## Monday, October 20
## 9:00 am-10:30 am

# 003 Gotcha! Top Ten Employer Compliance Mistakes

**Justin H. McCarthy**
*Senior Counsel*
DENTSPLY International, Inc.

**Sozeen J. Mondlin**
*Associate General Counsel*
The MITRE Corporation

**David R. Mowry**
*Attorney*
Xerox Corporation

# Faculty Biographies

**Justin H. McCarthy**

Justin McCarthy is senior counsel for Dentsply International Inc., the world's largest professional dental products company, in York, Pennsylvania. His responsibilities include providing a full range of legal services to all divisions of the company around the globe. Mr. McCarthy's practice emphasizes all aspects of business law, including commercializing new products and technologies, mergers and acquisitions, formation of foreign ventures, company commercial and corporate matters, labor and employment matters, as well as supervision of major litigation and dispute resolution, risk management, and employee benefit issues.

Prior to joining Dentsply, Mr. McCarthy served as the chief legal officer of The Vartan Group, a commercial development and investment group in Harrisburg, Pennsylvania, and previously, as an associate with Drinker, Biddle & Shanley, in Morristown, New Jersey.

Mr. McCarthy is a member of the Pennsylvania and New Jersey bars, and is a member of the Pennsylvania Bar Association, the ABA, and ACC, serving as project coordinator for the National Community Service Day project for ACC's Central Pennsylvania Chapter.

Mr. McCarthy received a BA from Franklin & Marshall College, and his JD from the Villanova University School of Law.

**Sozeen J. Mondlin**

Sozeen J. Mondlin is associate general counsel and director of compliance for The MITRE Corporation ("MITRE"). MITRE is a systems engineering and information technology company that works in the public interest on defense and intelligence, aviation systems development, and enterprise modernization. Ms. Mondlin is responsible for MITRE's ethics and compliance program. She also is responsible for advising management on employment law and employee relations and for oversight of the company's litigation.

Ms. Mondlin is a graduate of Wellesley College and Stanford Law School.

**David R. Mowry**

David R. Mowry is an attorney on the Xerox North America (XNA) legal team.

After graduating from law school, Mr. Mowry worked at Coudert Brothers. He then went on to one-year clerkships with the US District Court for the Western District of Oklahoma and then with the US District Court for the District of Columbia. Following the last of these clerkships, Mr. Mowry joined Nixon Peabody LLP as a litigation associate. His practice at Nixon Peabody focused on commercial litigation, primarily working on matters involving products liability, construction, utility tariffs, environmental, land use, securities fraud, and contract dispute issues.

Mr. Mowry has a BA from Emerson College and a JD from Brooklyn Law School.

## Gotcha! Top Ten Employer Compliance Mistakes

1. Compliance Plan for Employment Issues
2. Reductions in Force
3. Releases
4. Severance
5. Unauthorized Workers
6. Wage and Hour Issues
7. Independent Contractors
8. Non-compete Agreements
9. HIPAA/Gramm Leach Bliley
10. Hidden State and Local Issues

## 1. ESTABLISHING A COMPLIANCE PROGRAM FOR EMPLOYMENT ISSUES

## COMPLIANCE PROGRAM

- Biggest Compliance Issue
  - Not having a comprehensive formal Compliance Program
- What is it?
  - Function responsible for identifying significant legal risks in advance as the business goes forward and working to ensure that the risks are understood and mitigated
- How is a Compliance Program established?
  - Designate a CCO/Director of Compliance
  - Integrate into the business (e.g., officer meetings, staff meetings, etc.)
- Where should it report?
  - CEO?
  - Two-hatted General Counsel?
  - To General Counsel?
  - Dotted line to Audit Committee, etc.
  - HR/Finance

## Compliance Program (Cont'd)

- Many substantial legal risks are employment related and preventive measures are the key, including policies to manage the risk and training to ensure that the policies are understood and followed
- Some primary employment areas
  - Employment discrimination in general – particularly termination policies & harassment
  - Electronic communications policies (e.g., email, blogging, etc.)
  - Information privacy policies (HIPAA, FCRA, misc state and federal personal data regulations)
  - Non-retaliation policies
  - Medical leave (federal FMLA and state leave regulations)
  - RIFS/plant closing (WARN)
  - FLSA and state wage hour regulations
  - Non-Competes

## Compliance Program (Cont'd)

- Employee conflicts of interest (e.g., gifts and gratuities)
- Industry-specific issues
  - Government contractors
    - Hiring of former government employees
- How to identify risks
  - Formal risk assessments with input of attorney, line managers, directors, and HR (see ACC website)
  - Industry trends
  - Newspaper articles
  - Specialized trade publications
  - ACC newsletters and programs
  - Help-lines for reporting concerns (anonymous telephone and now web-based), open door policies (with help of robust credible investigation processes)

## Compliance Program (Concluded)

- Devise plan to mitigate risks
  - Investigate best practices
  - Review and create policies
  - Training, general and targeted (on-line or in-person)
  - Communications campaigns
  - Determine availability of third party vendors
  - Assign ownership to management
- Insurance (EPLI)
  - Watch choice of counsel provisions
- Periodically update as statutes, regulations, and industry changes occur
  - Institute regular schedule

## Compliance Program (Cont'd)

- How to identify risks (cont'd)
  - Internal audit findings
  - Exit interviews
  - Employee surveys
  - Lessons learned after significant cases, events, failures, etc.
- Prioritize by probability of occurrence and significance of risk to the company
  - Consider all risks
  - Legal
  - Operational
  - Reputational
- Coordinate with internal audit function

## 2. REDUCTIONS IN FORCE

## Plan In Advance

- Prepare timeline and set realistic expectations
- Prepare forms identifying areas for documentation
  - The business case (what changes or conditions in the business environment precipitated the need for the lay-off)
  - Why particular individual (or work group) selected
    - Based on objective criteria such as past performance, suitability to remaining and expected work
  - Efforts to find individual other work
  - Why relevant co-workers in the work group were not selected
- Drive down to lowest level for making the recommendation for termination, with concurrence of superiors
- Have cognizant HR representative prepare separate "approver memo," summarizing salient points and supporting recommendations
- Prepare attorney-client privileged adverse impact analysis
  - Have statistician on call

## Plan In Advance (Concluded)

- Train managers on how to deliver message to employees
- Inform the Corporate Security Office
- Have Human Resources (including benefits representatives) available on-site for consultation
- Offer outplacement services if at all possible
- Carefully monitor post-RIF vacancies

## Plan In Advance (Cont'd)

- Assess "Corporate" v. "smaller working Unit" RIFS
- Check WARN statute and state "Baby WARNS"
- Ensure that legal office reviews drafts of all documentation
- Carefully review files of selected individuals, particularly recent performance reviews, to ensure consistency with the stated rationale and identify any "red flags"
- Carefully review files of identified individuals in same category not selected to verify rationale
- Flag potential risk areas
  - Existing EEO or ER issues
  - Benefits issues
  - FMLA issues
- Weigh pros and cons of releases
  - Check OWBPA and any state requirements

## Releases

- "One size fits all" releases have come under increased attack
  - Recent federal court decisions have held several such releases to be null and void
  - Trouble spots:
    - EEOC claims
    - FMLA claims
    - vague language
    - not adequately describing the decisional unit in RIFs (OWBPA)

## Releases

- Must review release for particular circumstance
  - Reason for release (e.g., RIF, employment dispute, severance)
  - Should consider:
    - Claims and rights being waived
    - Jurisdiction/Location (different interpretations between federal circuits, different state and local requirements)
    - Protected class status of individual signing (e.g., OWBPA special requirements)

## 5. UNAUTHORIZED WORKERS

## Severance

- Must consider timing and consequences before offering/paying out severance
  - IRC Section 409A (affects timing of severance payout to key employees)
  - IRC Section 162(m) (limits deductibility of severance pay to certain executives)
  - Release and agreement (even if severance is paid pursuant a separate agreement, 409A may require additional documentation)

## E-Verify

- On-line system for employers to verify work status of employee
  - Compares information on an employee's I-9 form against SSA and DHS databases
  - To participate, and employer may initiate a query no later than 3 days after new hire's start date
- Free and voluntary for most employers
  - Only mandatory for federal contractors

## E-Verify

- Process gives an employer a confirmation or tentative non-confirmation of work eligibility
  - If employer receives a tentative non-confirmation, employee has 10 days to clean up discrepancy
  - Employers should not terminate workers that receive tentative non-confirmation until either they receive a non-verification of the 10 day period has elapsed without clean up of discrepancy

## No-Match Letter

- No-Match letter from the SSA, or "notice of suspect documents" from DHS
  - These notices call into question the validity of the named employee's identifying information
  - Puts employer on notice that the subject employee(s) might be unauthorized to work in the U.S.

## E-Verify

- Employer participation in program establishes a presumption that employer has not knowingly hired an unauthorized alien
  - Participation does not, however, provide a safe harbor from enforcement

## No-Match Letter

- Employers must perform reasonable due diligence on employee's work authorization status upon receipt of a No-Match letter, or risk being deemed to have constructive knowledge of employee's unauthorized work status
  - Potential civil and criminal penalties

## No-Match Letter

- Safe Harbor Provision
  - DHS Safe Harbor Provision protects employers from facing an enforcement action if they comply with it to rectify the no-match
  - Sets forth clear steps an employer may take in response to receiving a no-match letter
  - 90 days to complete all steps to be afforded Safe Harbor protection

## Wage and Hour Issues

- Elements giving rise to these issues:
  - Mobile workforce (e.g., working outside the office)
  - Telecommuting
  - State law requirements

## Wage and Hour Issues

- Recent wave of class and collective actions concerning wage and hour issues
  - Classification of workers as exempt from overtime
  - Employees who perform work off the clock (unauthorized OT, donning/doffing time)
  - Employees who work out of the office
  - Meal and break periods
  - On-call time

## Wage and Hour Issues

- Need to make sure that payroll policies and general break and compensation practices are in compliance with the law
  - Audit these policies and practices?

## Wage and Hour Issues

- May need to audit job classifications and job descriptions
  - At a minimum, should identify and examine job classifications that are potentially "at risk" (e.g., lowest paying exempt jobs)
  - Must not rely solely on job descriptions; need to scrutinize job functions and tasks performed
  - See FLSA Exemption flow charts in handout

## Wage and Hour Issues

- Also should make sure that managers are properly trained on preventing employees from working off the clock or unauthorized OT
  - Particularly need to know how to address telecommuters, home-workers, and company travel (e.g., trade shows, sales meetings)

## Wage and Hour Issues

- If audit reveals (potential) problems, it is best to remedy potential violations
  - 2 year statute of limitations under FLSA for unpaid back OT pay due for misclassification as exempt
  - No obligation to report the misclassification to the employee (though questions may inevitably arise about back pay if employer changes classification to non-exempt)

## FLSA

- Common Mistakes:
  - Salaried employees are automatically exempt
  - Too small to be covered by FLSA
  - Not paying for OT worked because it was not approved prior to employee working it
  - Allowing employees to "waive" OT pay
  - Giving "Comp Time" in lieu of paying OT
  - Basing OT exemption on title – must look at time and tasks worked

## 7. Independent Contractors

## Employee vs. Independent Contractor

- Multi-factor tests
  - May differ based on who is reviewing and why (e.g., OSHA, IRS, federal or state court)
  - Right to control work is common element
- Agreements not determinative
  - Focus on relationship and actual conduct
- Potential liability
  - Back taxes
  - Back pay/OT pay
  - Benefits (health, options, retirement)

## Employee vs. Coemployee

- Similar multi-factor tests
  - May differ based on who is reviewing and why (e.g., OSHA, IRS, federal or state court)
  - Right to control work is common element
- Leased employees/long-term temps at issue
  - Focus on relationship and actual conduct
- Potential liability
  - Back taxes
  - Back pay/OT pay
  - Benefits (health, options, retirement)

## References


- *Factors to Consider in Assessing Independent Contractor Status* (2006), www.acc.com/resource/v7294
- *Vizcaino v. Microsoft*, 120 F. 3d 1006 (9th Cir. 1997)
- *Eight Tips to Prevent the Coemployment Trap During Mergers and Acquisitions*, ACC Docket, May 2008

8. Non-Competes

Shields and Swords

Now, the Catch

- **You have represented to Corporation that you have not signed any type of agreement with your current or any former employer that could restrict your ability to accept employment with Corporation or to perform any duties at Corporation. Corporation has relied upon your representation in making you this offer of employment.**

Offer --- the Catch comes next

- On behalf of Corporation, I am pleased to offer you a position of Executive within North America, reporting to me in Denver, CO. Your starting salary for this position will be paid semi-monthly at the annualized rate of $. After an initial training period and upon assignment to a sales territory, your salary will be adjusted to the appropriate compensation in effect at that time. Should this position require travel, you will be reimbursed, and a valid driver's license and proof of insurance acceptable to Corporation will be required. You will be eligible for an additional annual vacation entitlement of 1 week, to be earned in accordance with the Vacation Policy.

More of the Catch

- **Your offer is also contingent upon** the following provisions:
- you are not to disclose any confidential or proprietary information of any former employer;
- you are not to use any confidential or proprietary information of any former employer; and
- if at any time you feel you might have to inherently use confidential information of your former employer to perform your duties at Corporation, you shall so advise your manager and your duties will be revised appropriately.

## **California** Non Compete Agreements

- Under California law, employee non-compete agreements are void. See California Business & Professions Code § 16600. See, also, *Kolani v. Guluska, et al.,* 64 Cal. App. 4th 402 (1998 Cal. App.).
- California Business & Professions Code § 16600 provides "every contract by which anyone is restrained from engaging in lawful profession, trade, or business of any kind is to that extent void." Therefore, the Non-Compete Agreements with McNasty are void and unenforceable in California.

## Document the Conversation

- This memo will confirm our conversation today. I told you that, by policy, Corporation respects your continuing obligation to your previous employers not to use or disclose confidential or proprietary information of those employers. I also told you that Corporation, by policy, would honor any valid post-employment restrictions contained in any previous employer's employment agreement with you. I told you that Corporation does not want you to disclose any confidential or proprietary information of a prior employer, and specifically directed you that you are not to disclose any such information to anyone at Corporation.
- I also told you that Corporation does not want you to use any confidential or proprietary information of any previous employer in the course of performing your duties at Corporation. If, at any time while employed at Corporation, you feel you might inherently have to use confidential or proprietary information of a previous employer in order to perform your Corporation job duties, immediately contact me or your then current manager. We will adjust your job duties so that you do not have to use the confidential or proprietary information.

## **California** Proprietary Information Confidentiality Agreements

- **California** Proprietary information confidentiality agreements
- However, proprietary information agreements are enforceable in California. Corporation, by policy, honors any valid post-employment restrictions contained in any previous employer's employment agreement with an employee. Thus, by policy, Corporation respects an employee's continuing obligation to his or her previous employers not to use or disclose confidential or proprietary information of those employers.
- Therefore, any employee with a valid proprietary/confidential information agreement with a former employer should be counseled that Corporation does not want him or her disclose any confidential or proprietary information of a prior employer, and specifically directed not to disclose any such information to anyone at Corporation.
- Additionally, the employee should be counseled that Corporation does not want the employee to use any confidential or proprietary information of any previous employer in the course of performing his or her duties at Corporation. The employee should be told that if, at any time while employed at Corporation, the employee feels he or she might inherently have to use confidential or proprietary information of a previous employer in order to perform their Corporation job duties, they should immediately contact you or their then current manager.
- Corporation then will adjust their job duties as necessary so that they do not have to use the confidential or proprietary information of the previous employer. This conversation should be documented.

## Working at a "Competitor"

- For a period of one year following either the (I) non-renewal or termination of the Corporation Authorized Service Agent Agreement between Service Agent and Corporation ("Service Agent Agreement") or (II) termination of Agent Owner's affiliation with Service Agent, Agent Owner shall refrain from providing any repair or maintenance services for any Corporation or non-Corporation products set forth on Exhibit 5 of the Service Agent Agreement, within a fifty mile distance of the Territory.

## Agreement with the Competition

- **Recruitment Policy. While Company is performing Services for McNasty under this Agreement, and for six months after this Agreement terminates, neither party will hire the other party's personnel with whom they became familiar as a result of this Agreement without the express written consent of the other party. If either party violates this clause, they shall compensate the other party with a one time settlement equal to $10,000 for each person so hired as compensation for screening, hiring, and training costs for such personnel. The parties agree not to affirmatively recruit employees of the other to fill vacant positions without the other party's consent.**

## New York is Different (Reasonable)

- In consideration for being granted employment with Corporation, and in consideration for any and all training, education and instruction Employee is provided in the course of employment with Corporation, Employee agrees that for a twelve (12) month period following Employee's termination of employment with Corporation for any reason, Employee will not, on Employee's own behalf or on behalf of any other person, firm, partnership or corporation:
- within the geographic area(s) covered by the Employee during any period of the last twelve (12) months of employment at Corporation, engage (as an employee, proprietor, partner, agent, consultant or otherwise) by any means in any business which is competitive with the business of Corporation, or
- solicit business from any customer of Corporation which Employee solicited or learned of while employed with Corporation, or
- Solicit, induce or assist any employee of Corporation to leave his or her employment with Corporation.
- Proprietary Information and Conflict of Interest Agreement:
- During and after my employment with Corporation, I will neither disclose nor assist in the unauthorized disclosure of Corporation confidential or proprietary information (which includes, but is not limited to, trade secrets, formulas, customer data, strategies, methods, processes, machines, inventions, discoveries, computer programs and systems, works of authorship, improvements, and other developments), nor will I use information except as required by Corporation.

## 9. HIPAA & GLBA

- The Health Insurance Portability and Accountability Act
- (HIPAA not HIPPA)

## HIPAA

- HIPAA requires a Covered Entity
- [ i.e., healthcare provider or insurer] to have in place appropriate administrative, technical and physical safeguards to protect the privacy of protected health information (*medical and billing*). 42 CFR 164.530.

## HIPAA

- Additionally, 42 CFR 164.514 requires covered entities to develop standard protocols for routine and recurring disclosures of protected health information and uses in order to assure a minimum necessary disclosure or use standard is enforced.

## HIPAA

- For non-routine disclosures, the security requirements imposed on the covered entity are more stringent, requiring a review of the individual request to determine if the information sought is limited to the minimum necessary for the purpose.

## HIPAA

- Minimum Necessary --
- The minimum necessary for the purposes of the disclosure/use.

## HIPAA

- Business Associate --
- In essence, any entity that does work for or on behalf of a Covered Entity that will bring that entity into contact with protected health information.

## HIPAA

- Business Associate Contract --
- HIPAA does not apply to Business Associates.
- Instead, HIPAA requires Covered Entities to have Business Associates contracts in place by April 1, 2003 (i.e., contractual, not statutory obligations).

## HIPAA

- HIPAA *does not* require that a business associate have the same security programs in place as the Covered Entity.

## HIPAA

- HIPAA requires the Covered Entity to obtain *satisfactory assurances* from the Business Associate that it will *appropriately safeguard* Protected Heath Information disclosed to the business associate in the form of a Business Associate contract.
- These are significantly less requirements than the "administrative, technical and physical" safeguards that are imposed on covered entities.

## HIPAA

- The HIPAA regulations (42 CFR 164.502; 164.504) require a business associate contract to contain certain specific provisions

## HIPAA

(a) Not use or further disclose PHI other than as permitted or required by the Agreement between the Covered Entity and the Business Associate, or as required by law;

(b) Use *appropriate safeguards* to prevent the use or disclosure of such PHI other than as provided for by the Agreement between the Covered Entity and the Business Associate;

## HIPAA

(c) Report to the Covered Entity any use or disclosure of such PHI not provided for by the Agreement between the Covered Entity and the Business Associate of which the Business Associate becomes aware;

(d) Ensure that any agents, including subcontractor, to whom the Business Associate provides PHI agree in writing to the same restrictions and conditions that apply to the BA with respect to such information;

## HIPAA

(e) Make such PHI available for inspection and copying by the individual subjects thereof in accordance with Sec. 164.524 (which contains certain limitations);

(f) Make such PHI available for amendment by the individual subjects thereof and incorporated any amendments to PHI, to the extent required and in accordance with Sec. 164.526 (which contains certain limitations);

## HIPAA

(g) Make available the information required to provide an individual subject with an accounting of disclosures of the subject's PHI, to the extent required and in accordance with Sec. 164.528 (requires record of *improper* disclosures to be maintained for 6 yrs.);

## HIPAA

(h) Make the Business Associates internal practices, books and records relating to the use and disclosure of PHI available to the Secretary of HHS for purposes of determining the Covered Entity's compliance with HIPAA;

## HIPAA

(j) Incorporate any amendments or corrections to such PHI when notified by Customer thereof.

(k) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

## HIPAA

(i) At termination of this Agreement, if feasible, return or destroy all PHI that the BA still maintains in any form and retain no copies of PHI, or if such return or destruction is not feasible, extend the protection of this Agreement to the PHI and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible; and

## HIPAA

- OPTIONAL PROVISONS:
- The Business Associate may use PHI received by the BA in its capacity as a BA to the Covered Entity, if necessary, for the proper management and administration of the BA, or to carry out the legal responsibilities of the BA
- The Business Associate may also use and disclose PHI to provide data aggregation services relating to the health care operations of the Customer.

## HIPAA

- The Termination Requirement –
- Requires that the Business Associate contract authorize termination if the Covered Entity determines the BA committed a material breach.
- A material breach is not defined by HIPAA.

## HIPAA

- Since the issue for the Covered Entity should be whether they remain HIPAA compliant, the requirements, read together, allow for a reasonable cure period for any material breach before the termination provision may be evoked, i.e.;

## HIPAA

- The Business Associate regulation also expressly provides that:
- A covered entity is not in compliance with HIPAA, if the Covered Entity knew of a pattern of activity or practice of the Business Associate that constituted a material breach or violation of the BA's obligation under the contract, unless the Covered Entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were
- unsuccessful, terminated the contract.

## HIPAA

- "If Customer believes that X has engaged in a pattern of activity or practice that constitutes a material breach of X's obligations under this Addendum, Customer agrees to notify X in writing of such failure so that representatives of both parties can meet to discuss Customer's concerns. X then will correct any identified material breach of this Addendum within 30 days. If X fails to do so, and Customer does not materially cause such failure, then Customer may terminate this Agreement with incurring any termination charges."

## HIPAA

- HIPAA contains no Covered Entity indemnification requirement, but Covered Entities routinely include one in their Business Associate contract.

## GLBA

- Intended to protect the privacy of consumer financial information.

## GLBA

- The Gramm-Leach-Bliley Financial Services Act,
- 15 USC Sec. 6801 et al.

## GLBA

- GLBA privacy and security obligations are imposed on financial institutions (which includes banking and insurance entities).
- Similar to the privacy and security requirements imposed by HIPAA. -- *a double whammy for health insurance entities*.

## GLBA

- Lead federal agencies, the Office of the Comptroller of the Currency, the Federal Reserve, the FDIC and the Office of Thrift Supervision. See, e.g., 12 CFR Parts 40, 216, 332 and 573.

## GLBA

- The GLBA regulations, 12 CFR Sec. 40.1:

(1) Requires a financial institution to provide notice to customers about its privacy policies and practices;

## GLBA

- The Agencies have issued certain "Interagency Guidelines Establishing Standards for Safeguarding Customer Information; published in 66 FR 8615 (2/1/01) and codified in 12 CFR Parts 30, 208, 211, 225, 263, 308, 364, 568 and 570.

## GLBA

(2) Describes the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and

## GLBA

(3) Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by "opting out" of that disclosure, subject to the exceptions in Secs. 40.13, 40.14, and 40.15.

## GLBA

- **The Guidelines require that banks implement information security programs to safeguard customer information**:
- "[E]ach bank shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. While all parts of the bank are not required to implement a uniform set of policies, all elements of the information security program must be coordinated.… A bank's information security program shall be designed to:
  - Ensure the security and confidentiality of customer information;
  - Protect against any anticipated threats or hazards to the security or integrity of such information; and
  - Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

## GLBA

- **The Guidelines also require that a bank's board of directors or an appropriate committee of the board shall:**
  - "Approve the bank's written information security program; and
  - Oversee the development, implementation, and maintenance of the bank's information security program, including assigning specific responsibility for its implementation and reviewing reports from management. "

## GLBA

- **The Guidelines additionally require banks to:**
  - < "Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;
  - < Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information;
  - < Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks;
  - < Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the bank's activities; and

## GLBA

< …consider whether the following security measures are appropriate for the bank and, if so, adopt those measures the bank concludes are appropriate:

< Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means;

< Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;

## GLBA

< Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;

< Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and

< Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.

## GLBA

< Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

< Procedures designed to ensure that customer information system modifications are consistent with the bank's information security program;

< Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information;

## GLBA

- SERVICE PROVIDERS --
- Financial institution are required to enter into contracts with Service Providers, by July 1, 2003, which will prohibit the Service Provider from disclosing nonpublic personal consumer information held by the financial institution other than to perform the service for which the Service Provider has been engaged.
- Like HIPAA, the obligations imposed on the Service Provider are contractual, not statutory.

## GLBA

- Service Provider is defined as:
- any person or entity that maintains, processes, or otherwise is permitted to access customer information (i.e.,non-public personally identifiable financial information) through its provision of services directly to the financial institution.

## GLBA

- As part of monitoring, the Guidelines provide that banks should review audits, summaries of test results, or other equivalent evaluations of its Service Providers.

## GLBA

- With respect to Service Providers, the Guidelines require banks to:
  - < Exercise appropriate due diligence in selecting its service providers;
  - < Require its service providers by contract to implement *appropriate measures* designed to meet the objectives of the Guidelines; and
  - < Where indicated by the bank's risk assessment, monitor its service providers to confirm that they have satisfied their obligations.

## GLBA

- But that is it!
- Unlike HIPAA, the GLBA, its Regulations and the Guidelines do not require that any specific terms be contained in a Service Provider contract.

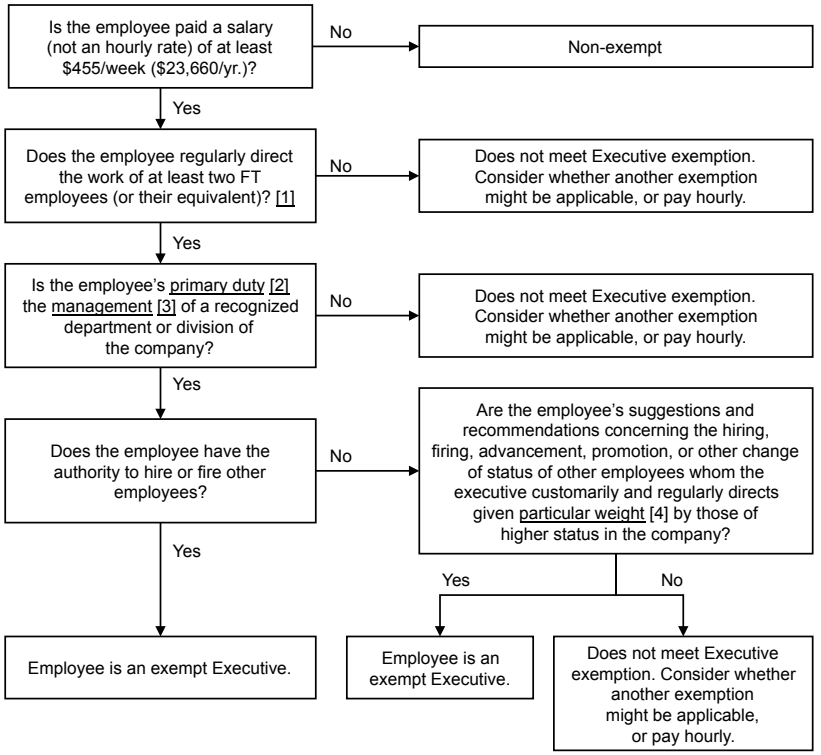
## GLBA

- Like HIPAA, the GLBA does not require that the Service Provider indemnify the Financial Institution for a breach of the Service Provider contract.

## Hidden State and Local Issues

- Many states and municipalities have their own set of "gotcha" laws and rules
  - immigration laws
  - final pay withholding
  - state FMLA laws
  - personnel file access
  - break/meal periods
  - vacation pay
- See *ACC Small Law Dept. Human Resources Manual InfoPAK*

## Executive Exemption



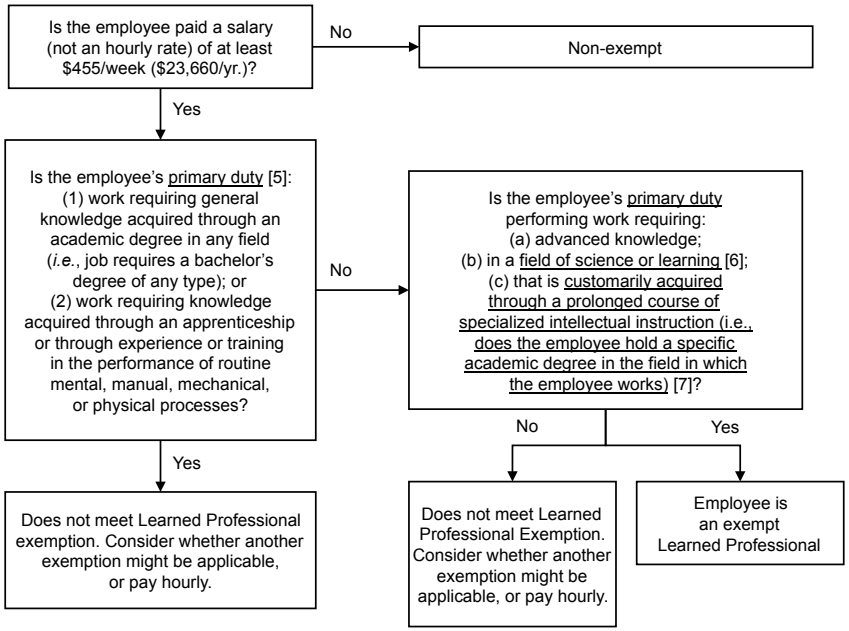

[1] "Equivalent" to two FTEs means the total of the employees' hours equals those of two full-time employees (*i.e.*, 80 hours). For example, one full-time employee (40 hours) and two part-time employees (20 hours each) are equivalent to two full-time employees. By contrast, one full-time employee (40 hours) and two part-time student employees who each work only 10 hours a week would *not* be the equivalent of two full-time employees.

[2} The "primary duty" is the main or most important duty the employee performs. Employees who spend more than 50% of their time performing exempt work generally will meet the primary duty requirement; however, it is possible that an employee's primary duty still might be exempt work even if he/she performs that duty less then 50% of the time.

[3] "Management" includes interviewing/selecting/training employees; setting/adjusting employees' rates of pay and hours of work; directing the work of employees; maintaining production or sales records for use in supervision or control; assessing employees' productivity and efficiency for purpose of recommending promotions/change in status; handling employee complaints; disciplining employees; planning work; determining techniques to be used; apportioning work among employees; determining type of materials/ supplies/machinery/equipment/tools to be used or merchandise to be sold; controlling flow and distribution of materials/merchandise/ supplies; providing for safety/security of employees or property; planning and controlling budget; monitoring or implementing legal compliance measures.

[4] Determining whether the employees' suggestions and recommendations are given "particular weight" requires a review of the following factors: (a) whether it is part of the employee's job duties to make such suggestions and recommendations; (b) the frequency with which the employee is asked to make suggestions and recommendations; (c) the frequency with which the employee actually does make suggestions and recommendations (whether requested to or not); and (d) the frequency with which the employee's suggestions and recommendations are accepted and relied upon by others with decision-making authority.

## Professional Exemption – Learned Professionals



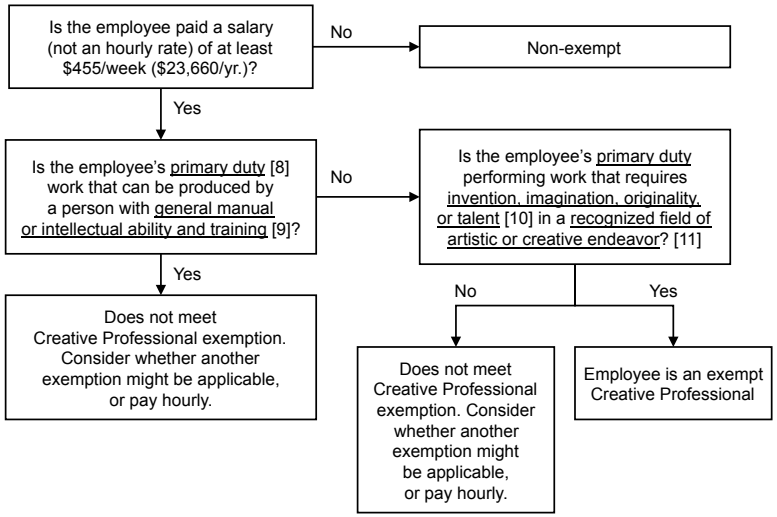

NOTE: Trainees who are not actually performing the duties of an exempt Learned Professional are not exempt.

[5] The "primary duty" is the main or most important duty the employee performs. Employees who spend more than 50% of their time performing exempt work generally will meet the primary duty requirement; however, it is possible that an employee's primary duty still might be exempt work even if he/she performs that duty less then 50% of the time.

[6] Examples: law, medicine, accounting, engineering, architecture, actuarial computation, pharmacy, teaching, and various types of physical, chemical, and biological sciences.

[7] The exemption is restricted to those professions where specialized academic training is a prerequisite for entrance into the profession. The best evidence of this requirement is the requirement that the individual hold a specific academic degree. Often, professionals also are licensed or certified by the state or an accrediting board. The exemption does not apply to occupations in which most employees have acquired their skill through experience rather than through advanced specialized intellectual instruction (*e.g.*, mechanical draftsmen).

## Professional Exemption – Creative Professionals




NOTE: The more an employee's day-to-day work is dictated by management, and the more well-defined the framework in which the employee's work is performed, the less likely it is that the employee qualifies as a creative professional.

NOTE: Trainees who are not actually performing the duties of an exempt Creative Professional are not exempt.

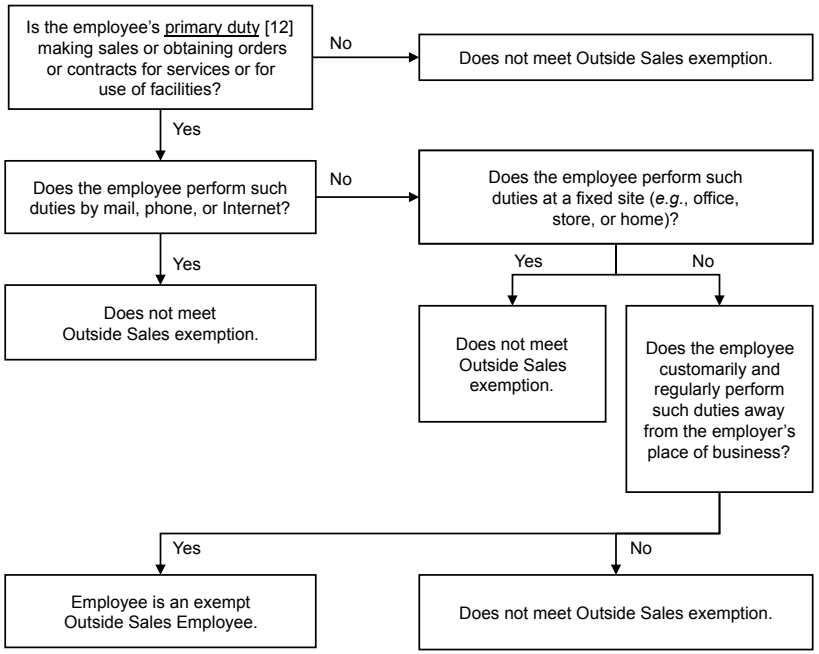
[8] The "primary duty" is the main or most important duty the employee performs. Employees who spend more than 50% of their time performing exempt work generally will meet the primary duty requirement; however, it is possible that an employee's primary duty still might be exempt work even if he/she performs that duty less then 50% of the time.

[9] Work that primarily depends on intelligence, diligence, or accuracy falls in this category. This work is distinguished from work requiring invention, imagination, originality, or talent, as discussed below.

[10] Work requiring "invention, imagination, originality, or talent" distinguishes the creative professional from individuals whose work primarily depends on intelligence, diligence, and accuracy. Examples of those demonstrating invention, imagination, originality, or talent include: actors; musicians; composers; painters who at most are given the subject matter of their painting; cartoonists who are given only the title or underlying concept of a cartoon and must rely on their own creative ability to express the concept; essayists, novelists, short story, and screenplay writers who choose their own subjects and turn in a finished piece of work to their employers; and individuals holding the more responsible positions at advertising agencies. Journalists may qualify for the creative professional exemption if their primary duty is analyzing or interpreting public events, writing editorials, opinion columns, or other commentary, performing on the air in radio or television, or acting as a narrator or commentator.

[11] Includes such fields as music, writing, acting, and the graphic arts.

## Outside Sales Employees



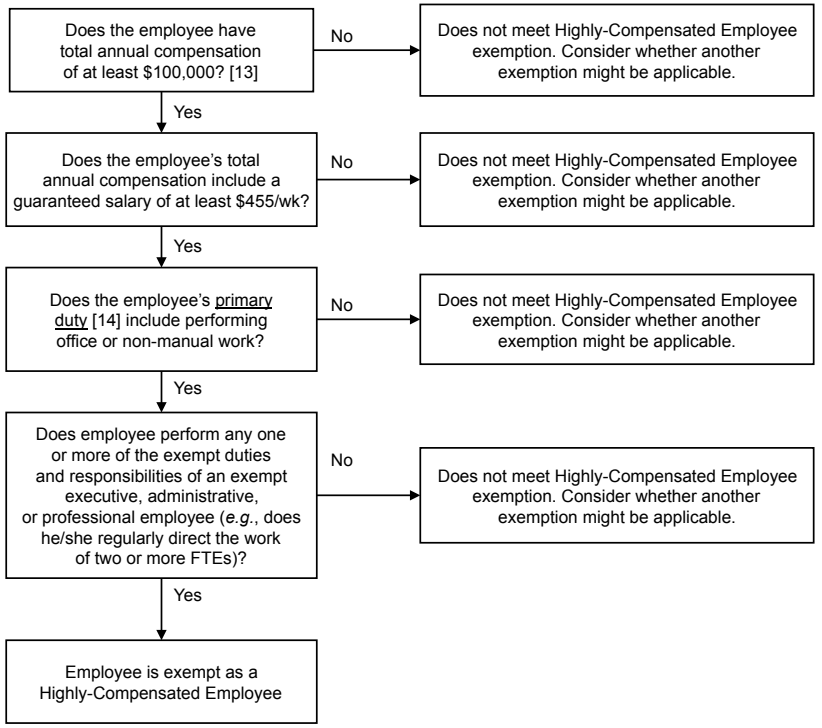

NOTE: Exempt Outside Sales Employees do *not* need to be paid on a salary basis, and there is no minimum pay requirement.

NOTE: For outside sales employees, work performed incidental to and in conjunction with the employee's outside sales activity (including incidental deliveries and collections) is regarded as part of the exempt sales work. Other work that furthers the employee's sales efforts (such as writing sales reports, updating or revising the employee's sales or display catalogue, planning itineraries, or attending sales conferences) also is considered part of the exempt sales work.

NOTE: Trainees who are not actually performing the duties of an exempt Outside Sales Employee are not exempt.

[12] The "primary duty" is the main or most important duty the employee performs. Employees who spend more than 50% of their time performing exempt work generally will meet the primary duty requirement; however, it is possible that an employee's primary duty still might be exempt work even if he/she performs that duty less then 50% of the time.

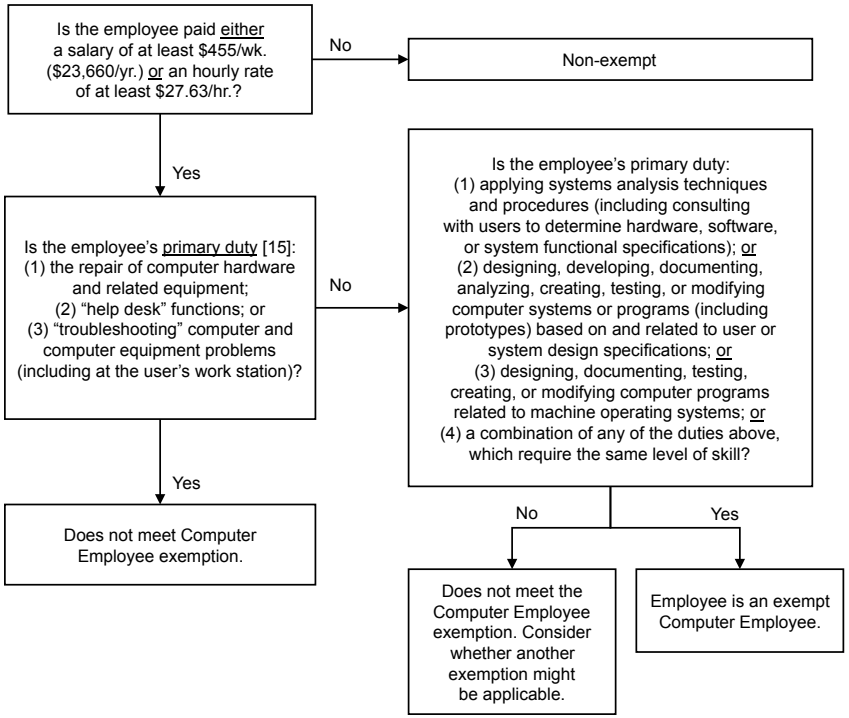
## Exemption – Highly-Compensated Employees




[13] "Total annual compensation" includes salary, commissions, non-discretionary bonuses, and other non-discretionary compensation earned during a 52-week period. Payments for medical insurance and life insurance, contributions to retirement plans, and the cost or value of other fringe benefits are *not* included in this calculation.

[14] The "primary duty" is the main or most important duty the employee performs. Employees who spend more than 50% of their time performing exempt work generally will meet the primary duty requirement; however, it is possible that an employee's primary duty still might be exempt work even if he/she performs that duty less then 50% of the time.

## Computer Employees




NOTE: Computer employees within this exemption or those outside this exemption may qualify for the Executive or Administrative exemption.

NOTE: Trainees who are not actually performing the duties of an exempt Computer employee are *not* exempt.

NOTE: If this employee is *exempt* but is paid hourly, hours worked over 40 are paid at straight time or some other method as agreed upon with the employee – *not* at time-and-one-half.

[15] The "primary duty" is the main or most important duty the employee performs. Employees who spend more than 50% of their time performing exempt work generally will meet the primary duty requirement; however, it is possible that an employee's primary duty still might be exempt work even if he/she performs that duty less then 50% of the time.