evid.] 501 manifests a congressional desire “not to freeze the law of privilege” but rather to provide the courts with flexibility to develop rules of privilege on a case-by-case basis, we are disinclined to exercise this authority expansively”); Southern Bell Telephone and Telegraph Co. v. Beard, 597 So.2d 873, 876 n.4 (Fla. 1<sup>st</sup> D.C.A. 1992) (noting that Florida state courts are forbidden from adopting new privileges by judicial decision); Cloud v. Superior Court, 50 Cal. App. 4th 1552 (Cal. App. 2d Dist. 1996) (refusing to find a common law self-critical analysis privilege and noting that “[t]he privileges contained in the California Evidence Code are exclusive and the courts are not free to create new privileges as a matter of judicial policy”).

The overwhelming majority of jurisdictions that recognize the self-critical analysis privilege have codified it as it applies to medical peer-reviews, environmental audits, or both. Any expansion of the privilege to cover financial institutions, therefore, is likely to occur only through legislative action. See, e.g., Wells Dairy, Inc. v. Am. Indus. Refrigeration, Inc., 690 N.W.2d 38 (Iowa 2004) (“Our legislature has recognized the self-critical-analysis privilege in the context of medical peer review committees. We decline to judicially extend the self-critical-analysis privilege, and we leave it to the legislature to do so if it finds the competing policy concerns weigh in favor of such an extension of the privilege.”)(citations omitted).

Two states (Louisiana and North Dakota) have adopted by statute a SCA privilege that may apply to a lending institution. See La. R.S. 6:284.1 (LEXIS 2005); N.D. Cent. Code § 6-13-02 (LEXIS 2005). A caveat, however, is that the scope and applicability of these statutes

vary. The North Dakota statute refers to a SCA privilege for all “financial institutions” governed by federal law. By contrast, the Louisiana statute refers only to a SCA privilege for **state** banks where the self-analysis is done as a result of compliance procedures created by a committee of the state bank’s board of directors.

Government regulation of lending institutions also makes it extremely unlikely that courts will expand the SCA privilege to protect self-analysis of HMDA data. Because HMDA regulations already contain a limited self-test privilege, courts most likely will resist changing the scope to cover an area which existing regulations decline to reach. See U.S. ex rel Falsetti v. Southern Bell Tel. & Tel. Co., 915 F. Supp. 308, 311 (N.D. Fla. 1996) (“We are especially reluctant to recognize a privilege in an area where it appears that Congress has considered the relevant competing concerns but has not provided the privilege itself. The balancing of conflicting interests of this type is particularly a legislative function.”) (citations omitted).

Even if a court recognizes the common law SCA privilege as it may apply to financial institutions, it remains uncertain whether self-generated reports analyzing HMDA data would fall under its protection. Courts have applied varying test-criteria for the SCA privilege to attach, but all tests include some form of balance of the public benefit of protecting SCA from disclosure against the needs of an individual plaintiff for discovery.

The application of this balancing test does not always favor the attachment of SCA privilege. In Warren v. Legg Mason Wood Walker, Inc., 896 F. Supp. 540 (E.D.N.C. 1995), for example, the plaintiff alleged negligent supervision of defendant’s employee, an investment broker, who managed plaintiff’s investment accounts. The plaintiff sought disclosure of the broker firm’s internal branch audits. In its analysis of whether the internal

audits could be protected from disclosure, the court pointed out that “the self-critical analysis privilege exists out of concern for the public and is not personal to the one asserting the privilege.” The court went on to note that the intent of the broker company when conducting an internal audit was to “discover any wrongdoing and correct it.” Despite this apparent acknowledgment that the broker company was engaged in self-evaluation, the court held that the SCA privilege did not apply because “[d]efendants should not be allowed to shield the results...regardless of whether they contain evidence of wrongdoing, because [the] audits were done to protect defendants’ clients and the public in general.” This is a tough result for the SCA privilege under North Carolina law.

Pennsylvania has used the balance differently. In Clark v. Pennsylvania Power & Light Co., 1999 U.S. Dist. LEXIS 5118 (E.D. Pa. 1999), an employee brought a gender discrimination claim against her public utility employer. The employee sought disclosure of the utility’s affirmative action plan and reports regarding implementation of the plan. The district court found that the subjective parts of documents created by the public utility in order to assess and ensure compliance with Title VII requirements were protected by the SCA privilege. But, the objective data contained in the documents were not protected. The court also found that the employee failed to show a “compelling need” for the documents in that she would have access to the objective data and so could formulate her own subjective conclusions as to the utility’s compliance. Good news for the SCA privilege, but this was in the factual context of a discrimination claim.

Given the uncertainty surrounding application of the SCA privilege, even lending institutions in jurisdictions that recognize this privilege should not depend solely upon it to protect internal analyses of HMDA data from disclosure. As a first line of defense, HMDA

evaluators should put very little in writing and seek to communicate orally as much as possible among a small control group. As a second line of defense, lending institutions should prepare evaluative reports in such a way to enable easy separation of all subjective analysis and conclusions from the objective data used to perform the analysis. Preparing reports in this way will bolster the argument that an opposing party seeking discovery has access to all necessary facts to reach its own conclusions, and perhaps tip the balancing test in the direction of the application of the SCA privilege.

### **C. Work-Product Doctrine**

Another potential common-law protection is the work-product doctrine, which protects documents prepared by or for another party in anticipation of litigation. Work product is a limited privilege. It can be overcome if a party shows a substantial need for data and no reasonable opportunity to obtain it elsewhere.

The major problem with attempting to protect a lending institution's internal reports with the work-product doctrine is the "anticipation of litigation" requirement. To meet this requirement, the threat of litigation has to be both real and imminent. As applied in McCoo v. Denny's, Inc., 192 F.R.D. 675, 683 (D. Kan. 2000), this means that "[t]he inchoate possibility, or even likely chance, of litigation does not give rise to the privilege." As such, it seems unlikely that the work-product doctrine would assist lending institutions in protecting their internal reports analyzing HMDA compliance which are generated in the ordinary course of business. The privilege could apply only if an analysis of specific HMDA data is undertaken in response to a lawsuit or threatened lawsuit by an identifiable party or parties.

**D. Attorney-Client Privilege**

The most likely source of protection for lending institutions' internal HMDA analyses is the attorney-client privilege, which protects confidential communications between client and lawyer for the purpose of seeking or obtaining legal advice. Lending institutions may seek protection of internal reports by having their attorneys both provide the analysis and generate the reports. While there is no guarantee that such a strategy will succeed in every jurisdiction, it is the most assured path to protect internal analysis of HMDA data. As recently noted by the ABA Section on Litigation,

The entire area of internal audits continues to be a troubling one for corporations, since the findings of such an audit...are not necessarily privileged. Companies conducting such audits would be well advised to attempt to structure the audit as fact gathering with the purpose of giving legal advice. It is not certain that such structuring will be sufficient to erect a wall of privilege. Yet without it, it is fairly certain that the privilege will not apply.

The Attorney-Client Privilege and the Work-Product Doctrine, 53 (Edna Selan Epstein, ed., ABA 4th ed. Supp. 2004). The above comment was made in the context of a legal audit performed in reaction to malfeasance by a company's employee, and not regarding compliance with HMDA. As noted in Seibu Corp. v. KPMG LLP, 2002 U.S. Dist. LEXIS 906 at \*9-10 (N.D. Tex. 2002), the "critical inquiry is whether...any particular communication in connection with [the] investigation facilitated the rendition of legal advice to the client."

In this context, as discussed below, lending institutions should structure their internal analysis and reporting so that a report generated to analyze data for compliance with HMDA "facilitates the rendition of legal advice." While the individual data components included in the report likely would not be privileged, the subjective components of the report should be.

### **III. Creating an Effective Stakeholder Communication Program – Implications for Preventing Unwanted Disclosure of Internal Self-Audits and Compliance Reports**

The following guidelines address how to assist an institutional lender’s legal department in setting up an internal analysis structure. This structure should be flexible and sufficiently comprehensive to support regularly scheduled activities such as internal compliance reviews, internal audit examinations, and external examinations conducted by the lender’s regulators. In addition, the structure should also support activities necessitated by unscheduled events, such as customer complaints, class action lawsuits, self-initiated or referral investigations by government enforcement agencies, reports on the lender’s fair banking performance developed by community-based organizations, consumer advocate allegations of predatory lending or redlining, and academic research inquiries.

In order to avoid unwanted and potentially damaging disclosure of subjective internal analysis, the lending institution’s staff must adhere strictly to a detailed set of procedural guidelines that define the appropriate process for a given situation. This section reviews the key concerns that must be addressed and associated procedures that should be implemented to create the internal structure that will support the required analysis, while providing all possible legal protections from disclosure. The implications for software solutions are also discussed where applicable.

At the highest level, a compliance self-testing program cycle consists of four basic phases, as shown in Figure 1 below:

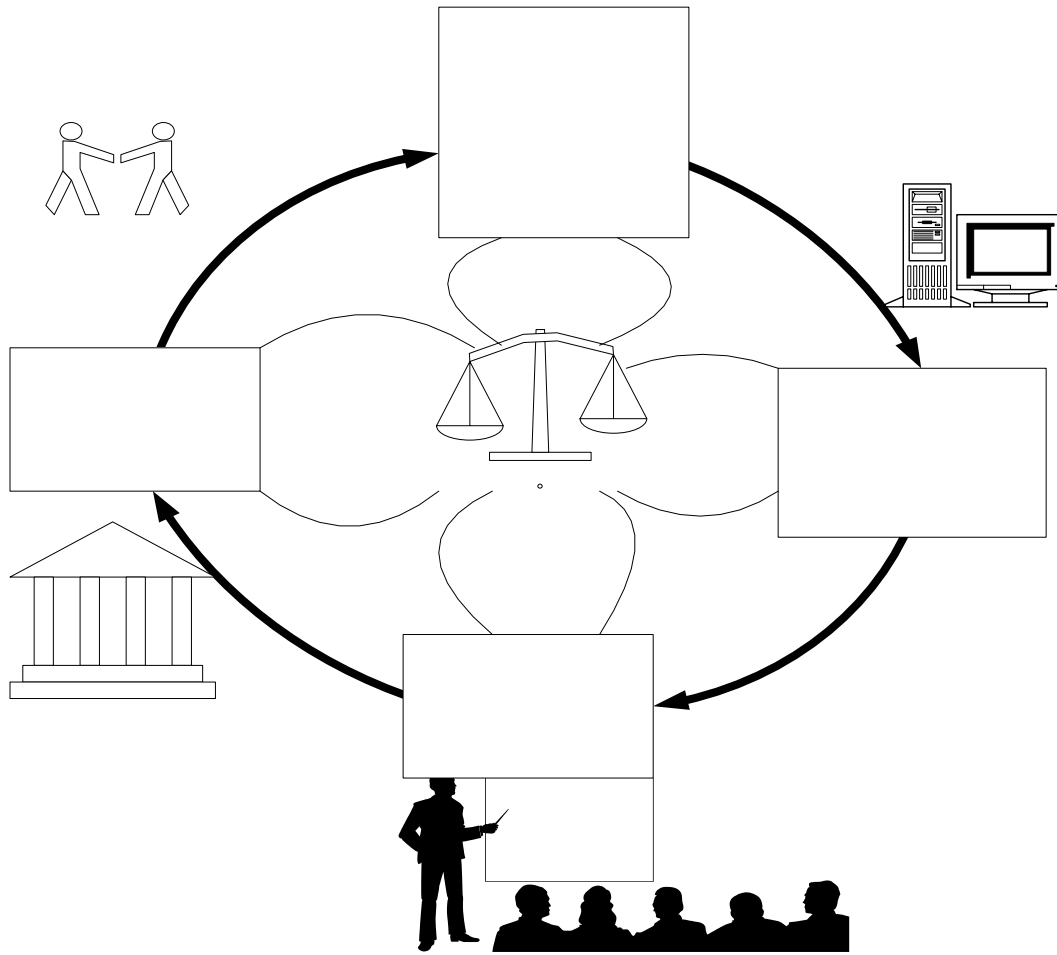


Figure 1. A Compliance Self-Testing Program Cycle

It is important that the appropriate communication discipline be in place, and that strict confidentiality be maintained, in each of the four phases. The following guidelines apply to all phases, and they also apply in the non-routine situations that require a formal, or public, response from the lending institution.

## Partnership: Line Org & Compliance

**A. Administration**

As a general rule, involve legal counsel prior to engaging in any self-assessment activity. As a first step, legal counsel will typically send out a request memo (Figure 2 below).

<b>“Confidential; Attorney-Client Privileged Communication”</b>
<b>Institution Name</b>
<b>Attorney Name</b>
<b>City</b>
<b>Date</b>
<b>Subject: Self-Testing Project for: &lt; Title of Project &gt;</b>
<b>(Addressees)</b>
<b>Please conduct (description of self-testing project). Please send all related material and any findings to the attention of (specific attorneys).</b>
<b>Chief Legal Counsel for Fair Lending Assessment</b>

Figure 2. Sample Request Memo

In every instance where a compliance matter is investigated, either as part of a routine examination process, or due to a special request, there should be an individual appointed to be responsible for maintaining all records in an organized fashion for safekeeping. The same individual who serves as the custodian of all relevant material relating to the compliance matter may, where appropriate, also serve as the point person for:

- Fielding inquires;
- Providing legal affidavits;
- Conducting due diligence;
- Giving depositions;
- Attending depositions;
- Attending court sessions;
- Preparing cross examination questions;

- Providing testimony in court.

Note that the custodian of compliance data and documents is not necessarily the corporate secretary, who routinely receives and responds to subpoenas from a grand jury, state attorneys general, etc. Custodial responsibilities can be specific to a particular matter or they could span several compliance matters.

## **B. Verbal Communication**

Directions to staff who may be involved in gathering factual information or performing analysis pertaining to a compliance matter must be crystal clear. Specifically, all compliance team and non-compliance team staff who are asked to compile information in conjunction with a compliance matter must be informed at the outset that they:

1. Must treat the compliance matter as strictly confidential and that they cannot discuss it with others, either inside or outside of the lending institution. Disclosure of the confidential communication to any non-privileged parties automatically and instantly waives the privilege (even if unintentional). As a result, disclosure of information related to the self-testing project can take place only at the direction of the responsible attorney for the matter in question; and
2. Must not create any written documentation related to the compliance matter, except as directed to do so by the designated legal counsel. Any written material must be created, distributed and maintained in accordance with the guidelines for written communication that appear in the following section.

Rules pertaining to meetings, teleconferences, web-based whiteboard/placeware sessions that are held to discuss a compliance matter and any information pertaining to it include the following:

1. Never hold any meetings, conduct any teleconferences, or present any material via web-based communication vehicles that relates to information being gathered, analytical findings, or to discuss the compliance matter without notifying the appropriate legal counsel and the compliance team leader in advance.

**Important:** The responsible attorney, and the compliance team leader, will jointly direct precisely how such communications should be handled.

2. Never generate any written or electronic material related to any meeting (including notices and agendas) without obtaining the advice of the responsible attorney.

**Important:** Always contact the responsible attorney to discuss the need for meetings, teleconferences or web-based sharing of information related to a compliance matter.

**Special Case: Verbal External Communications with Vendors and 3<sup>rd</sup> Parties**

In instances where information is needed from external sources, verbal requests should never disclose the fact that a compliance matter is being investigated, or why the information is being requested. If asked, the external party should simply be informed that the inquiry pertains to an internal matter.

**C. Written Communications**

**1. Notification**

All documents pertaining to the compliance matter should have a standard notification footer on each and every page (attachments included).

CONFIDENTIAL INFORMATION SUBJECT TO ATTORNEY CLIENT AND ATTORNEY WORK-PRODUCT PRIVILEGES. DO NOT COPY OR DISSEMINATE WITHOUT PRIOR APPROVAL FROM _____ < Insert Name of Institution > LEGAL COUNSEL.
--

Figure 3. Example of Standard Notification

**Note:** Do not restrict to the lender’s legal department, because their legal counsel on certain matters may be external—this handles all cases.

The implication for software solutions is that all fair lending and HMDA analysis procedures, computer programs, data displays, report screens, report images, visualization screens and screen captures, mapping images, hardcopy maps and reports, and all other documents related

to fair lending compliance matters must have the standard notification on every page and screen.

E-mails and all electronic documents also should have this standard notification. In addition, a distribution notification should be placed at the bottom of the e-mail.

"Confidential Notice. This transmittal constitutes a confidential attorney-client communication or it may otherwise be privileged or confidential. If you are not the intended recipient, then you have received this transmittal in error and you are prohibited from review, dissemination, distribution or copying any/all of this transmittal. If you have received this communication in error, please notify legal counsel immediately at \_\_\_\_\_ <Insert Name of Institution, phone number, or e-mail contact> and delete this message (and any/all attachments, if any)."

Figure 4. Example of Distribution Notification

**Note:** E-mail attachments require the standard notification on every page.

The implication for HMDA software solutions is that the solution should include the distribution notification on automatic e-mail notifications from all alert engines that are designed to provide notice of potential compliance violations. A possible exception to this rule would be the HMDA submission file data cleansing process, wherein e-mail notifications of invalid data may be triggered by a HMDA edit failure alert engine and routed to operations staff for corrective action. This, and any other proposed distribution notification exceptions, should be reviewed and approved by legal counsel in advance of planned implementation of software solutions to ensure the vendor-supplied solution is properly configured to support what is required.

## 2. Distribution<sup>1</sup>

There are several distribution issues to consider involving compliance matters, which for purposes of this discussion are defined as any specific concern or issue that is the focus of either a routine examination, or a special study that may be triggered by an internal or external request or event.

### Issue 1. Information sourced or created

Compliance reports analyzing HMDA data should be generated by attorneys. In the event that it is necessary for someone with special training and technical education to access the required information and perform the analysis (e.g., a Ph.D.-level statistician) the following precautions must be taken:

- All documents must be addressed directly to the attorneys responsible for compliance self-testing;
- All documents should be sent by the person who has directly obtained the information and performed the analysis on that information (hence creating new information);
- The outside party should be retained by the attorney and should have a written agreement whereby it is made clear that he is conducting his analysis for the attorney on behalf of the client.
- **Caution:** The situation where one party collects information and then sends it on to another party, who in turn sends it on to the attorney, is to be avoided at all cost.

### Issue 2. Information that is copied

When copies are made, the same procedure should be followed as in subparagraph 1, with the additional provision that no one should be copied on any correspondence with the attorney

**Note:** Copies may be maintained at the source provided they are maintained in a file in a locked environment to prevent unauthorized access. The jacket of that file must have the standard notification.

---

<sup>1</sup> Including copying and maintenance of documents, including compliance audits and reviews, executive briefings on findings extracted from audit reports and compliance reviews, etc.

### **Issue 3. E-Mails**

E-mails must bear the distribution notification. All individual e-mails must be maintained by individual senders and receivers of those transmissions in a separate folder for each compliance matter.

### **Issue 4. Intranet Broadcast**

Reports and screens on the company's private network relating to the compliance matter must bear the standard notification. Access must be restricted to those individuals expressly approved by legal counsel.

### **Issue 5. Internet (Web-Based) Broadcast**

Web-based reports and screens relating to the compliance matter must be encrypted and bear the standard notification. Access must be restricted to those individuals expressly approved by legal counsel.

## **3. Content Scope for Written Material**

All written materials (independent of the medium on which they reside) must be limited to an objective, factual description of the specific matters that are the subject of the compliance testing process or matter that is being investigated (triggered by customer complaint, discovery order, request letter, regulatory examination, etc.).

## **4. All Other Written Communications**

In situations where there is a compliance team, a designated team leader can request that non-compliance team staff communicate with other employees of the lending institution in writing or by email in the course of gathering information during an assessment or analysis phase. All such communications must include both standard and distribution notifications.

At the close of the assessment and analysis phases, all documents and copies of documents (including written communication, correspondence, associated materials, hard copies of e-mails, screen prints of data, reports and models, CD-ROM media containing soft copies of related documents, data, models and results) should be returned to the team leader.

#### **5. All EDP-Related Material**

Computer program specifications and source code, data, metadata, documentation, project files and plans, reports, intermediate output files, testing-specific or methodology manuals and guides, and all other material in hard or soft copy form must be secured at the direction of legal counsel. This includes, but is not limited to, password protection of every individual document created, file encryption where warranted, physical restriction using key or combination locked rooms housing dedicated servers, hardcopy files, and staff work areas.

#### **6. Aggregated Data**

Attorneys should be provided the HMDA data in raw form, allowing them to aggregate the data for the purpose of generating all reports and their accompanying analyses. This provides the safest way to protect aggregated data.

**Caution:** Record retention procedures and all routine purging and destruction of documents relating to the *compliance matter* must be suspended if counsel issues a “hold order.”

The implication for software solutions is that they must possess the ability to restrict access to all fair-lending functional reporting, analysis, and visualization capabilities in the solution to only those staff that have been approved by legal counsel. Furthermore, the capability must also exist to restrict access to segments of data, or to particular data elements, in the solution. In the earlier discussion of self-testing privilege, it was noted that reports generated by lending institutions that merely analyze existing HMDA data or existing loan files do not fall under this

privilege because they do not produce new data. If, however, the lender combines HMDA filing data and loan file data with new, and/or updated data relating to topics such as the following:

- 1) channel;
- 2) the property financed (e.g., rapid appreciation/depreciation);
- 3) market (relative to timing, shifts, and volatility);
- 4) borrower risk changes (e.g., credit score migration, recent payment performance, current borrower indebtedness, and alternative credit scores based on remittance data); and
- 5) exercise of options subject to the terms and conditions of the mortgage agreement;

and if the lender creates a summary indicator based upon the totality of the information, then it is likely that the combination would be considered new information under the self-testing privilege rule. It is recommended that, notwithstanding the somewhat intuitive conclusion regarding the protection of information in the form of a global fair lending risk indicator,<sup>2</sup> institutions should seek a legal opinion on how best to handle this type of analysis.

## **7. External Communications with Vendors and Third Parties**

In instances where information is needed from external sources, written requests should never disclose why the information is being requested, nor should they include either the standard or distribution notification.

---

<sup>2</sup> A definition and description of a global fair lending risk indicator appears in Abrahams and Zhang (2005) *Managing Risk Exposure with SAS's Global Indicator: Fair Lending and Beyond*, A SAS Institute White Paper. Essentially, the indicator provides the ability to examine fair lending performance from a variety of perspectives using a standardized risk indicator that captures the overall potential fair lending risk for any well-defined subset of the HMDA loan application records.

There are additional caveats for HMDA and fair lending software solution providers. Because in-house counsel may have more difficulty asserting a particular privilege, the solution vendor may need to license the solution to an external law firm that represents one or more clients who require the type of compliance support it affords. There are also traps for the unwary depending on how the product is implemented. Alternatives to the typical installation on site at a client lending institution's facility would include at least the following: 1) installation on a law firm's computer; 2) installation in an ASP arrangement internal to the solution vendor; 3) installation in an ASP arrangement through a third-party provider; or 4) installation on a consulting firm's computer, where the consulting firm in question is retained by the law firm representing a particular client and the consulting firm performs the analysis under the direction of the law firm on behalf of its client.

In either the consulting firm scenario, or the ASP setting, there are complications due to privacy regulations that may require that every distinct client organization have its own data maintained on an entirely separate computer. This is especially true in cases where customer identifying data is maintained. The lending institution should seek a legal opinion to determine which arrangement affords the best protection of its internal analytical documents. One arrangement may also be preferable based upon other important factors, such as operational risk, regulatory concerns, total cost of ownership, segregation of duties, availability and maintenance of in-house expertise, responsiveness, and preservation of critical data.

Finally, communications addressed to, or written by, attorneys may not be shared in any way. In the event that distribution to other parties is required, the appropriate attorney should be contacted and the attorney should send the communication directly to those parties using a distribution memo (Figure 5 below):

“Confidential; Attorney-Client Privileged”
Institution Name
City
Date
Subject: <Title of self-testing project>
(Addressees)
Contained herein are the results of (description of self-testing project). Any questions regarding this material must be directed to (Corp. Fair Lending Manager or Attorney in Charge of the matter). This information may not be further distributed. Copying of this information is expressly prohibited.
Name of Legal Counsel

Figure 5. Sample Distribution Memo

By following the aforementioned procedures diligently, the lender can be assured they have taken all possible steps to protect their internal self-audits and compliance reports from discovery. Like a chain, the process is only as strong as the weakest link. Therefore it is critical to ensure that once the proper process is developed and deployed, that it is followed without exception.

**IV. A Final Caution – Avoiding the Spoliation Trap**

Document and data management has become a costly and time-consuming issue for many companies. Adding to the otherwise considerable burden is the duty to preserve indefinitely documents and data pertaining to the subject of anticipated litigation. This obligation, which has been the subject of much discussion in recent years by courts across the country, presents difficult issues for lending institutions which undertake an internal fair lending analysis. Given the controversy surrounding the recent release of HMDA data, some lenders could reasonably anticipate litigation concerning significant portions of their loan

portfolios. The dilemma for those companies is when to institute “litigation holds” on the routine destruction of documents and data pursuant to existing retention policies. On the one hand, failure to retain documents and electronic data that could be relevant to future litigation could result in draconian sanctions down the road. On the other hand, retaining vast quantities of documents and electronic data imposes severe burdens from both a time and cost perspective. This is an issue that will become more prominent in the future, not less. Thus, companies that maintain extensive volumes of documents and electronic data must plan now for how to deal with the inevitable onslaught of burdensome discovery.

**A. Spoliation of Evidence**

Document control issues have taken on a growing importance in complex litigation in recent years. No longer can defendants wait until they are served with a request for production to begin collecting documents and electronic data. Federal and state courts are increasingly willing to impose heavy sanctions -- even outcome determinative sanctions such as a default judgment -- when a party fails to retain and produce relevant evidence after receiving notice of a potential dispute. Such sanctions are usually based on some variation of the legal theory called “spoliation of evidence”.

Generally speaking, spoliation is “the destruction or significant alteration of evidence, or the failure to preserve property for another’s use as evidence in pending or **reasonably foreseeable** litigation.”<sup>3</sup> When spoliation occurs and evidence is lost because of a party’s neglect or misconduct, courts may sanction the offending party to remedy the inequitable

---

<sup>3</sup> Byrnie v. Town of Cromwell, 243 F.3d 93, 107 (2d Cir. 2001).

effects of the spoliation, to punish the spoliator, and to deter further misconduct by other litigants.<sup>4</sup>

## **B. Spoliation Sanctions**

The cost of spoliating evidence, even negligently, can be devastating. Courts have a wide panoply of sanction options, including granting default judgment in favor of the prejudiced party, suppressing the offending party's evidence, imposing fines, awarding attorney's fees, or, most commonly, giving an adverse inference that permits a jury to infer that "destroyed evidence might or would have been unfavorable to the position of the offending party."<sup>5</sup>

The court's opinions in the Zubulake case provide an instructive overview of how spoliation principles can alter the course of litigation. A party seeking to impose sanctions on a party that has destroyed or otherwise failed to produce requested evidence or documentation must demonstrate: "(1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed with a 'culpable state of mind' and (3) that the destroyed evidence was 'relevant' to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense."<sup>6</sup>

In determining the appropriate level of sanction, the court must consider the degree of the spoliator's fault, the degree of prejudice suffered by the opposing party, and whether a lesser sanction that would serve the remedial, and any punitive purpose of the sanction.<sup>7</sup> The

---

<sup>4</sup> Mosaid Technologies Inc. v. Samsung Elec. Corp., 348 F. Supp. 2d 332, 335 (D.N.J. 2004); see also Zubulake v. UBS Warburg LLC, 2004 WL 1620866 at \*6 (S.D.N.Y.) (hereinafter Zubulake V) (noting that the Rules of Civil Procedure and the court's inherent powers permit a court to sanction litigants who fail to preserve evidence); Wal-Mart Stores, Inc. v. Johnson, 106 S.W.3d 718, 721 (Tex. 2003) (noting that a trial court has discretion to fashion an appropriate remedy for spoliation).

<sup>5</sup> Schmid v. Milwaukee Elec. Tool Corp., 13 F.3d 76, 79 (3d Cir. 1994).

<sup>6</sup> Zubulake V, 2004 WL 1620866 at \*6.

<sup>7</sup> Mosaid, 348 F. Supp. 2d at 335.

most common sanction, the spoliation inference, may be imposed when (1) the evidence in question is in the spoliator's control; (2) there has been actual "suppression or withholding" (e.g., destruction) of the evidence; (3) the evidence destroyed was relevant to underlying claims or defenses; and (4) it was reasonably foreseeable that the destroyed evidence would later be discoverable.

Lest anyone doubt the potential impact of a spoliation sanction, the 2005 decision in Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.<sup>8</sup> serves as a wake-up call. Email back-up tapes were at the center of the problem. This case arose out of Sunbeam Corp.'s acquisition of Coleman Co. After accounting fraud was discovered at Sunbeam, its stock price collapsed and Coleman's parent sued Morgan Stanley for allegedly knowing about the fraud and Sunbeam's inflated stock price, and failing to disclose material information. During discovery, Morgan Stanley falsely certified in June 2004 that it had complied with a court order to review its oldest backup tapes and produce emails relevant to the Sunbeam/Coleman deal. In fact, Morgan Stanley failed to review well over two thousand back-up tapes, the existence of which it was objectively aware of at the time of the certification, failed to notify Coleman about the additional tapes until November 2004, continued to discover back-up tapes that had not been searched for relevant emails well into 2005, and did not withdraw its certificate of compliance until shortly before the trial was due to begin.

The court found that Morgan Stanley had committed numerous willful and gross abuses of its discovery obligations and imposed a number of harsh sanctions to "level the playing field." The sanctions included giving an adverse inference jury instruction, reading a

---

<sup>8</sup> No. 2005 WL 679071 (Fla. 15<sup>th</sup> Jud. Cir. Mar. 1, 2005).

statement of conclusive facts to the jury regarding Morgan Stanley’s discovery abuses, allowing Coleman to argue in the punitive damages phase of the case that Morgan Stanley’s concealment of its role in the Sunbeam transaction was evidence of malice or evil intent, shifting the burden of proof on the fraud and conspiracy claims to Morgan Stanley, and ordering Morgan Stanley to pay the costs of the sanctions motion. The jury returned a verdict for \$604 million in compensatory damages and \$850 million in punitive damages.

**C. Scope of the Spoliation Doctrine**

Companies involved in litigation must understand the expansive scope of the spoliation doctrine. Sanctions are not limited simply to those entities which willfully destroy documents and attempt to cover up their malfeasance. To the contrary, courts are increasingly inclined to impose spoliation sanctions in a wide variety of cases involving arguably “innocent” document destruction. Here are three imperative areas to understand.

**1. Motive or “Bad Faith” Is Not Always Relevant**

A party’s good faith is usually irrelevant to a spoliation charge. In many instances, documents are shredded and emails are deleted pursuant to routine document retention policies that are implemented by employees who are either totally unaware of pending litigation, or are unaware of the importance of the destroyed documents to the pending litigation. Unfortunately, a document retention policy provides little or no defense to a spoliation claim. In general, courts expect a document retention policy to give way to a party’s duties to preserve evidence for litigation.<sup>9</sup>

---

<sup>9</sup> See, e.g., Stevenson, 354 F.3d at 750 (defendant “cannot rely on its routine document retention policy as a shield”); Renda Marine, 58 Fed. Cl. at 61 (“The court does not believe that a records retention policy which is inconsistent with a party’s obligations to a potential or actual adversary in litigation operates to excuse the party’s failure to respond to discovery.”).

Some courts have sanctioned defendants for acting negligently by failing to take reasonable precautions to preserve evidence.<sup>10</sup> In those jurisdictions, a plaintiff need only show that the destruction of relevant evidence occurred, and that such destruction could have been prevented if the defendant had taken reasonable precautions. Conversely, some jurisdictions do require a showing that the destruction of evidence occurred either intentionally or in “bad faith”.<sup>11</sup> Most companies do business in many jurisdictions across the country; therefore, the stricter, negligent spoliation standard should provide the guidepost for future document and data management.

## **2. Lack of Relevance of Destroyed Evidence Is No Defense**

An often-heard defense to spoliation charges is that the destroyed evidence or data is not relevant to any issue or claim in the case, and thus sanctions should be denied. This argument has intuitive appeal, since in many cases plaintiffs serve overly broad document requests. Yet, there is no safe harbor here either. Some courts may and will presume the relevance of destroyed documents and data.<sup>12</sup>

---

<sup>10</sup> See Zubulake V, 2004 WL 1620866 at \*6 (negligence standard); Mosaid, 348 F. Supp. 2d at 338 (negligence standard); Ward v. Texas Steak Ltd., 2004 U.S. Dist. LEXIS 10575 at \*8 (W.D. Va.) (negligence standard; applying Virginia law); Residential Funding Corp. v. DeGeorge Financial Corp., 306 F.3d 99, 108 (2d Cir. 2002); Kucala Ents. Ltd. v. Auto Wax Co., 2003 U.S. Dist. LEXIS 8833 at \*13-14 (N.D. Ill. May 27, 2003)(discovery sanctions can be imposed for gross negligence); Pfantz v. Mid-Century Ins. Co., 85 P.3d 564, 569 (Colo. 2003) (negligence standard).

<sup>11</sup> See, e.g., Hodge v. Wal-Mart Stores, Inc., 360 F.3d 446 (4<sup>th</sup> Cir. 2004); Stevenson v. Union Pacific R.R. Co., 354 F.3d 739, 746-47 (8<sup>th</sup> Cir. 2004); Bashir v. Amtrak, 119 F.3d 929, 931 (11<sup>th</sup> Cir. 1997); Renda Marine, Inc. v. United States, 58 Fed. Cl. 57, 60 (2003); Aramburu v. Boeing Co., 112 F.3d 1398, 1407 (10<sup>th</sup> Cir. 1997). Cf. Concord Boat Corp. v. Brunswick Corp., 1997 WL 33352759 (W.D. Ark.) (noting split among the federal circuits as to whether bad faith was a required element of spoliation).

<sup>12</sup> See, e.g., Residential Funding, 306 F.3d at 109 (holding that where a spoliator’s gross negligence is demonstrated, the fact finder may infer that the destroyed evidence is relevant); Kucala, 2003 U.S. Dist. LEXIS 8833 at \*18 (although the trial court admitted it had no direct evidence that relevant documents were among those destroyed, the court expressly considered the likelihood that relevant documents were lost in mass deletion in determining appropriate spoliation sanction).

### 3. When Does the Duty to Preserve Arise?

Perhaps the greatest dilemma facing companies that must manage significant volumes of data and documents is determining precisely **when** the duty to preserve evidence arises. Unfortunately, there are no hard and fast rules to follow. In Stevenson v. Union Pacific Railroad, 354 F.3d 739 (8<sup>th</sup> Cir. 2004), for example, the court upheld spoliation sanctions imposed when the defendant railroad destroyed a tape recording of a train engineer made contemporaneously with an accident that caused serious injury. Although no lawsuit had been filed at the time the tape was destroyed, the court based its holding in part on defendant's "knowledge that litigation is frequent when there has been an accident involving serious injury or death."<sup>13</sup> The duty to preserve evidence often arises "not only during litigation but also . . . [during] that period before the litigation when a party **reasonably should know** that the evidence may be relevant to anticipated litigation [emphasis added]."<sup>14</sup>

In Renda Marine, Inc. v. United States, the court held that the defendant's duty to preserve evidence arose when defendant received notice from the plaintiff demanding cure of an alleged breach of contract. When a party "reasonably should know" that litigation is imminent is in many ways akin to crystal-ball gazing. This uncertainty forces companies to treat virtually every customer complaint as a triggering point for retaining documents and data relevant to that complaint. This defensive posture is both time consuming and burdensome,

---

<sup>13</sup> 354 F.3d at 748. Compare *id.* with Concord Boat Corp. v. Brunswick Corp., 1997 WL 33352759 (E.D. Ark. Aug. 29, 1997) (noting that corporation was under a duty to preserve documents where "the corporation knew or should have known that the documents would become material at some point in the future," and holding that duty to preserve arose upon filing of action).

<sup>14</sup> Renda Marine, Inc. v. United States, 58 Fed. Cl. 57 (2003) (quoting Silvestri v. General Motors Corp., 271 F.3d 583, 591 (4<sup>th</sup> Cir. 2001)) (alterations in original). Compare *id.* to Wal-Mart Stores, Inc. v. Johnson, 106 S.W.2d 718 (Tex. 2003) (holding that duty to preserve evidence arises upon party's knowledge of a "substantial chance" of litigation; no "substantial chance" of litigation arose where personal injury plaintiff was not severely injured and had not yet made any threat to sue).

however, because it creates repeated exceptions that “swallow” the document and data retention rules.

**D. Requests for Electronic Discovery Present Unique Problems**

The latest and most controversial battleground in the spoliation arena is electronic discovery. The Zubulake and Coleman cases discussed above demonstrate the increasing importance of adequately preserving and producing electronic documents and data. A party’s discovery obligations extend to its electronic data as well as paper files.<sup>15</sup> This includes not only all current electronic data stored on a party’s computer system, but all information retained on back-up tapes or other storage media. The costs of retrieving and producing such information can be staggering, and courts must find some way to allocate those costs.<sup>16</sup>

Regardless of who pays for retrieving and producing electronic data, spoliation principles apply to the failure to identify its existence and produce relevant portions. The Zubulake V decision arose out of a fairly routine employment case, but it gave rise to a costly side battle over electronic discovery. In that case, the plaintiff filed a motion for sanctions after re-deposing a number of defendant’s employees and discovering that some of them continued to delete relevant emails long after the defendant had notice of the plaintiff’s claims. Some of the emails had been deleted even after a litigation hold had been put in place. Moreover, plaintiff had failed to produce some electronic files that had been retained.

---

<sup>15</sup> Rowe Entertainment, Inc. v. The William Morris Agency, Inc., 205 F.R.D. 421, 428 (S.D.N.Y. 2002).

<sup>16</sup> As discussed in Rowe, the courts balance a variety of different factors in determining which party should bear the expense of restoring or retrieving relevant electronic data such as email server back-ups. Among the factors considered are: (1) the specificity of the discovery request, (2) the likelihood of discovering critical information, (3) the availability of the requested information from other sources, (4) the purposes for which the responding party maintains the requested data, (5) the relative benefit to the parties of obtaining the data; (6) the ability of each party to control costs; and (7) the total cost and relative resources of the parties. See also McPeck v. Ashcroft, 202 F.R.D. 31 (D.D.C. 2001).

The court held that spoliation sanctions were warranted in response to at least some of these failures, and it observed that reasonable defense counsel should take the following steps to preserve evidence<sup>17</sup>:

- (1) The first and most important step in preserving documents is the implementation of a “litigation hold”: “Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a ‘litigation hold’ to ensure the preservation of relevant documents.”<sup>18</sup> A litigation hold memorandum should be re-circulated periodically to remind employees of their continuing duty to preserve documents and data.
- (2) Counsel should communicate directly with the “key players” (i.e., those company employees most involved in the subject matter of the litigation) regarding document collection and preservation issues. “Since these ‘key players’ are the ‘employees likely to have relevant information,’ it is particularly important that the preservation duty be communicated clearly to them.”<sup>19</sup>
- (3) Counsel should instruct all employees to produce copies of relevant electronic files and should also take control of any relevant electronic back-up media to ensure it is not recorded over or otherwise destroyed.

The Zubulake court found that defense counsel had neglected to communicate the litigation hold to all key players and failed to actually request production of documents and data from certain key players. In addition, some of the defendants’ employees continued deleting relevant emails despite having received explicit instructions not to do so. As a result, certain emails were permanently deleted and the production of other emails was significantly delayed because they had to be retrieved from backup media. The Zubulake court ruled that it would give an adverse inference spoliation instruction, that the defendant must pay the costs of

---

<sup>17</sup> The Zubulake V court did indicate that these steps might be sufficient, or might be overkill, in a given case.

<sup>18</sup> Zubulake v. UBS Warburg LLC, (Zubulake IV), 220 F.R.D. 212, 218 (S.D.N.Y. 2003).

<sup>19</sup> Zubulake V, 2004 WL 1620866 at \*9.

any re-depositions necessitated by the belated productions, and that the defendant would bear plaintiff's costs in bringing the motion for sanctions.

## V. Conclusion

Given the importance of HMDA data, the reputation risk and need to avoid any appearance of discrimination in mortgage lending, and the threatened litigation risk, it is necessary to vet and scrub the data before releasing it for publication. This self-analysis process must be done with utmost care, control and confidentiality. The way to protect the self-evaluation process from being discovered by hostile litigants or regulators is to cloak the process in some type of privilege.

This paper explains the potential application of four different types of privilege protections for HMDA data analysis: (1) the self-test privilege in the HMDA Regulations; (2) the self-critical analysis privilege; (3) the work-product privilege; and (4) the attorney-client privilege. Some protections are statutory, some are the result of regulatory rulemaking approved by Congress, but most are the result of judicial decisions by courts through the years, which makes them part of the common law.

While each of the above four privileges offers some level of protection under various factual scenarios, only the attorney-client privilege can deliver the degree of protection over the process which lenders need. However, the attorney-client privilege must be overseen, directed and handled with great care. There are multiple players in a HMDA data analysis project, and they must be coordinated closely by the lender institution -- including outside counsel, consulting experts, in-house counsel, employees with responsibility in the process or access to the process, and all third party communicators. This paper explains in detail how to establish protocols to protect and preserve the attorney-client privilege and to avoid the dreaded

consequences of waiving that privilege. The paper also examines the related issue of document and data management, and the avoidance of spoliation of evidence problems which could support severe sanctions.

Unfortunately, there are no guaranteed means for a lender to cloak its self-analysis of HMDA data in an impenetrable privilege. But, for the diligent and wise lenders, this paper presents a path of protection. Although the proffered process is costly to administer, it provides the best solution to the HMDA internal analysis conundrum -- not having your hard work at self-analysis used against you to establish liability for your mortgage lending business.