

CHECKLIST – LEGAL RISKS OF SOCIAL MEDIA – HUMAN RESOURCES

Employee Personal Use of Social Media

1. Confusing personal opinion with bank's opinion. When that happens, you have all the risks of bank use without the benefit of risk mitigation procedures used by the bank.
2. Major risks:
 - Disclosure of confidential bank/third party business information.
 - Disclosure of customer information.
 - Defamation/Trade Libel/IP rights violation.
 - Admissions against interest.
 - Binding bank to a promise.
 - SEC violations.
 - Inability to regulate communication outside bank's IT system, but potentially subject to discovery
 - Reputational risk.
3. Risk Mitigation:
 - A. *Clear internal written* policies for what is and is not permitted (See previous list for bank internal policies).
 - Require disclaimer that when mentioning the bank, that is personal, not bank opinion.
 - No use of bank or customer information, logo, trademarks, etc. without written permission.
 - Don't talk about bank plans, policies, financial information, other than what has already been made public. Consider banning any discussion of bank's business through non-bank social media.
 - Personally responsible for all social media conversations. Violation of policy grounds for termination.
 - Consider having employee sign the policy.
 - B. Clear "Rules of the Road" for blogging, etc. Here's how to stay out of trouble.
 - C. Monitoring more problematic.
 - D. Enforcement critical. Consistent and fair.

Hiring Due Diligence

Currently, three views by bankers:

1. It's negligent not to review information that might be pertinent and that is so easily available.
2. Social media information not proven to be reliable (e.g. fake Facebook or MySpace pages) and, therefore, not as reliable as other conventional background checking sources.
3. The "Amegy Option": Because you can't "filter" "permissible" hiring information from "impermissible" information, never use it and never let third party search firms use it.

4. Risk Mitigation:

A. Whether prohibiting or permitting the “mining” of social media data, have a clear written policy for HR employees and bind search firms to it.

B. If permitting “mining,” the policy should:

- Make clear what data can and cannot be used (conform to bank’s existing hiring policies and applicable law). Train the employees. Bind third party search firms by contract.
- Require that HR employees and search firms not violate the social medium’s terms of use as to data mining. Usually not a problem, but some advise either employer “vet” the TOU first or have HR “data miner” include copy of the site’s terms of use with the data when submitted for review.
- Only use “mined” data that related to work and not otherwise impermissible.
- Get the applicant’s permission to search. Be able to demonstrate that permission is given voluntarily.