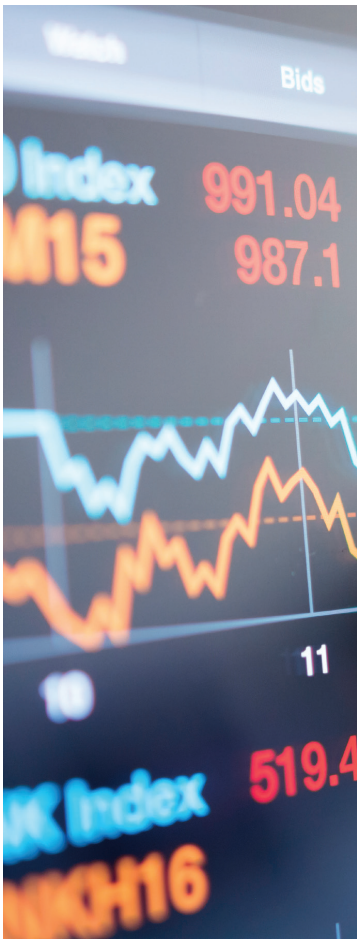
BakerHostetler

Brief

Financial Services Risk Summit

March 2016



On March 3, 2016, the BakerHostetler Financial Services industry team held its inaugural Financial Services Risk Summit. The speakers and panels addressed several key areas affecting the financial services sector: regulatory compliance, internal investigations, privacy and data security, and whistleblower investigations and response.

The state of the industry

Jeffrey D. Quayle, *Senior Vice President & General Counsel, Ohio Bankers League*

Mr. Quayle began the Summit by providing an overview of the current state of the financial services industry, focusing on financial trends in FDIC-insured institutions, trends in the U.S. mortgage market, regulatory developments in cybersecurity and "right sizing" regulatory oversight.

Financial trends in FDIC-insured institutions

Quayle noted that FDIC-insured institutions have enjoyed 20 quarters of solid growth and that the number of institutions on the "problem bank" list has dropped from 203 to 183, the first time it has been below 200 in the past seven years. The percentage of unprofitable institutions, as reported at year-end 2015, is 4.61 percent, down from 6.27 percent in 2014.

Banks earned $40.8 billion in net income during the fourth quarter of 2015, which is an increase of $4.4 billion (11.9 percent) over the same quarter of 2014. These earnings were driven by a $6.8 billion jump in net operating revenue and a $2.7 billion decline in noninterest expenses. All of this means that the average return on assets rose to 1.03 percent from 0.95 percent and net interest income grew 3.6 percent compared with the fourth quarter of 2014. Servicing income and asset sales also fueled revenue growth, with noninterest income up 5 percent year to year. Total industry capital now stands at $1.8 trillion, exceeding the most stringent regulatory standards. It is up 3.5 percent for the year and up 25 percent from the end of the recession. The industry's strong capital buffer is seen as making it capable of handling any economic circumstance that may arise.

But regulators also gave the industry cautionary news: There are signs of growing credit risk, and asset quality dipped slightly in Q4 2015. Net charge-offs rose 7 percent to $10.6 billion, the first year-on-year increase since 2010, with the charge-off growth being concentrated in commercial and industrial loans (especially in the energy sector) and auto loans. In addition, provisions set aside in the fourth quarter for loan and lease losses rose by 45.5 percent to $12 billion, a three-year high.

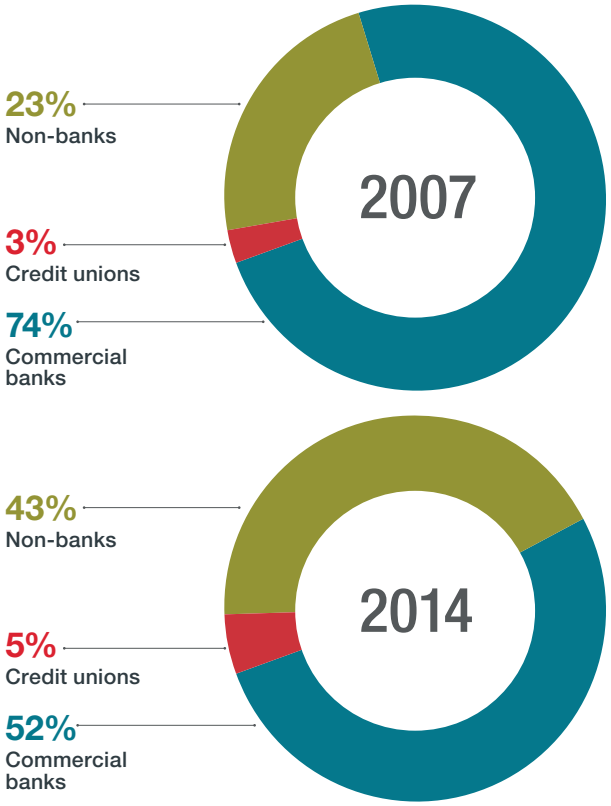
Several regional banks have increased their loan loss reserves related directly to energy loans, i.e., primary loan losses. Community banks have suffered secondary loan losses; that is, loans to businesses either supporting energy or in regions where the energy industry has a big impact.

Most other credit categories saw lower charge-offs, and in consumer loan portfolios, credit losses are tracking consumer loan growth.

Overall, healthy revenue growth continues to be held back by narrow interest margins. Net interest margin grew slightly to 3.13 percent in the fourth quarter, the first time in five years the margin has not declined. However, the improvement only occurred at the big banks, which are better positioned to take advantage of the Federal Reserve's December 2015 rate hike.

To the concern of regulators, many institutions are reaching for yield, going farther out on the risk spectrum, given the competition for borrowers and the low interest rates.

Trends in the U.S. mortgage market



Source: Mortgage Bankers Association

Quayle reported that the share of mortgages originated by banks fell from 74 percent in 2007 to only 52 percent in 2014. According to many observers, large commercial banks now face a regulatory environment so strict that many are hesitant to lend, even to customers with the best credit. In addition, there is essentially no private bond market to which mortgages can be sold.

Industry sources expect that the four largest commercial banks will downsize or even exit the business of originating and servicing residential mortgages. However, many large and regional banks remain committed to the mortgage market.

Of the top 10 originators in 2015, banks lent 28.6 percent of all mortgages, down almost half from 2012 when banks among the top 10 originators accounted for 54.4 percent of all mortgages.

Community banks and credit unions are candidates to step into this void, although Quayle reports they will not be major players because of post-crisis regulations that limit how much mortgage debt they can hold. Credit unions originated 39 percent more mortgage loans for home purchases in the first nine months of 2015 than during the same period in 2014.

The biggest players could be online and nonbank lenders. In 2015, four of the top 10 originators were such entities: Quicken Loans, PennyMac Financial, PPH Mortgage and Freedom Mortgage.

Independent mortgage bankers made up 43 percent of all originations in 2014, a share that has remained steady or grown every year since 2007, when it stood at 23 percent.

Cybersecurity

Cyber risk is top of mind for financial services policymakers. Quayle reports that recent bank exams at all types of institutions reflect this priority. Even though financial institutions recognized the risks early, the sophistication and number of cyberattacks grows daily. In fact, the U.S. Congress passed the Cybersecurity Information Act of 2015 in response to the growing threats to the U.S. economy and its consumers, businesses and government. The Act required the federal government to share more information, including classified information under appropriate safeguards, with the relevant private sector entities to further cybersecurity efforts. It also includes legal authority and protections for private companies to monitor their networks for cybersecurity, take defensive measures and share cyber threat information with each other and with the government.

All federal banking agencies have released a framework for managing cybersecurity risk that outlines key issues and provides tools to help smaller banks assess the risks and develop solutions. This framework can be found on the FDIC's website.

Right-sizing regulatory burdens

Quayle identifies the increasing burden of regulation as one of the largest threats to competitiveness in the financial services sector. Five years after passage of Dodd-Frank, it has become clear that the regulatory pendulum has swung too far. The United States loses banks at the rate of one per day. The burden is particularly severe for smaller community banks, which serve as economic engines for their communities, because the regulations treat them as presenting the same type of risk to the financial system as a multinational institution and require them to invest the same resources into regulatory compliance as much larger regional banks.

Policymakers are beginning to understand how these increased regulatory costs adversely impact their constituents. There are two bills currently under consideration. The first, the Taking Account of Institutions with Low Operation Risk Act, H.R. 2896 (TAILOR Act), was approved by the House Financial Services Committee and would direct financialregulators to tailor regulatory actions to the sizes, business models, risk profiles and other characteristics of the institutions they supervise rather than implement one-size-fits-all "best practices" regulation on everyone. The Senate Banking Committee has approved S. 1481, the Regulatory Relief and Protection Act, to provide certain regulatory relief to community banks. However, it is difficult to build consensus in the current political environment, and the future for both bills is unclear.

What it means to be compromise ready

Theodore J. Kobus III, *Partner and Leader, Privacy and Data Protection Team, BakerHostetler*

Craig A. Hoffman, *Partner, BakerHostetler*

> "We are building walls, but the armies of cyberattackers are against us and they are knocking down the walls and getting what they want – intellectual property, personal information they can monetize, or other information valuable to them." – Ted Kobus

The cyber environment has changed dramatically. Hackers can be in and out of your network before you discover the breach. This fact should change the way businesses manage incident response plans and shift the focus from simply focusing on preventing a breach to detecting and containing a breach quickly. In other words, companies need to become compromise ready.

A few years ago, it was not uncommon for a breach to go unnoticed for months. However, businesses have gotten better at discovering incidents. Mandiant, a U.S. cybersecurity firm, reports that two years ago, there was an average of 243 days from the date of a breach to the date of detection. In 2015, that figure was 205 days. In 2016, it's less than 200 days. Improvement is clearly possible.

It's vital to work with a forensic firm up front to develop plans that maintain forensics and log data in real time so that when a breach is discovered, the forensic firm has a chance to identify the extent of the breach. Without that log data and visibility to endpoints, a business may never be able to tell the extent of the breach or what data was actually compromised.

> "Having a breach is not a disaster. Mishandling it is. People know bad things happen and that people make mistakes at work. When a company is transparent in its communications, and unless it is something really avoidable, people who receive notification letters say 'Thank God it wasn't me who caused the incident.' " – Ted Kobus

Becoming compromise ready involves including several key elements in your cybersecurity program and reviewing them regularly as part of ongoing due diligence. These components include:

- Threat information gathering
- Technology (including encryption)
- Personnel
- Security assessments
- Incident response tabletop exercises
- Ongoing diligence (cyber insurance, vendor management, etc.)

The tabletop exercise is a critical part of the plan. It brings together legal, compliance, privacy, IT, human resources and management. Having periodic exercises brings the team together and ensures critical team members are familiar with the incident response plan, which is critical to making sure the company is prepared for a breach, avoids panic and ensures a better outcome.

Equally important is the concept of threat intelligence and information sharing. A great example of this concept is the "phishing attack" – a fake email designed to deceive its recipients into revealing passwords and other key information. The best "phishing" emails trick 40 percent of employees; the worst 1 to 2 percent. Businesses must empower employees to say, "If I get an email from the CFO that looks a little off, I have to question it." Companies must also brief each other and their workers on these attacks so others know to question the slightly off email message, too.

The importance of rapid detection

Rapid detection is important to contain intrusions and minimize harm. The first step in that process is to establish a "kill chain" – a plan to detect a cyberattack and to stop it before the intruder reaches critical data and/or segmented environments. Companies should ensure they are maintaining and securing forensic data: At the first sign of a breach, collect logs before they have been overwritten or deleted.

When detection of a breach has been delayed, third parties may identify signs of publication or misuse. The news may be made public before the business is even aware of the incident, which in turn forces the business to address the incident publicly before it has the necessary information.

Incident response plans

Kobus and Hoffman stressed that an effective incident response plan should be flexible. Every breach is different and overscripting a response plan can be counterproductive. A response plan should not, for example, dictate exact time frames in which certain tasks may not be completed, because those time frames may not always be realistic. Keeping in mind this flexibility, incident response plans should address these basic issues:

- Preparation
- Identification
- Validation and assessment
- Communication
- Containment
- Eradication
- Recovery
- Post-incident analysis

Regulatory scrutiny

Kobus explained that it is critical for companies to provide their regulators with timely, accurate information as to data security incidents and to explain their approach to the problem, what they are doing to fix it, and how they plan to prevent future incidents. Most of these concerns are the same as those shared by customers: What happened? How did it happen? What are you doing to protect me? And what are you doing to prevent this from happening again?

Kobus and Hoffman are seeing that regulators of the financial services industry have certain hot-button issues that may trigger increased scrutiny of an organization in the wake of a breach, including:

- Encryption of portable devices, which may include backup tapes
- Patching of servers and routers
- The extent of security and awareness training (annual training, orientation, and ongoing communications and events). Keep records of all such activities.
- Ignoring risk assessments
- Two-factor authentication, especially for retailers
- Slow detection of incidents
- Slow notification
- Repeat offenders

Financial institutions should review their security and compliance plans to ensure that these issues are addressed. Banks have a built-in trust factor that can be lost if there is a failure to build in data security. In the face of pressure to push out new technology, such as mobile wallets, it is vital to put the security and privacy measures up front. The Consumer Financial Protection Bureau (CFPB) has just announced a "no-action letter" program for a new financial technology product, but companies should note that these letters are not binding and can be revoked.

Whistleblowing in the financial services industry

Tracy Cole, *Partner, BakerHostetler*

Martin T. Wymer, *Partner, BakerHostetler*

Tracy Cole and Martin Wymer presented an overview of whistleblower regulations and actions in the financial services industry. They began with an overview of three particularly relevant statutes affecting financial services businesses:

- Sarbanes-Oxley Act of 2002
- Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010
- Consumer Financial Protection Act of 2010

They examined these regulations and the current state of law regarding the various whistleblower applications.

They noted that there are several practical issues that affect the industry, including the fact that the government's approach, including the SEC's whistleblower bounty program, is both "a carrot and a stick." Regulations allow a whistleblower to participate in the program even if he or she is one of the wrongdoers. Conversely, if an employee is aware of wrongdoing and fails to report it, that person can be held personally liable in some circumstances.

It is vital to identify someone outside of the reporting line to whom employees can turn with a concern. If they are uncomfortable with the in-house reporting protocol, they may report the issue to regulators or call a plaintiff's firm. This is one cultural concern that businesses can change that may reduce their exposure in these areas.

Lawyers as whistleblowers

Sarbanes-Oxley provides that if an attorney becomes aware of evidence of a "material violation," the attorney must report it up the specified ladder. In addition, the attorney may reveal confidential information to the Securities and Exchange Commission (SEC) to the extent that he or she reasonably believes necessary to prevent commission of a material violation likely to cause substantial injury, perjury in an SEC proceeding or fraud on the SEC or to rectify the consequences of certain material violations.

However, there are a number of state bar rules that govern attorney ethics, including the duty of confidentiality, that are sometimes inconsistent.

Under Dodd-Frank's regulations, where internal reporting is protected, attorneys are included. Many courts have found that attorneys also may bring retaliation claims. As for a whistleblower bounty, while lawyers' information is not generally considered "original information," under certain circumstances they can claim a bounty.

Critically, compliance employees also are eligible for a whistleblower bounty. Under Dodd-Frank, an audit or compliance employee is eligible for a bounty if the individual made an internal report and 120 days have lapsed, if there is a reasonable basis to believe that disclosure to the SEC is necessary to prevent the entity from conduct likely to cause substantial injury to the financial interest or property of the entity or investors, or if there is a reasonable basis to believe that the relevant entity is engaging in conduct that will impede an investigation of the misconduct.

Minimizing risk when an employee blows the whistle

When faced with a whistleblower action, a business should:

- Ensure timely and accurate documentation of performance issues.
- Insulate decision-makers vis-à-vis complaining employees from any corporate investigation of complaint.
- Follow corporate policies and procedures.

An additional risk-mitigation measure that businesses should consider including in severance agreements is a representation by the employee that he or she has no knowledge of a regulatory or legal violation or has never complained about misconduct. This can give employers crucial ammunition if there is a subsequent complaint.

Internal investigations

John J. Carney (Moderator), *Partner and Co-Leader of White Collar Defense and Corporate Investigation Team, BakerHostetler*

Steven M. Dettelbach, *Partner and Co-Leader of White Collar Defense and Corporate Investigation Team, BakerHostetler*

Matthew Greenblatt, *Senior Managing Director, FTI Consulting*

Carlton E. Langer, *Executive Vice President, Chief Legal Officer, and General Counsel, FirstMerit Bank, N.A.*

In September 2015, Deputy Attorney General Sally Quillian Yates issued a memo titled "Individual Accountability for Corporate Wrongdoing," which applies to both criminal and corporate instances of wrongdoing. It was written to address concerns in the financial industry, as well as public expectations that individuals would be held accountable for corporate misdeeds. It also is intended to encourage changes in corporate behavior.

The Yates Memo lays out six key principles:

- To be eligible for any cooperation credit, corporations must provide to the Department of Justice (DOJ) all relevant facts about the individuals involved in corporate misconduct.
- Both criminal and civil corporate investigations should focus on individuals from the inception of the investigation.
- Criminal and civil attorneys handling corporate investigations should be in routine communication with one another.
- Absent extraordinary circumstances, no corporate resolution will provide protection from criminal or civil liability for any individuals.
- Corporate cases should not be resolved without a clear plan to resolve related individual cases before the statute of limitations expires and declinations as to individuals in such cases must be memorialized.
- Civil attorneys should consistently focus on individuals as well as the company and evaluate whether to bring suit against an individual based on considerations beyond that individual's ability to pay.

Essentially, the Yates Memo sets a higher benchmark for cooperation; providing complete information about individual involvement is the "threshold hurdle." It also adds challenges to any internal investigatory team's work, including a greater risk of limited cooperation from key individuals because they fear personal liability, a greater risk that access to critical information may be curtailed, and consequently, the heightened concern by auditors and regulators that the internal investigation team did not access all the critical facts and evidence.

However, there are some provisions for "responsible conduct credit" like that given by the CFPB to several financial institutions. In these cases, the CFPB rewarded institutions that self-reported by lowering penalties and not publicly disclosing the names of those involved. The CFPB notes, however, that "in order for the Bureau to consider awarding affirmative credit in the context of any enforcement investigation, a party's conduct must substantially exceed the standard of what is required by law."

In most internal investigations, the question of privilege arises. According to 12 U.S.C. § 1828(x), banks can disclose materials containing privileged communications to regulators such as the CFPB, federal bank agencies, a state banking supervisor or a foreign bank authority without waiving privilege. Under § 1821(t), one covered agency shall not be deemed to have waived any privilege by transferring that information to another covered agency. Here, privilege is defined as work-product, attorney-client or other recognized privilege.

National banks also are required to file Suspicious Activity Reports (SARs) with the applicable agencies and the Department of the Treasury whenever they detect known or suspected violations of federal law or a suspicious transaction related to money-laundering activity or a violation of the Bank Secrecy Act. In addition, a SAR must be sent to the Financial Crimes Enforcement Network of the Department of the Treasury (FinCEN) if there is insider abuse when the bank has a substantial basis for identifying one of its directors, officers, employees, agents or affiliates as having aided in or committed a criminal act; if there is a violation of $5,000 or more, or a violation of $5,000 or more in funds and involving money laundering.

If the bank files a SAR and the suspect is a director or executive officer, the bank may not notify the suspect, but is required to notify all the directors who are not suspects, 12 CFR § 21.11(h). In its ruling on *Desimone v. Barrows*, 924 A.2d 908, 934-35 (Del. Ch. 2007), the court held that under the Yates Memo, "[b]y consciously causing the corporation to violate the law, a director would be disloyal to the corporation and could be forced to answer for the harm he has caused. Although directors have wide authority to take lawful action on behalf of the corporation, they have no authority knowingly to cause the corporation to become a rogue, exposing the corporation to penalties from criminal and civil regulators. Delaware corporate law has long been clear on this rather obvious notion; namely, that it is utterly inconsistent with one's duty of fidelity to the corporation to consciously cause the corporation to act unlawfully."

In discussion after the formal presentation, the speakers noted that internal investigations are often an art, not a science. They recommend that banks hire outside counsel to conduct the investigation – counsel known for independence and trustworthiness and which possesses the necessary expertise to handle the issue. While there are sound arguments favoring the attorney-client privilege when an internal investigation is conducted by in-house counsel, there is a risk of receiving advice that is weighted toward minimizing the risks to the business rather than a completely independent evaluation of the legal challenges at issue.

Compliance panel

Karl Fanter (moderator), *Partner, BakerHostetler*

F. Thomas Eck IV, *Senior Vice President, Associate General Counsel, The Huntington National Bank*

Ronald V. Johnson, Jr., *Senior Vice President, Compliance Risk, KeyBank National Association*

Jeff Campbell, *Senior Counsel, Quicken Loans, Inc.*

The panel addressed a number of trends and questions.

Should compliance be separated from the in-house legal departments?

The panelists generally identified a trend in the industry to separate the compliance and legal departments of a financial institution. The compliance group generally handles monitoring, testing and training and renders compliance advice. Johnson described the compliance group as a "second line of defense" to management to ensure that controls are in place and being tested.

The panel agreed that there is a close interaction between the legal and compliance functions, with a lot of attention focused on the issue of what constitutes legal advice. Eck acknowledged that there can be "overlap" between the compliance and legal functions. The most pressing concern is capturing areas where a financial institution's compliance program identifies findings or observations of areas where they want to improve and putting that information into an enterprise risk management system to identify, monitor and follow up. But because data are so widely distributed in the organization, it raises questions about attorney-client privilege. Financial institutions must consider competitive, reputational and legal risks from the compliance standpoint, which causes daily tensions within the institutions.

What is the relationship between compliance and federal bank examiners?

The panelists explained that financial institutions should evaluate their policies, procedures and practices in advance of a CFPB examination to ensure that they are prepared. During an examination, there may be eight examiners working 30 hours a week on-site for eight weeks. When the exam begins, a compliance team should explain the organization's culture and guiding principles to the examiners, as those things guide the compliance team's processes and how they implement them, thereby giving the exam team a glimpse into how the institution works on a day-to-day basis. The cooperation should then continue through weekly touchpoint meetings during the examinations to ensure the institution is providing timely and coordinated responses to CFPB queries.

What challenges are you seeing while implementing the new integrated mortgage disclosures, the TILA RESPA Integrated Disclosures (TRID) Rules, also known as "Know Before You Owe?"

Our panelists reported three challenges with TRID implementation. The first is dealing with TRID's three-day waiting period. Under the TRID rules, borrowers must receive the closing disclosure three business days prior to closing. However, lenders have reported an increase in requests from borrowers who want to close prior to the expiration of the three-day period. Further complicating this issue is the mailbox rule, which institutions must use when the borrower does not have an online account. Under the mailbox rule, once the closing disclosure is mailed to the customer, the institution must assume mail delivery will take three days, then wait an additional three days prior to closing.

The second issue revolves around enforcement. Although CFPB Director Richard Cordray said the agency would work with institutions and not take immediate enforcement actions in TRID matters, that does not necessarily mean the plaintiffs' bar will give banks a grace period. TRID has private right of action.

Finally, there was a typographical error in the preamble to the December 2013 rule that dealt with tolerances for prepaid property insurance premiums, taxes and HOA dues. The word "not" was omitted from the preamble. Some businesses programmed their systems to treat those charges as having no tolerance. The CFPB recently corrected the TRID rule to correct the typographical error and clarify the tolerance of those items.

The bottom line is that, through a combination of the TRID rules, ATR, and the Qualified Mortgage rule, it takes longer to process mortgage originations and thus longer to close mortgage loans.

What are the emerging trends in Fair Lending?

Johnson reports that there has been more regulatory activity around Fair Lending, in large part because we are moving out of the recession, resulting in an increase in the need for capital, especially in communities that were seriously affected by the crisis of foreclosure and abandoned homes. In addition, Fair Lending issues – which traditionally have involved mortgage lending – are now coming up in the auto lending context. Lenders pay attention to regulatory guidance and know Fair Lending is a priority for the DOJ and CFPB.

> Mr. Eck commented that "everything that's old is new again in Fair Lending." The original focus was on redlining, then pricing, and now the regulators are looking at redlining anew.

The question they are asking is whether institutions are meeting the needs of predominantly minority communities.

From a compliance perspective, institutions should take note of Reg. B under the Equal Credit Opportunity Act (ECOA), which encourages financial institutions to self-test for compliance. If a financial institution does self-testing and identifies an issue and corrects the issue in a timely and effective manner, Reg. B allows the institution to not disclose the details to regulators. Many see this as an opportunity not to provide a road map to enforcement.

The caveat is that the testing must solely be done for ECOA compliance. Thus, if an institution engages in "mystery shopping" to test for Fair Lending compliance, the mystery shopper should not also be evaluating sales and service quality more generally. Institutions should also consider the practical implications of that privilege, which can be difficult to assess. For example: Does invoking the privilege affect an institution's relationship with the regulator?

What is the impact of the proposed CFPB rule eliminating class action arbitration waivers?

Generally, arbitration provisions in standard consumer contracts are going away. The biggest impact on customer agreements is that the arbitration provision serves as a good check on class action attorneys by forcing people to address individual concerns on an individual basis. Elimination of arbitration waivers will lead to more class actions.

How does the CFPB enforce its prohibitions on UDAAP (unfair, deceptive and abusive practices)?

Under Dodd-Frank, the "abusive" component was added. It is not a "check the box, do X and Y and you're covered" issue. If a practice is likely to cause harm, the rule provides action. UDAAP is being used in conjunction with other regulatory violations. Institutions must focus on their marketing materials, disclosures, and other customer-facing materials. The key is to ensure accuracy.

In addition, financial institutions should be responsive to complaints. One way is to look at systematic trends and problems with respect to complaints and work with the various business lines to ensure compliance. In addition, institutions should look at enforcement actions in the industry from a compliance perspective. There UDAAP is being used as a lever in other regulatory enforcement actions.

Conclusion

The varied panels that addressed the audience at the Financial Services Risk Summit provided a practical overview of many of the key issues that face the industry. For additional information on any of the subjects discussed above, please contact one of these BakerHostetler attorneys.

Financial Services Industry Key Contacts

Brett A. Wall
T 216.861.7597
bwall@bakerlaw.com

Anthony M. Sharett
T 614.462.4771
asharett@bakerlaw.com

Additional Contacts

John J. Carney
T 212.589.4255
jcarney@bakerlaw.com

Tracy Cole
T 212.589.4228
tcole@bakerlaw.com

Steven M. Dettelbach
Cleveland
T 216.861.7177
Washington, D.C.
T 202.861.1621
sdettelbach@bakerlaw.com

Karl Fanter
T 216.861.7918
kfanter@bakerlaw.com

Craig A. Hoffman
T 513.929.3491
cahoffman@bakerlaw.com

Theodore J. Kobus III
T 212.271.1504
tkobus@bakerlaw.com

Martin T. Wymer
T 216.861.6021
mwymer@bakerlaw.com

bakerlaw.com

Celebrating the 100th anniversary of its founding this year, BakerHostetler is a leading national law firm that helps clients around the world to address their most complex and critical business and regulatory issues. With five core national practice groups – Business, Employment, Intellectual Property, Litigation, and Tax – the firm has more than 940 lawyers located in 14 offices coast to coast. For more information, visit bakerlaw.com.