Hot Topics in Lawyer and Accountants’ E&O

Thursday, May 16, 2013

University of Chicago Gleacher Center
Introduction

by

James G. Stewart, RPLU
Senior Vice President
ProAccess, LLC
Introduction
by
Lawrence R. Smith
Partner
SmithAmundsen LLC
Lawyer E&O Panelists

• Dennis L. Bissett – Moderator
  – Claims Manager, Sedgwick

• Gawain Charlton-Perrin – Panelist
  – Risk Control Director, Hanover Insurance Group

• Andrew C. Seiber – Panelist
  – Partner, SmithAmundsen

• Jody A. Harris RPLU – Panelist
  – Managing Director, Arthur J. Gallagher & Co.

• Paul C. Wright RPLU – Panelist
  – Underwriting Consulting Director, CNA

Special Thanks to…
Jim Stewart, ProAccess and Larry Smith, SmithAmundsen
Dennis L. Bissett
Claims Manager
Sedgwick
Your source for professional liability education and networking.
The recommendation(s) and contents of this material are provided for informational purposes only. This material does not purport to address every possible legal obligation, hazard, code violation, loss potential or exception to good practice. It should not be construed as indicating the existence or availability of any insurance coverage. Hanover Insurance Companies and their affiliates and subsidiaries specifically disclaim any warranty or representation that compliance with any advice contained herein will make any premises, property or operation safe or in compliance with any law or regulation. The Hanover Insurance Group with Eagle Icon is a trademark of The Hanover Insurance Group, Inc.

Copyright © 2013
The Hanover Insurance Group, Inc.
Outline

• Lawyer Claim Statistics and Claim Trends
Profile of Legal Malpractice Claims 2008-2011
(Introduced at the ABA's Fall 2012 National Legal Malpractice Conference, held in Chicago Sept. 5-7, 2012)

• Based on information reported by malpractice insurers in the United States and Canada from 2008-2011
  – 8 Commercial Insurance Companies
  – 11 members of NABRICO
• Data from 53,000 claims – most ever
• Claim data
Profile of Legal Malpractice Claims 2008-2011

- Top Six Problem Practice Areas
  1. Real Estate (20.33% of all claims)(+.28% diff from 2007)
  2. Plaintiffs' Personal Injury (15.59%)(-5.97%)
  3. Family Law (12.14%)(+1.81%)
  4. Estates, Trust, and Probate (10.67%)(+.99%)
  5. Collection and Bankruptcy (9.20%)(+1.93%)
  6. Corporate/Business Organization (6.79%)(+1.85%)

- Notable Real Estate 1st for 1st time
  - Reasons? Future?
Profile of Legal Malpractice Claims 2008-2011

• 2006-2011 Real Estate Percentage of Claims
  2006 (19.25% of all claims)
  2007 (23.44%)
  2008 (23.36%)
  2009 (20.88%)
  2010 (19.12%)
  2011 (17.56%)
Profile of Legal Malpractice Claims 2008-2011

• Top Percentage Increase Change from 2007
  1. Collection and Bankruptcy (+1.93%)
  2. Corporate/Business Organization (+1.85%)
  3. Family Law (+1.81%)
  4. Estates, Trust, and Probate (+.99%)
  5. Labor Law (+.78%)
  6. Criminal (+.58+)
  10. Real Estate (+.28%)
Claim Stats and Claim Trends

Profile of Legal Malpractice Claims 2008-2011

• Top Percentage Decrease Change from 2007
  1. Personal Injury (-5.97%)
  2. International Law (-2.02%)
  3. Business Transaction Commercial Law (-.59%)
  4. Civil Rights Discrimination (-.32%)
  5. Taxation (-.25%)
Profile of Legal Malpractice Claims 2008-2011

- Top Claims by Number of Attorneys
  1. Solo (33.93% of all claims)(-3.31% diff from 2007)
  2. 2-5 attorneys (32.09%)(-.76%)
  3. 11-39 attorneys (11.37%)(+1.64%)
  4. 6-10 attorneys (10.02%)(+1.04%)
  5. 100+ attorneys (8.48%)(+.54%)
  6. 40-99 attorneys (4.10%)(+.85%)

Reasons?
Profile of Legal Malpractice Claims 2008-2011

- Top Five Claim Activities Leading to Claims
  1. Prep, File Documents (28.33% of all claims)(+2.94% diff from 2007)
  2. Advice (20.19%)(+7.51%)
  3. Commencement Action (17.31%)(-.02%)
  4. Pre-Trial, Pre-Hearing (8.55%)(-2.74%)
  5. Settlement/Negotiation (6.79%)(-.87%)
Claim Stats and Claim Trends

Profile of Legal Malpractice Claims 2008-2011

• 45.07% due to alleged Substantive Errors
• 30.13% due to alleged Administrative Errors
• 14.61% due to Client Relations
• 10.19% due to Intentional Wrongs
Ames & Gough Claim Survey Results 2012

2012 Claims Flat Compared to 2011

• Claims Flat (all but one insurer indicated 2012 claims being filed was flat compared to 2011)
• 2011 – Claims had increased by 6-10% with all insurers
$50-$100 Million Dollar Payouts increasing

- Share of claims resulting in multi-million dollar payouts has grown exponentially
- 4-6 insurers indicated their company had paid or had participated in paying a claim of $100 million or greater and another had a payment between $50 million - $100 million
Claim Stats and Claim Trends

Ames & Gough Claim Survey Results 2012

Claim Severity (over $500K) is Steadily Increasing

- The number of large claims has risen sharply
- 5-6 insurers indicated their company seen an increase in claims with a reserve (including loss and expenses) of more than $500K in 2012.
Andrew C. Seiber
Partner
SmithAmundsen
Jody A. Harris RPLU
Managing Director
Arthur J. Gallagher & Co.
The Lawyers E&O Market

- Hard Market from Late 2001 to 2004
- Soft Market from 2004 to 2011
- Economic Downturn Catches Up with the Lawyers – Deals Unraveled, More Claims
- Expenses on the Rise – Cost of Defense, Experts, E-Discovery, Life-Span of Cases Longer
The Lawyers E&O Market

- Firming Market from 2012 to ???
- Primary Market Rate Increases but Excess Market Competition
The Lawyers E&O Market Changes

- Rate Increases for Good Law Firm Risks - Vary by Size of Firm, Time Carrier has Been in the LPL Market and Historical Carrier Approach to Pricing
- Stricter and More In Depth Underwriting
- Movement to Non-Admitted Paper - More Flexibility
- Carrier Commitment to Long Term Clients
The Lawyers E&O Market

• Expense Priority:
• Control of Defense Costs
• Pre-Agreed Choice of Defense Counsel
• Pre-negotiated rates before the claim

• The Good News – Carriers are not Leaving the LPL Marketplace – Growth is Still a Priority – 40+ Markets
Cyber Liability for Law Firms

- Doesn’t the Lawyers Professional Policy Cover all a Firm’s Cyber Risks? - Not Really…..
- Law Firms are Hacker Targets – One Stop Shopping for Hackers
- Small to Mid-Size Entities – Less Sophisticated Systems Make Attractive Targets
- Law Firm Cyber Attacks Originating from China
Overview: Cyber Liability for Law Firms

- Retaining Clients:
  - RFPs regularly request cybersecurity information
  - Lawyers are valued for confidentiality, but breach exposes sensitive information.

- Protecting the Bottom Line:
  - Breaches are expensive
  - Are firm reserves/insurance adequate?
How Do Law Firm Breaches Happen?

• Lost/Stolen Portable Device
• Breaking and Entering Office Theft
• Unauthorized System Access: Hack or Disgruntled/Careless Employee
• Downstream Vendor/Expert
Not Covered by the LPL Policy?

- Forensic IT Costs – *Not Covered by Lawyers Professional*
- Breach Notification Mailing, Call Centering and Identity Restoration Services Costs – *Not Covered by Lawyers Professional*
- Public Relations Costs – *Not Covered by Lawyers Professional*
- Regulatory Investigation – *Not Covered by Lawyers Professional*
- Regulatory Fine – *Not Covered by Lawyers Professional*
- Litigation Defense, Settlement or Judgment?? - Is the claim related to rendering professional services? Strict definitions of legal services. Is it administrative versus professional?
Liability for Breaches: Regulations

• Most Regulations Trigger by the “Residence” of a Breached Individual – A Breach Can Mean Compliance with Multiple State Regulations.

• NOT:
  – Where Defendant Does Business,
  – Where Defendant is Located, or
  – Where a Plaintiff and Defendant Interacted
• Law Firms are Directly Liable for Multiple Provisions of HIPAA Rules

• Law Firms are “Business Associates” – Third Parties That Perform Services for Health Care Organizations Involving the Use of Protected Health Information (PHI)

• Law Firms Directly Liable for – Privacy, Breach Notification, Security Rule
Changes - HIPAA Omnibus Rule Effective 03/26/13

- Privacy – Law Firms must make reasonable efforts to limit access to Protected Health Information (PHI) exclusively to Lawyers who need it. Lawyers must request only the PHI needed to defend a case and no more.

- Breach Notification – Omnibus Rule now extends the Federal Breach Notifications Requirements under the 2009 HITECH Act to Business Associates (Law Firms)

- Security Rule – Includes more than 40 standards to safeguard ePHI
# Available Coverages

<table>
<thead>
<tr>
<th>Exposure Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Security Liability</td>
<td>Provides liability coverage if an Insured's Computer System fails to prevent a Security Breach or a Privacy Breach</td>
</tr>
<tr>
<td>Privacy Liability</td>
<td>Provides liability coverage if an Insured fails to protect electronic or non-electronic information in their care custody and control</td>
</tr>
<tr>
<td>Media Liability</td>
<td>Covers the Insured for Intellectual Property and Personal Injury perils the result from an error or omission in content (coverage for Patent and Trade Secrets are generally not provided)</td>
</tr>
<tr>
<td>Regulatory Liability</td>
<td>Coverage for lawsuits or investigations by Federal, State, or Foreign regulators relating to Privacy Laws</td>
</tr>
<tr>
<td><strong>Crisis Management</strong></td>
<td></td>
</tr>
<tr>
<td>Notification Expense</td>
<td>1st Party expenses to comply with Privacy Law notification requirements</td>
</tr>
<tr>
<td>Credit Monitoring Expense</td>
<td>1st Party expenses to provide up to 12 months credit monitoring</td>
</tr>
<tr>
<td>Forensic Investigations</td>
<td>1st Party expenses to investigate a system intrusion into an Insured Computer System</td>
</tr>
<tr>
<td>Public Relations</td>
<td>1st Party expenses to hire a Public Relations firm</td>
</tr>
<tr>
<td>Data Recovery</td>
<td>1st party expenses to recover data damaged on an Insured Computer System as a result of a Failure of Security</td>
</tr>
<tr>
<td>Business Interruption</td>
<td>1st party expenses for lost income from an interruption to an Insured Computer System as a result of a Failure of Security</td>
</tr>
<tr>
<td>Cyber Extortion</td>
<td>Payments made to a party threatening to attack an Insured's Computer System in order to avert a cyber attack</td>
</tr>
<tr>
<td>Technology Services/Products &amp; Professional Errors &amp; Omission Liability</td>
<td>Technology Products &amp; Services and Miscellaneous E&amp;O can be added to a policy when applicable</td>
</tr>
</tbody>
</table>
Has the Next Big Litigation Trend Arrived?

Social Media Ethics Issues
Firms Need to Have a Social Media Policy due to:

- Risks of Not Maintaining Client Confidentiality
- Attorneys Blogging About Cases
- Attorneys Posting About Cases
- Attorneys Tweeting About Cases
Some Social Media Issues

• Risks of “False Friending” to Gather Information:
• Transactions With Persons Other Than Clients
  Rule 4.2 Communication With Person Represented By Counsel
• In representing a client, a lawyer shall not communicate about
  the subject of the representation with a person the lawyer
  knows to be represented by another lawyer in the matter,
  unless the lawyer has the consent of the other lawyer or is
  authorized to do so by law or a court order.
Duties to use technology and know the risks:

Rule 1.1 – Includes:

• Maintaining Competence

• [8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology (includes social media), engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.
Some Social Media Issues

- Preservation of Evidence - Can you advise a client or insured to take down harmful social media content, or are you risking spoliation of evidence?
- Lawyers need to know how to use social media ethically in their jurisdiction.
- Lawyers need to know that they can’t advise clients on the destruction of “social media” evidence any differently than they advise clients on other forms of evidence – Lester vs. Allied Concrete (Virginia)- $722,000 sanctions against lawyer and client for lawyer advising client to take down his Facebook page.
- Litigation holds should be extended to social media profiles, blogs, etc
• Rule 7.4 provides that an attorney cannot claim a specialty unless it is in admiralty or patent law, or unless the lawyer has obtained a certification.

• This rule also applies to social media

• LinkedIn use by lawyers can easily violate this rule by listing specialties
Some Social Media Issues

• Social Media is subject to the same ethical rules as all other forms of communication
• Firms need to adopt a firm-wide social media policy that conforms with the Rules of Professional Conduct for your jurisdiction, formal opinions and case law.
Law Firms Can’t Afford This….

“The motion has been made and seconded that we stick our heads in the sand.”
Paul C. Wright, RPLU
Underwriting Consulting Director
CNA
$PLUS$ Plaintiff/Real Estate/Intellectual Property

- Exposure Differentiation and Keys to Profitability
- Regulation
- Specialization
- Client Selection
- Communication
Obstacles To Hard Market Underwriting

- Continuing Economic Pressures
- Shifting Carrier Philosophies
- Available Capacity
- Inconsistent (Inadequate) Pricing
- Account Selection
New Hard Market Objectives:

• Portfolio Profitability
• Capacity Management
• Consistent Philosophy and Pricing
• Patrick J. Lubenow – Moderator
  – Partner, SmithAmundsen
• Amy K. Egelston – Panelist
  – Senior Manager - Litigation, PlanteMoran
• Howard Fishbein – Panelist
  – Chief Claims Officer/Senior Vice President, York Pro Inc.
• Tony J. Novak – Panelist
  – Attorney, Larson King
• William J. Thompson – Panelist
  – Claims Manager, Monitor Liability Managers

Special Thanks to…
Jim Stewart, ProAccess and Larry Smith, SmithAmundsen
What Kinds of Risk Management Services Are available?

- Hotlines
- Websites
- Forms libraries (engagement and disengagement letters)
- CE credits via website and webinars
What Not To Do When You Have a Claim

- Panic
- Admit liability
- Try to settle on your own
- Retain counsel
- Be difficult with your carrier
- Offer to help your client for free
What Should an Insured Do When They Have a Claim?

• Do not panic
• RTFP
• Check your policy (RTFP)
• Notify your broker and carrier ASAP (See Cuthill v. Eddy v. Cont. Casualty 784 F.Supp2d 1331(MD FL 2011)
• “As a condition precedent to coverage, the Insured shall give written notice of any claim as soon as practicable”
• Details, facts, names, dates, addresses, phone numbers, circumstances.
• A narrative helps.
Common Coverage Issues

• Def. of damages: monetary judgment, award or settlement, pre-judgment interest and post judgment interest
• Does not include:
  – Civil or criminal fines, penalties, sanctions or penalties imposed by law or otherwise
  – Punitive or exemplary damages
  – Fees and costs paid or incurred or charged by the insured
  – Non-pecuniary or injunctive relief
Common Coverage Issues

• Policy only covers Professional Services defined as:
  – Performed by an Insured solely in the Insured’s practice in accountancy, financial planning and consulting
  – As administrator, executor, mediator, notary public, trustee or similar fiduciary capacity
  – Performed by an Insured in consulting, training, servicing, ordering, delivering or installing computer software for the sole use of insured or client
  – Performed by an insured in connection with formal accreditation board, stands review or similar activity related to the profession

For remuneration inuring to the benefit of the insured (or predecessor firm) or on a pro bono basis (if approved)
China Reverse Mergers
Coming to America – The Reverse Merger Process

• **STEP 1** - Businesses in China locate shell companies in the US and propose a merger.

• **STEP 2** - An underwriter hires a CPA firm to prepare the financial statements required for the merger to be approved by the SEC.

• **STEP 3** - Once the merger is approved, the company is renamed. Oftentimes, the new company name has the word “China” in it.
Coming to America – The Reverse Merger Process

• **STEP 4** - The new company is registered to trade on a US stock exchange, generally an OTC exchange, but will move up on the exchanges as they gain credibility.

• **STEP 5** - The company works with an investment banker to sell additional shares and as they do the stock price increases. Additional financial statements are issued.
Key Audit Risks in Emerging Markets (China)

- Chinese GAAP v. US GAAP differences (receivables, revenue)
- Large unexplained discrepancies between amounts included in financials in SEC filings v amounts included in financial reports to local Chinese regulators
- Government owned entities & related parties impact financial statements significantly
### Example CRM Delistings:

<table>
<thead>
<tr>
<th>Company Name</th>
<th>Date</th>
<th>Type of Suspension</th>
<th>Reason for Suspension/Delisting</th>
</tr>
</thead>
<tbody>
<tr>
<td>China Intelligent Lighting &amp; Electronics, Inc.</td>
<td>March 2011</td>
<td>Halted by SEC</td>
<td>Forged acctg records, bank stmts. No longer rely on FS.</td>
</tr>
<tr>
<td>China Century Dragon Media, Inc.</td>
<td>March 2011</td>
<td>Halted by SEC</td>
<td>Falsified acctg records &amp; potential material errors in FS.</td>
</tr>
<tr>
<td>China Changjiang Mining &amp; New Energy Co., Ltd.</td>
<td>4/1/2011</td>
<td>Temporary</td>
<td>Failure to disclose CPA resigned. SEC filings inaccurate/incomplete/not reviewed by CPA. Audited FS not reliable.</td>
</tr>
<tr>
<td>Subaye</td>
<td>4/7/2011</td>
<td>Halted</td>
<td>Inadequate documentation related to sales agents &amp; promotion activities.</td>
</tr>
<tr>
<td>China Agritech, Inc.</td>
<td>4/18/2011</td>
<td>Delisted by NASDAQ</td>
<td>Auditors fired. BOD members resigned. Fraudulent financial reporting.</td>
</tr>
<tr>
<td>NIVS IntelliMedia Technology Group, Inc.</td>
<td>April/May 2011</td>
<td>Delisted</td>
<td>Massive acctg fraud involving co records &amp; bank stmts.</td>
</tr>
<tr>
<td>China MediaExpress</td>
<td>5/19/2011</td>
<td>Delisted from NASDAQ</td>
<td>Cannot rely on FS &amp; mgt representations.</td>
</tr>
<tr>
<td>Douyuan Printing</td>
<td>5/31/2011</td>
<td>Delisted by NYSE</td>
<td>Co. misconduct related to fraud in sale of securities, filing false documents with SEC. Engaging in deceit w/auditors.</td>
</tr>
<tr>
<td>China-Biotics Inc.</td>
<td>6/15/2011</td>
<td>Delisted from NASDAQ</td>
<td>CFO &amp; Audit committee chairman resignations. Co. falsified records.</td>
</tr>
</tbody>
</table>

Source: SEC website and press releases for individual companies
<table>
<thead>
<tr>
<th>Audit Firm *</th>
<th>CRM Issuer Engagements as of March 31, 2010</th>
<th>U.S./Non-U.S. Audit Firm</th>
<th>Date of Last Published Inspection Report **</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Malone Bailey, LLP (f/k/a Malone &amp; Bailey, PC)</td>
<td>10</td>
<td>U.S.</td>
<td>April 2009</td>
</tr>
<tr>
<td>3. PKF (Hong Kong SAR)</td>
<td>7</td>
<td>Non-U.S.</td>
<td>March 2010</td>
</tr>
<tr>
<td>5. AGCA Inc.</td>
<td>5</td>
<td>U.S.</td>
<td>December 2010</td>
</tr>
<tr>
<td>6. Albert Wong &amp; Co. (Hong Kong SAR)</td>
<td>5</td>
<td>Non-U.S.</td>
<td>March 2010</td>
</tr>
<tr>
<td>7. Frazer Frost, LLP (f/k/a Moore Stephens Wurth Frazer &amp; Torbet, LLP)</td>
<td>5</td>
<td>U.S.</td>
<td>May 2008</td>
</tr>
<tr>
<td>8. Goldman Kurland and Mohidin, LLP (f/k/a Goldman Parks Kurland Mohidin LLP)</td>
<td>5</td>
<td>U.S.</td>
<td>N/A</td>
</tr>
<tr>
<td>9. Samuel H. Wong &amp; Co., LLP</td>
<td>5</td>
<td>U.S.</td>
<td>N/A</td>
</tr>
<tr>
<td>10. HKCMCPA Company Limited (f/k/a ZYCPA Company Limited)</td>
<td>5</td>
<td>Non-U.S.</td>
<td>February 2010</td>
</tr>
<tr>
<td>11. Child, Van Wagoner &amp; Bradshaw, PLLC</td>
<td>4</td>
<td>U.S.</td>
<td>July 2010</td>
</tr>
<tr>
<td>12. Friedman LLP</td>
<td>4</td>
<td>U.S.</td>
<td>March 2010</td>
</tr>
<tr>
<td>14. Patrizio and Zhao, LLC</td>
<td>4</td>
<td>U.S.</td>
<td>November 2009</td>
</tr>
<tr>
<td>17. Acquavella, Chiarelli, Shuster, Berkower &amp; Co., LLP</td>
<td>3</td>
<td>U.S.</td>
<td>N/A</td>
</tr>
<tr>
<td>18. BDO Limited (Hong Kong SAR)</td>
<td>3</td>
<td>Non-U.S.</td>
<td>N/A</td>
</tr>
<tr>
<td>19. Dominic K.F. Chan &amp; Co</td>
<td>3</td>
<td>U.S.</td>
<td>N/A</td>
</tr>
<tr>
<td>20. Etna Audit Group P.C. (f/k/a Davis Accounting Group PC)</td>
<td>3</td>
<td>U.S.</td>
<td>April 2008</td>
</tr>
<tr>
<td>22. Madsen &amp; Associates CPA’s, Inc.</td>
<td>3</td>
<td>U.S.</td>
<td>December 2009</td>
</tr>
<tr>
<td>23. MS Group CPA LLC</td>
<td>3</td>
<td>U.S.</td>
<td>N/A</td>
</tr>
<tr>
<td>24. UHY Vocation HK CPA Limited</td>
<td>3</td>
<td>Non-U.S.</td>
<td>N/A</td>
</tr>
<tr>
<td>Total</td>
<td>110</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total CRM companies</td>
<td>157</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Percentage of total CRM companies</td>
<td>70%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
FBAR (Foreign Bank Account Report)

- Bank Secrecy Act Section 5314(a), 1970 established FBAR.

Who must report:

1. A U.S. person;
2. Had a “financial interest” in, “signatory authority” or “other authority” over;
3. One or more “financial accounts”;
4. Located in a “foreign country”;
5. The aggregate value of such account(s) exceeded $10,000.00; and
6. At any time during the calendar year.

Definition of Financial Account includes bank accounts, security accounts, securities derivative accounts, other financial instruments accounts, savings accounts, demand accounts, deposit accounts, time deposit accounts, and mutual funds.
• In 2001, the Patriot Act included language that FBAR would also be useful in conducting activities to protect against international terrorism.

• In 2003 the Secretary of Treasury delegated the authority to investigate FBAR violations to the IRS (stepped up enforcement of FBAR violations)

• On October 22, 2004 the American Jobs Creation Act of 2004 added civil penalties for “non-willful” violations of FBAR (maximum penalty of $10,000.00). Increased the maximum penalty for “willful” violations of FBAR (maximum penalty of $100,000.00 or 50% of the amount of the transaction or the balance in the account at the time of the violation, whichever is greater).

• Penalties for criminal violations result in a fine of not more than $250,000.00 or five years in prison or both and if the failure to file is a pattern of illegal activity, a fine up to $500,000.00 and imprisonment of up to ten years.

• Previous penalty ranged from $25,000.00 to $100,000.00
Non-Willful Violation and Willful Violation

- Non-Willful: Any failure to file the FBAR.

- Willful: Case law defines it as “voluntary, intentional violation of a known legal duty.” If one knows an FBAR must be filed and doesn’t do it, it’s willful.
How to Report

1. Form 1040, Schedule B, Part 3 asks if the individual has an interest in a financial account in a foreign country by checking “Yes” or “No”; and

When Must an FBAR Be Filed

• By June 30 the following year and no extensions are available, it must arrive at the IRS on or before June 30.

• Beginning July 1, 2013 all FBAR forms must be filed electronically with certain limited exceptions
• The IRS Office of Professional Responsibility issued this statement in response to taxpayers blaming tax preparers for failing to file FBAR. It cited Circular 2320, Section 10.22 for the level of due diligence required to prepare correct responses to FBAR.

• Circular 230, §10.22 addresses the level of due diligence required. It says:

§ 10.22 Diligence as to Accuracy: Each attorney, certified public accountant, enrolled agent, or enrolled actuary shall exercise due diligence:

(a) In preparing or assisting in the preparation of, approving, and filing returns, documents, affidavits, and other papers relating to Internal Revenue Service matters;

(b) In determining the correctness of oral or written representations made by him to the Department of the Treasury; and

(c) In determining the correctness of oral or written representations made by him to clients with reference to any matter administered by the Internal Revenue Service.
Circular 230, Section 10.34(d) states:

A practitioner may generally rely, in good faith and without verification, on information furnished by a client. However, good faith reliance contemplates that a practitioner will make reasonable inquiries when a client provides information that implies possible participation in overseas transactions/accounts subject to FBAR requirements. A practitioner may rely on information provided by a client in good faith. However, a practitioner may not ignore the implications of any information provided to or actually known by the practitioner. If the information furnished by the client appears to be incorrect, inconsistent with other known facts, or incomplete, the practitioner is required to make further inquiry. The practitioner is also required by Circular 230, Section 10.34(c) to advise a client of any potential penalties likely to apply to a position taken on a return the practitioner is preparing or on which he/she is advising…
Examples of Required Reporting

1. You have a bank account in a foreign bank in Switzerland with a maximum of $25,000.00 in it during the year you must file an FBAR reporting the existence of the account and pay taxes on the income.

2. You have an elderly relative in France who wants to leave you the money in her security account. Prior to her death she adds your name as a signatory on the account to make it easier for you to receive the money in the account upon her death. Even though you may have received no income, you still must file an FBAR form disclosing the existence of the account.

3. Your aunt dies in Italy and leaves you her home. After a month the home is sold for $100,000.00 and the proceeds of the home are placed in an account in Italy in your name. A week later the proceeds from the sale of the home are converted to U.S. dollars and a check is mailed to you in the U.S. Even though the account was only opened in your name for one week, you are obligated to file an FBAR.

4. Your company transfers you to work in Germany. You move to Germany for one year. You open a bank account in Germany to pay expenses. If that bank account has more than $10,000.00 at any time, you have to file an FBAR.
FATCA (Foreign Account Tax Compliance Act)

- FATCA was part of the hiring incentives to restore Employment Act signed March 18, 2010 which took effect January 1, 2013.
- Makes significant changes for information reporting of foreign held assets.
- Foreign banks voluntarily file a Foreign Financial Institution (FFI) Agreement with the IRS and agree to identify U.S. citizen held accounts, comply with due diligence procedures and IRS reporting requirements.
- Those that do not file will be subject to a 30% withholding of income derived from the U.S. citizen held account beginning January 1, 2014.
- The FFI must report the name, address and TIN of each U.S. account holder, the account number, value at year-end, gross dividends, interest and other income paid to the account.
• FATCA also has its own reporting requirement. A new tax form, 8938, must be attached to the taxpayer’s annual income. Reporting is required if the value of the foreign held financial asset is more than $50,000.00 on the last day of the tax year or more than $75,000.00 at any time during the tax year for single tax payers; $100,000.00 on the last day of the tax year or more than $150,000.00 at any time during the tax year for married tax payers filing jointly.

• Failure to file form 8938 will result in a $10,000.00 fine and additional penalties of up to $50,000.00 for continued failure to file after being notified by the IRS.

• As a result of the regulations created by FATCA, many foreign banks have been closing accounts and denying new accounts for U.S. customers.
The AICPA “Clarity Standards” (Clarified Statements on Auditing Standards)
Auditing Standards Board-Clarity Project Goals

- Address concerns over length and complexity of standards
- Make standards easier to read, understand and implement
- Lead to enhancements in audit quality
Clarity Format

- Introduction
- Objectives
- Definitions
- Requirements
- Application Material
- Appendices and Exhibits
Changes to the Clarity Standards

- Primary difference relates to “Group” Audit Standard
- Enhanced “Quality Control” guidance for CPA firms
- Changes in audit opinion to more clearly describe management’s responsibility
Auditor’s Reports (AU-C 700, 705, 706)

Headings and Subheadings

Management’s responsibilities

Opinion
- Basis for qualified, adverse, or disclaimer opinion

Emphasis of Matter
- Matters appropriately presented or disclosed

Other Matter
- To understand audit matters

Other auditor reporting responsibilities
<table>
<thead>
<tr>
<th>AU Section</th>
<th>AU % Superseded</th>
<th>Superseded by:</th>
<th>Related ISA</th>
<th>Status (Feb. 2013)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statements on Auditing Standards-Introduction</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>110 Responsibilities and Functions of the Independent Auditor</td>
<td>All</td>
<td>Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance With Generally Accepted Auditing Standards [1]</td>
<td>200</td>
<td>FS</td>
</tr>
<tr>
<td>120 Defining Professional Requirements in Statements on Auditing Standards</td>
<td>All</td>
<td>Quality Control for an Engagement Conducted in Accordance With Generally Accepted Auditing Standards</td>
<td>220</td>
<td>FS</td>
</tr>
<tr>
<td>150 Generally Accepted Auditing Standards</td>
<td>All</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>161 The Relationship of Generally Accepted Auditing Standards to Quality Control Standards</td>
<td>All</td>
<td>Quality Control for an Engagement Conducted in Accordance With Generally Accepted Auditing Standards</td>
<td>220</td>
<td>FS</td>
</tr>
<tr>
<td><strong>The General Standards</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>201 Nature of the General Standards</td>
<td>All</td>
<td>Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance With Generally Accepted Auditing Standards [1]</td>
<td>200</td>
<td>FS</td>
</tr>
<tr>
<td>210 Training and Proficiency of the Independent Auditor</td>
<td>All</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>220 Independence</td>
<td>All</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>230 Due Professional Care in the Performance of Work</td>
<td>All</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The Standards of Field Work</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>311 Planning and Supervision</td>
<td>All except .08-.10</td>
<td>Planning an Audit</td>
<td>300</td>
<td>FS</td>
</tr>
<tr>
<td></td>
<td>.08-.10</td>
<td>Terms of Engagement</td>
<td>210</td>
<td>FS</td>
</tr>
<tr>
<td>312 Audit Risk and Materiality in Conducting an Audit</td>
<td>All</td>
<td>Materiality in Planning and Performing an Audit</td>
<td>320</td>
<td>FS</td>
</tr>
<tr>
<td></td>
<td>All</td>
<td>Evaluation of Misstatements Identified During the Audit</td>
<td>450</td>
<td>FS</td>
</tr>
<tr>
<td>314 Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement</td>
<td>All</td>
<td>Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement</td>
<td>315</td>
<td>FS</td>
</tr>
</tbody>
</table>
• Summary of Differences Between Existing SASs and Clarified SASs
• Substantive Differences Between the ISAs and GAAS
• Mapping of Existing AU sections to AU-C sections (see handout)
• Listing of Effective Dates of Each AU-C section
• History and Role
• Created with Sarbanes-Oxley to oversee auditors of US public companies
• Previously: Self-regulated
• SEC has oversight of PCAOB
Required Inspections

- Annually for accounting firms that provide audit reports for more than 100 issuers
- Triennially for firms that provide audit reports for less than 100 issuers
- January 2011 – 2,388 public accounting firms registered with PCAOB
Process

- Inspector reviews work on numbers audits
- No firm influence on selection
- Inspecting design of quality control and procedures implemented by firms
- Cooperation required
Sanctions

• Meant to deter recurrence and enhance QC
• Possible suspension or revocation of registration
• Suspension or bar of an individual
• Civil monetary penalties
• Other remedial or training measures
Recent Orders

• E&Y – product returns at a pharmaceutical company (Feb. 2012)
  – Firm censured and fined $2M
  – Partners and staff barred or censured ($25K-$50K fines)

• D&T – understated return reserves
  – Firm fined $1M
  – Partner barred
State Disciplinary Action

- Failure to renew / Logistical Action; OR
- Standard of care allegations
  - Precursor to litigation?
  - Record setting for future claim?
Koss (video)
Sujata Sachdeva, VP of Finance, Secretary and Principal Accounting Officer of Koss embezzled $34 million dollars from Koss from 2004 through December, 2009.

$15 million dollars stolen by authorizing 500 cashier checks to retailers for personal goods (for example cashier’s checks to Neiman Marcus and Saks Fifth Avenue were identified as “N-M” and “SFA.”)

Stole $16 million dollars by authorizing more than 200 bank wire transfers from company funds to pay her personal American Express credit card.

Issued checks payable to “petty cash” and had Koss employees negotiate and return the money to her which she used for personal expenses.

Converted unused travelers checks that the company had purchased for use by its employees traveling on company related business and fraudulently used them for herself.
• A former senior accountant, Julie Mulvaney, assisted in concealing the theft by overstating assets, expenses, and cost of sales and by understanding liabilities and sales.

• Michael Koss, Chief Executive Officer, Chief Financial Officer and President issued the required certifications for the company stating he reviewed the annual report on Form 10K of Koss Corporation and that the report did not contain any untrue statements and among other things that the report fairly presented the financial condition of the company and he evaluated the effectiveness of the company’s disclosure controls.

• The embezzlement was discovered when American Express Company contacted Koss Corporation after tracking wire transfers from Koss Corporation to pay Sachdeva’s personal American Express bills.
• On June 24, 2010 Koss Corporation sued Sachdeva and Grant Thornton, Koss’ accounting firm in Cook County, Illinois. The counts against Grant Thornton were for professional negligence; fraud and deceit; and negligent misrepresentation.

• The alleged false representations made by GT included that it did plan and conduct its audits in accordance with GAAS; that Koss’ financial statements were presented fairly in conformity with GAAP; that those financial statements were free from material misstatement and that the system and internal accounting controls at Koss were adequate.

• In articles reporting on the suit, GT stated it was not retained to evaluate Koss Corporation’s internal financial reporting controls.
Dixon (video)
Rita Crundwell, the Dixon controller, embezzled $53 million dollars between 1991 to April 17, 2012.

In 1990 Crundwell opened a secret bank account in the name of the City of Dixon.

As comptroller, she wrote checks on the City of Dixon Capital Development Fund Account made payable to “Treasurer”, she signed those checks and deposited them into the secret City of Dixon bank account.

She then transferred the funds from the secret account to pay her personal and private business expenses including expenses relating to her horse farming operations, personal credit card payments and the purchase of real estate and vehicles.

She also created fictitious invoices purported to be from the State of Illinois to show the auditors for the City of Dixon that the funds that she fraudulently took from the Capital Development Fund were being used for a legitimate purpose.

She concealed her scheme by telling City officials that the City’s budgetary shortfalls were due to the State of Illinois being late in the payment of tax revenues
Dixon (facts)

• She concealed her fraudulent scheme by picking up the mail for the City of Dixon and separating the secret bank account statements. When she was on vacation she had a relative or another Dixon employee separate her mail including the statements for the secret account.

• The fraud was detected when a staffer filling in when Crundwell was on vacation became suspicious and discovered the secret bank account.

• Crundwell lived lavishly, owning a $2.1 million dollar motor home, expensive jewelry.

• Owned 400 horses, horse farms in Dixon, Illinois and Beloit, Wisconsin.

• Owned a home in Florida and threw lavish birthday parties.

• But had only a purported $80,000 salary.
Lawsuit Filed in 2012 by the Same Firm that Sued Koss, (Power, Rogers & Smith)

- Lawsuit against Janis Card Company, Clifton, Larson, Allen and others alleging professional negligence and negligent misrepresentation.
Why Do These Employee Embezzlement Cases Go On Undetected

- Too much authority and not enough controls on one financial person.
- The criminal is able to cover-up the fraud by “cooking the books” to make the embezzlement hard to discover by an outside auditor.
- A traditional financial statement audit is designed to determine if the accounting rules have been properly applied to the company’s financial statements and to run a basic check of the math so as to provide reasonable assurance that financial statements are fairly stated.
- Auditors do not provide absolute assurance on the financial statements (if an employee is good at covering up the embezzlement in the financial records, a properly performed audit may not detect the fraud).
- A company’s internal controls are inadequate.
- Other employees observe the criminals extravagant lifestyle and fail to connect the dots.
When Defending The Auditor, What Do You Look For

1. Was the audit done in accordance with professional standards?
   * Generally Accepted Auditing Standards (GAAS) and Statements on Auditing Standards (SAS) are the most extensive rules for professional standards but others may apply as well.
   * SAS 99 Auditors Responsibility for Fraud Detection. This outlines the process auditors must go through as they consider the possibility that fraud could occur within the company (need to look at whether the issue of fraud was appropriately considered and whether audit procedures were designed accordingly).

2. Do the working papers of the auditor show that the auditors completed all the procedures suggested by the audit program?
3. Did managers and partners sign off on the work programs appropriately?
   * Did the auditors document their work and considered relevant
     issues in the work programs.
   * Do the work programs show the work was actually done? (The
     auditors’ retained expert will go through the work programs in conjunction
     with the work papers to be sure that the representations in the work programs
     match the documented work)

4. How good was the cover-up?
   * The better the criminal covered up the fraud internally, the stronger
     the auditors’ defense will likely be.
Company’s Responsibilities

• A company has to have adequate controls in place to detect unusual variances in the company’s numbers.
• Controls should have detected wire transfers from the company’s bank to Sachdeva’s personal credit card accounts in Koss.
Lessons Learned

• Don’t let your top executives operate in a vacuum. Other executives need to be actively involved in the finance functions so thefts do not go unnoticed.

• Institute some redundancy in your financial system. For example, require more than a single signature on checks.

• Institute better internal controls, for example, to Sachdeva’s personal credit account in the Koss embezzlement.
Lessons From Litigation

• Damages - Keep Your Eye on the Ball
• Audit Frauds-Scope Limitations
• Family Dynamics-Disputes
Cyber Liability for Accountants

- Mostly a first party, not third party risk
- More than just paying damages (notification, letter writing, credit monitoring, press, forensic IT costs, etc.)
Other Cyber Concerns

• What if you are not sure about a breach?
• What if a server is stolen?
• In 39 states, you must notify customers and those whose data may have been compromised.
Cyber Take-A-Ways

- Small breaches not publicized
- About 40% of all breaches* are internal and not necessarily intentional (lost thumb drive, negligence, etc.)
- Reputational damages may be significant
- If a small breach, you can’t get your side of the story told.
- Average cost of data breach is $194 per lost or stolen record* (*Ponemon Institute, 2013)
- BYOD creates new and challenging problems