ASSOCIATION OF CORPORATE COUNSEL

TITLE: **Recent Developments in the World of Anti-Money Laundering**

DATE: **November 19, 2008**

PRESENTED BY: **ACC Financial Services Committee**

SPONSORED BY: **Steptoe & Johnson, LLP**

FACULTY: **William Gordon**, Steptoe & Johnson, LLP
Owen Bonheimer, Steptoe & Johnson, LLP

MODERATOR: **Brennan Holland**, Vice President and General Counsel, Home Loan Services, Inc. and Chair of ACC's Financial Services Committee

*****

Operator: Just a reminder, today's conference is being recorded. Welcome to this ACC webcast. Brennan, please go ahead.

Brennan Holland: Thanks, (Megan).

Welcome to the Association of Corporate Council Financial Services Committee webcast entitled, Recent Developments in the World of Anti-Money Laundering. My name is Brennan Holland, and I will be the moderator for today's presentation. I am Vice President and General Counsel for Home Loan Services, and I'm the current Chair of the ACC Financial Services Committee.

We are very pleased to have today Owen Bonheimer and Bill Gordon with our sponsor firm, Steptoe & Johnson, as our presenters. Owen and Bill are both with the International Department of Steptoe & Johnson, in their Washington office. Their practice specialties are in anti-money laundering investigation, Foreign Corrupt Practices act, and other international white collar crime involving money laundering.

So they have quite a lot of experience between them, having appeared in front of the Department of Justice and Securities Exchange Commission on (SEPA) matters, and before the International Center for settlement of investment disputes. And both Owen and Bill have a significant amount of experience in international matters generally.

A couple of housekeeping things, this webcast is being presented through the updated webcast page. You all can pose questions to Owen and Bill by using the chat function on your screen. There's a box at the bottom left-hand corner, and you can click the chat button, and you can submit questions to the panelists by typing the question and then pressing the send button.

Your question won't appear on the other attendees' screens, but will be visible to the panelists and to me. If your question doesn't get answered during the course of the presentation, we will put answers to questions posed at a later date on the financial services Web site. If you have a question after the presentation, you can contact Owen or Bill at the address – e-mail address on the bios, which are over on the left-hand side of your screen, as well.

This webcast, of course, is being recorded. The audio file for this webcast will be available for replay on the ACC Web site about three hours after the end of this presentation and will then be archived on the ACC Web site for about a year.

During the course of the webcast, you will see a satisfaction survey on your screen. And you access that survey by clicking on the button over to the left, where the – where that biography box is. Just click on that, and I ask you to please rate this presentation. It will help us out a lot in deciding what sort of information and materials our membership is interested in.

And now let me turn the presentation over to Owen and Bill.

Owen Bonheimer: Well, thank you very much, Brennan, and hello, everyone. We hope that you don't do the survey until the end of the presentation, because we'll be talking about the most interesting issues at the end, the case studies, where the rubber hits the road and what – how the law is really applied.

But, first, we should apologize. Matt Herrington was not able to make the presentation today, because he got called into court for an emergency hearing in Federal Court, and apparently the Federal Judiciary doesn't accept the priority of training corporate counsel on money laundering compliances as an excuse for not appearing at hearings. Although maybe they should, it would prevent more cases being filed in corporate fraud situations.

But anyway Bill and I are here, and we are experienced in this area, and we can give you some basic information to help keep you out of court and your clients as well.

So why don't we start with the slide on introduction to money laundering. I think that many of you may be familiar with money laundering and the laws regulating it. Others maybe not so much, but one thing about this area is it never hurts to go back and review the basics, because it can get quite complex.

And so there really are two types of transactions that qualify as money laundering. The practical definition, although the statute is quite complex, is that transactions that are designed to conceal the proceeds of crime or transactions that are defined to fund criminal activity, those are the two types of money laundering.

One is – the first one is a transaction that comes after the crime, in the case of concealing the proceeds, and the other type comes before the crime, in the case of promoting criminal activity.

And so with the definition of money laundering discussed, there are different types of cases that arise. The classic case, I think before some years ago, people would always think of money laundering, and they would think of drug dealing. And that's no longer the only situation where this can occur. But even legitimate businesses may encounter situations where drug dealers are trying to conceal the proceeds of their activity by passing them through legitimate businesses.

And so the concealment is one of the key themes that come up in money laundering. It's the effort of criminal enterprises to conceal what they're doing, make their proceeds look legitimate so they can then spend them and conduct activity in the financial system that doesn't lead them to be caught.

Now, the newest case is – if you can – yes, on the 2007 case, this is what's really happening now in the money laundering area is an emphasis on antiterrorism. Since 9-11, the money laundering law has been used as a tool to prevent terrorism and to fight terrorist activity and terrorist financing. And so there are several initiatives in that area.

OK, so now what types of activity – where might you see money laundering? It can really occur when you're dealing with any number of different institutions or different parties acting in different roles.

Your customers could be participating in money laundering, for example, if they buy goods or services that you sell and they use tainted proceeds to buy them, then they are engaging in money laundering through your business. Or you could have a supplier who is selling you what seem to be normal goods or services, they're in a normal business, it appears, but in reality they're selling you tainted goods. And so that kind of example you might see in the case of organized retail theft, where retail goods are stolen, and they are then processed through your business.

Also, third parties can cause problems in the money laundering area, so financial institutions dealing with different types of third parties, like private banks in the late 1990s, face these issues where their customers were conducting transactions through their business and they were not taking adequate steps to prevent them or detect them.

Also, in mergers and acquisitions, you may not realize it but you could be acquiring a business, and that business itself was acquired through bribery or crime or some sort of criminal activity. And the shares in the business could constitute the proceeds of crime.

Or also a joint venture partner, perhaps they're engaged in criminal activity and they're commingling the funds in your joint venture business, and so suddenly you're stuck in a money laundering situation where you need to figure out what to do.

Or, finally, in a transactional context, you could be a bank, and you're issuing a loan, and someone is engaged in mortgage fraud, then the loan proceeds are the proceeds of that fraud, and then you need to figure out what to do in that kind of situation.

And so how are these problems being addressed at the international level? The Financial Action Task Force is an intergovernmental body that has 34 members, including two territories, and the U.S. takes an active role in that organization.

It sets policy goals for national members through what is called the (40-plus-nine) recommendations. And recently it has placed an increasing emphasis on any terrorism efforts, what we might call the nine-elevenfication of any money laundering law.

At the international treaty level there are global and regional treaties, particularly the UN Convention against Corruption, which believe it or not now has 128 countries who have ratified it and the treaty is in force. And Article XXIII of the Treaty requires that parties criminalize money laundering. So it's no longer the United States that has this money laundering regime in a world not concerned with this issue. You have over 30 members in the FATF, and you have over 125 countries that must criminalize money laundering. So what we're going to go through today, some of the U.S. cases, you may start to see similar issues arising in legal systems outside the United States.

Now, the anti-money laundering laws are admittedly complex. The first type of law that we're going to talk about is the criminal statute, it's called the Money Laundering Control Act. And what that prohibits is participating in transactions that are designed to further crime or to conceal the proceeds of crime, what they would call specified unlawful activities, and they are defined by the statute and as well as transporting funds over a U.S. border that are connected with crime.

Now, the statute gives some complex definitions of the elements of the crime and the mental states that are required, it'll take a little too much time to go through those here, but we can refer you to Sections 1956 and 57 of Title 18 of the U.S. Code to get a picture for what's involved in money laundering crime.

An important feature of that crime, though, is that the definition of knowing is quite broad, so the crime occurs when someone knowingly participates in these types of transactions but knowing doesn't mean necessarily actual knowledge. It could also mean willful blindness to circumstances that indicate money laundering. So the "I didn't know" or sort of head in the sand excuse doesn't work.

Brennan Holland: Owen, this is Brennan. How – I know it's got to be difficult to be able to anticipate something that – or to recognize something that by its nature is hidden, but what kind of things can ordinary financial institutions be on the lookout for?

Owen Bonheimer: Well, we're going to talk about what they call red flags in a few minutes, and those red flags are signs of suspicious activity. It's really a risk-based assessment based on what facts and circumstances are known to the financial institution, as to whether there are indicators that something might be wrong. And so this can be sort of a complex exercise. It really depends on what you know about the transaction.

And so one other…

Brennan Holland: And what you know about the law?

Owen Bonheimer: And what you know about the law, which I hope we can help you with today. Although the law doesn't define what is suspicion, it's going to be judged in hindsight by regulators and potentially enforcement authorities based on what evidence you have in the files and what electronic information and documentary information and other information was available to you at the time.

Now, one other thing I should mention about the criminal law is it's no longer excuse if you're operating from abroad. There's extraterritorial jurisdiction under the Money Laundering Control Act over conduct by U.S. citizens or conduct of foreign nationals that occurs partly in the United States.

Now, the last bullet here talks about forfeiture risks, actually that comes later, but I'll mention forfeiture. This is another issue to be concerned about in the money laundering area because even if you're not engaged in a criminal money laundering scheme, if you come into possession of assets that were originally part of that scheme and had been laundered through your organization, it's possible that the government could then forfeit those as the proceeds of crime, and you could unwittingly lose important assets.

The one way to prevent that is to engage in due diligence in your corporate transactions to identify risks and to avoid transactions that appear to be associated with money laundering. And if the due diligence is done, it could establish a defense of good faith and show that you weren't aware of any problems with the transaction. And in that case it would be considerably more difficult for the assets to be forfeited from your organization.

Now, on the last bullet, with regulatory requirements, here's where we're going to spend a little bit of time in the presentation. The main regulation is called the Bank Secrecy Act. It's somewhat of a misnomer because its purpose is to prevent excessive secrecy in banking, and it's also a misnomer because it no longer focuses only on banks. The definition of financial institutions is now quite broad and growing. What this law covers is what steps financial institutions need to take to detect and to prevent money laundering.

Now, I should mention that this law, the Bank Secrecy Act, is quite complex and can be confusing with its definitions, but as corporate counsel you may want to see the Web site of what's called the Financial Crimes Enforcement Network, or FinCEN, they're proposing to reorganize the

regulations, recognizing how complex they are and to simplify them. And so the Web site at www.FinCEN.gov can give you more information on that.

Now, the criminal money laundering statute, that I mentioned, the Money Laundering Control Act involves transactions that are tied to specified unlawful activity. It's probably best that if you have a question or you wonder if a crime is covered under this act to assume it is until you check the law, because the number of specified unlawful activity offenses are quite broad. It's also important to remember that now the SUAs include foreign law violations in some cases, like corruption.

Now, what are the penalties for violating the Money Laundering Control Act, the criminal law? In some cases you'll find that the punishment for violating this law is worse than what you'd call the predicate crime, itself. In other words, if someone engages in money laundering with the proceeds of bribery, it may be that the punishment for the bribery itself would not be as great as the punishment for laundering the proceeds. As you can see, 20 years is quite a long time.

I just gave everyone a chance to look at this slide here. OK?

Now, many of you may work for banks or non-bank financial institutions, and one of the basic questions in this area is are you covered by the Bank Secrecy Act, do you have to comply with the regulations imposed under the Bank Secrecy Act?

As I mentioned, it's a misnomer that this is the Bank Secrecy Act, because it applies now to a broader range of financial institutions. And so the term, “financial institution” is now a term of art, and there are a long list of examples of institutions that qualify as financial institutions under the Bank Secrecy Act.

And some of them are listed here. Now, some of the institutions that you might not typically think of as a financial institution in the banking sense would be listed on this slide, like sellers of vehicles, investment companies, insurance companies.

I should mention as part of the recent regulatory enactments of the outgoing administration, the FinCEN has decided that investment advisors do not have to adopt any money laundering programs, and they are not treated as financial institutions for that purpose under the Bank Secrecy Act.

That was a recent announcement in the last two weeks or three weeks, and that decision was made because investment advisors tend to work through entities that are already regulated under the Bank Secrecy Act, like broker dealers and banks.

Now, why are we talking about the Bank Secrecy Act, and why are we going to focus on that? It's because the requirements of it really affect many aspects of how financial institutions do their business.

As you can see from the slide, the compliance program is required, but also that banks have to focus on policies to know their customers and also to identify their customers, and then there are other requirements, such as recordkeeping, and we'll explore in the case studies the third requirement, which is reporting. Financial institutions have to report certain types of customer activity to the Federal authorities. These are called suspicious activity reports or are commonly referred to as SARs.

Now, Brennan, to go to your question about what are the indicators of a problem, how do you know when you've got an issue, these are some of the examples of red flags that institutions could commonly see.

Now, these help you to see where there might be a problem, because money laundering involves concealment and an effort to conceal illicit activity, it's not typically possible that the financial institution is going to know that some crime is definitely occurring or some criminal activity is behind the transaction.

But indicators, such as those listed on this slide, start to give you a good idea that there might be a problem, like unusual payment methods, whether by amounts involved, if this is not a typical amount that you see pass through a customer's account, or by type, if there's a deal in cash that isn't typically done in cash, or if transactions are structured in small amounts to avoid a reporting requirement, or if third parties are involved without an explanation. Or, as we'll see later, if the parties involved are located in an unusual jurisdiction that doesn't seem to have an explanation.

Now, there are other examples of red flags here, one of them that we'll see in the later case study is that there's conduct that's unusual in the industry, and we'll let you go through these slides at your leisure later. In the interest of time, though, I think we're going to go through the red slides – the red flag slides and go on to recent developments.

Now, this is the fun part. The SEC is what we're going to focus on in these case studies. These four cases that we're going to talk about are cases brought by the SEC, although they focus on broker dealers, the conduct involved has to do with suspicious activity reporting and customer identification procedures. And those two compliance functions are performed by all financial institutions under the Bank Secrecy Act, so these cases provide lessons for all financial institutions, not just broker dealers.

But it's also important to recognize that the SEC isn't the only agency active in this area. The Office of the Comptroller of the Currency, the FDIC, the Federal Reserve, state banking authorities, they are all involved in enforcing these laws.

Now, these four cases are brought by the SEC, which is a newcomer to any money laundering enforcement, because the PATRIOT Act decided that broker dealers were a gap in the system and they needed to be treated as financial institutions.

And so these four cases are breaking into two areas, the Crowell, Weedon case and the E*Trade case cover know your customer, customer identification procedures. And the Park Cantley case and the Pettus case follow – deal with the suspicious activity reporting requirement.

Now, the first case, Crowell, Weedon, is what the legal community called the groundbreaking SEC case where the SEC brought its first enforcement action under the PATRIOT anti-money laundering regulations.

And the interesting thing about this case is the way the SEC prosecutes this type of conduct. The broker dealer here, Crowell, Weedon, had to follow a rule that said that it needed to establish a customer identification program on paper, documenting how it would proceed to verify and establish its customers' identities. And so Crowell, Weedon identified these procedures on paper as checking government identification and checking public records, but in practice what Crowell, Weedon actually did was let its representatives vouch for the identities of its customers.

And so its representatives would say to the company, "Well, I know this customer personally, it's a friend or a family member, or it's a referral." And then Crowell, Weedon wouldn't actually check the government identity or even the public record database. And on the basis of the vouching by the representative or representatives, Crowell, Weedon opened some 2,900 accounts until it fixed these problems.

And the way the SEC prosecuted the case was to say that the customer identification policy was inaccurate because it didn't describe what Crowell, Weedon was actually doing. In other words,

they expected that if Crowell, Weedon was using representatives vouching for customers, then its customer identification policy would actually say that.

And so the SEC expects that the procedures should reflect the practice, and the practice should reflect the procedure. If they're not mirror images of one another then the customer identification program rules would be violated.

An interesting thing about this case is when the SEC brought it, they said, "The case is part of its effort and its commitment to doing its part to protect our homeland." Now the use of the word homeland reminds you that this is part of the antiterrorism effort since 9-11, of which all the money laundering enforcement authorities are part. And in bringing these cases, they're doing so more aggressively because they believe that this is part of a larger policy, not just to combat financial fraud, but to combat terrorism.

Now, the next case, after the warning shot of the Crowell, Weedon case, the SEC brought a bigger case against E*Trade. And similar to Crowell, Weedon, E*Trade said it would do certain things to verify identities. In particular it said it would verify the identities of joint account holders but in practice, it didn't do so for an extended period of time. And the SEC, therefore, found that its policy was inaccurate because its policy said it was doing something when in practice it wasn't doing that.

So the outcome of the case was a $1 million penalty for E*Trade, but perhaps even more significantly than the money E*Trade had to pay was that E*Trade had to engage a compliance monitor for a period of over a year to review its compliance with these requirements.

No doubt this outcome was aggravated by the fact that E*Trade had delayed corrective action even though it had discovered the problem for some time. And so if you compare this case to the Crowell, Weedon case which didn't involve a penalty, only an injunction or a cease-and-desist order, you see that Crowell, Weedon had a procedure, it just wasn't the one they had described in their program. It involved fewer problem accounts and didn't involve an allegation of a failure to promptly correct a problem once it was discovered.

Now, this case, the E*Trade case also emphasizes the significance of antiterrorism policy. The Director of Enforcement at the SEC explained that in their view, a lapse of the type encountered with E*Trade, which affected 65,000 accounts, had the potential to undermine the nation's antiterrorism efforts.

Now, the next two cases concern the suspicious activity reporting requirement. The Park Financial case was the first SEC action against a broker dealer for a failure to file such a report, and it's a good case to explore Brennan's question about how do you know when your customers may be engaging in suspicious activity? And so I'll briefly summarize for you the facts, some of which are described here and which you can find in detail on the SEC Web site.

Park Financial was a broker, and Cantley was a representative at Park Financial, who opened several accounts in the name of companies that were located offshore in the British Virgin Islands. And these BVI companies traded in only one stock, the stock of a company called Spear & Jackson, which was listed as an over-the-counter stock.

Now, Park Financial took instructions on these BVI accounts from the CEO of Spear & Jackson even though the CEO was not authorized to give instructions on the accounts. And in that situation the price of the stock rose quite dramatically, the BVI companies heavily sold the stock, and the stock tumbled. And the SEC took action against the CEO of the company for doing what they called pumping and dumping.

Now, in the action taken against the broker, the SEC cited the failure by the broker to identify and report the suspicious activity. In effect, the broker had failed to detect the red flags involved and to report the activity.

Now, this leads to the question, well, what is the reporting obligation? And it is to report transactions that are known, suspected or where there's reason to believe there's involvement of the proceeds of crime, disguising the proceeds of crime, the evasion of a bank secrecy requirement, use of the financial institution to facilitate crime or a catch-all, where there's no business purpose or apparent lawful purpose or the activity is not normal for the customer while there's no reasonable explanation for what's going on after examine all the facts. And, also, there's a threshold of above $5,000.

Now, looking at…

Brennan Holland: When I had listened to this, one of the things that occurs to me is we're talking about duties to report and duties to disclose, but what about civil liability? I mean if I'm going to hand over a lot of information about a customer, based on a suspicion of activity, what is there to protect me from civil liability?

Owen Bonheimer: Well, there's a pretty strong law that protects against that. It's called the Safe Harbor Provision in the Bank Secrecy Act, and pretty much financial institutions who file these reports will be presumed to be immune from civil lawsuits by customers.

There's a slight range of court cases that refine this standard. In the 11th Circuit it's been determined that the financial institution will have this immunity if it files the report in good faith. Now, in the Second Circuit, there's a finding that no showing of good faith is necessary. So there's a slight split there.

Now, in one state court, there was a decision that the financial institution was not immune, but in that case it was seen that there was an appearance that the bank was acting maliciously against its customer and was basically trying to file a retaliatory SAR, and it didn't do so in good faith in the findings of the court.

So there's a slight range in how this works, but in general, I would estimate the Safe Harbor Provision must be working pretty well because since 1996, over six million suspicious activity reports have been filed. And this year alone 600,000 have been filed, and it's growing every year. So one of the problems the regulators are dealing with is too much information, rather than less, and I think that suggests the Safe Harbor must be working pretty well.

Now, if we look at the Park – Cantley, Park Financial case, considering what would be reported, what did they do wrong, you'd have to consider the last catch-all element of the duty to report, whether a transaction is conducted for no business or apparent lawful purpose.

Now, if Park and Cantley were looking at the situation, they would have to ask themselves what would be the business or lawful purpose for a CEO not named on the account to be trading in his own company stock? What would be the reason for a British Virgin Island corporation to open an account in the first place, particularly, when it's only trading in one stock.

So you might think with those two warning signs that might be enough to trigger a suspicious activity report. Certainly, that's what the SEC expects. What happened to Park was a $30,000 disgorgement of profits, $50,000 in penalties, an official censure, and Cantley faced a two-year broker dealer bar, $8,000 in disgorgement and $25,000 in penalties.

Now, the Pettus case, I'll only mention briefly in the interest of time, but this is a similar case where the conduct was not recognizing suspicious activity and, in fact, obscuring it so the institution could not adequately identify and detect the activity.

And so here the stock exchange is taking action against Pettus because he's basically interfering with the ability of the financial institution to detect suspicious activity, which they believe should have been reported.

Now, it's good to know in these days, where the emphasis is on antiterrorism in the anti-money laundering area, what countries are particularly problem countries. The Treasury Department, through the financial crimes enforcement network, puts out useful guidance in press releases that you can see on their Web site, and two examples of these are cited here. They have to do with the jurisdiction of Cyprus and the jurisdiction of Iran.

Now, transactions involving these jurisdictions could almost on their own perhaps be a factor in considering whether the transaction is suspicious. The Treasury has said in Cyprus, particularly northern Cyprus or what's the area controlled by Turkish Cypriots, there's not adequate oversight of the banking industry there, and the banks in this region tend to operate through third countries, trying to conceal their involvement in transactions.

Similarly, in Iran, almost the entire banking sector has been listed as a problem by the Treasury in terms of money laundering risks, and if you go to the FinCEN Web site you can get a list of institutions that are viewed as institutions that raise risks and could perhaps lead to the filing of a suspicious activity report.

And these are examples of other Treasury guidance or FinCEN guidance on what types of things are suspicious and how to file suspicious activity reports. One of the things that the Treasury was finding is that the financial institutions who file these reports sometimes don't complete the narrative that explains why they're filing the report or what they find suspicious and describing the supporting documents. It's important to, as the FinCEN says, provide complete and accurate information about why you're making the filing or you may not be found to be in compliance, the filing could be disregarded, and the penalties could be imposed.

Now, one of the issues identified at the end, there could be a situation when law enforcement would request that you keep an account open even though suspicious activity has occurred so you can help law enforcement further investigate.

Now, even FinCEN, who itself is law enforcement, suggests that if this occurs and you decide to follow the request, you get the request in writing, because if you don't and it's later – occurred to another agency that this account was suspicious and why was it not closed, if you don't have it in writing, your institution could have problems for keeping the account open.

Now, another jurisdiction that has a problem with terrorism or is a jurisdiction with a problem in foreign relations is North Korea. Banco Delta Asia was found to have been giving access to North Korea to the international banking system. So similar to Iran and Northern Cyprus, this institution was acting as a straw man or an intermediary.

And so if you're conducting transactions internationally or doing banking or financial dealings internationally, it's really important to watch for transactions that are tied directly or indirectly to Iran, North Korea and Northern Cyprus, in particular.

Now, there is a particular issue that illustrates the complex – complexities involved in money laundering compliance. Often the financial institutions interact with one another and have to rely on one another to perform different roles in terms of knowing customers, identifying customers and detecting suspicious activity.

This slide is an example where a U.S. clearing institution partners with a foreign introducing broker, and so the foreign broker gets the customers who want to trade through the U.S. clearinghouse, and the request was made to FinCEN to clarify what are the compliance

obligations of the clearing house? Does the clearing house have to know the customers of the introducing broker?

And FinCEN's reply was that the clearing house doesn't have to treat the broker's customers as its own, but the clearing house does have to do due diligence on the foreign broker itself, and verify the identity of the foreign broker, and take a risk-based approach to whatever else it may do in the anti-money laundering area, and also to file suspicious activity reports based on whatever information may become known to the clearing house, recognizing that the clearing house may not know everything about who is the customer and why the customer is conducting certain types of activity.

Now, with that, I'll turn it over to Bill Gordon. I imagine that some of you, if you've heard this presentation for the first time or many of you, if you've been involved in this area for awhile, experienced the Bank Secrecy Act as a particularly cumbersome type of regulation, and may even wonder is there a way to engage a third party perhaps a specialist to carry out the compliance function?

And so we're going to talk about the option of outsourcing compliance with the Bank Secrecy Act. Bill?

Bill Gordon: Thank you, very much, Owen. And so what I'm going to talk about for a few minutes here is what is business process outsourcing in the anti-money laundering sense, and why would we do it?

As you can imagine, in recent years lots of firms, both in the financial and other industries have turned to outsourcing to save money. Financial institutions with anti-money laundering in particular are no exception.

When a firm decides to look at outsourcing their AML compliance, one of the things that they're probably thinking of is saving money. AML compliance is very costly. Firms that specialize in AML compliance, whether it's the financial institutions themselves or specialized AML compliance monitors have very expensive software that they use to track suspicious activities.

Smaller firms may feel that this software and this process is not cost efficient for them, and therefore like other firms that decide to go to outsourcing they will outsource their AML compliance. Now, this raises many questions and problems for these firms.

Regardless of whether a firm decides to outsource its AML compliance, for the most part, it is still responsible for ensuring that compliance. There's only one exception to this, and that's the customer identification program requirements. The customer identification program requirements, as you can imagine, are the requirements of institutions before opening an account to verify who an individual or institution is that's opened the account.

The Treasury Department has outlined very specific ways in which if the CIP requirements are outsourced, the institution itself will find itself in a safe harbor and will not be in trouble if the third party messes up in its CIP compliance.

That being said, however, every other form of AML compliance remains the risk of the institution. Therefore, even if an institution decides that they are going to outsource their AML compliance programs they're going to need to be very vigilant with their third-party monitor in checking to make sure that that third party is doing a good job because if that party does not do their job, if they miss things, and the financial institution is notified by the government, the government can and will go after the financial institution in the first sense.

Now, another issue regarding AML outsourcing is the technical problems that outsourcing third-party financial monitoring can have on institutions, what I mean by that is a financial institution or

any institution that falls under the umbrella of needing to comply with AML rules most likely knows their customers and their transactions better than any third party can.

So, as an example, a small community bank may understand the transactions of its customers better than a compliance monitor in Arkansas or India can. So one of the issues that outsourcing – which we find in outsourcing is the exchange in information.

Now, this information can either be too small or too great, and either one can cause problems. Therefore, it's very, very important if an institution decides to go to outsourcing that they have a way to monitor their third-party compliance monitors.

Now, as I mentioned briefly before, the financial institution itself retains the obligation to comply with any money laundering obligations. Therefore, even if a third-party source identifies a suspicious activity, the third-party source is supposed to notify the institution, and the filer of the SAR needs to be or should be an employee of that institution.

So in a sense before an SAR is filed it is possible that an employee can look and say, "OK, this is what I have been notified of," and can then go back and make a decision about whether an SAR is required.

Now, the other extreme of that is not so simple. Say, for example, a third-party monitor fails to identify something that is suspicious? Most likely the institution is going to have no real way of tracking those charges or tracking those transactions since the points of AML outsourcing is to allow the third party to take care of that monitoring. So that is a very significant risk that anyone considering outsourcing of AML compliance needs to consider.

Now, if someone does consider outsourcing their AML requirements, there are some things that the institution will need to consider. The first is data privacy. As you can imagine, it's necessary to ensure that any sensitive and confidential information is properly handled. Institutions that fall under the umbrella of the AML requirements do handle sensitive information, and the great majority of that information is – has no illegal part to it, whatsoever.

And the owners of that information would understandably be very upset if a third party is not as sensitive and does not maintain confidentiality in the same way that your local institution would. And if that happens, it is probable that in the long run that institution would lose business.

We also need to define the scope of the contract. What of the parameters of the services to be outsourced? AML outsourcing does not have to be a one size fits all. Institutions can outsource totally the CIP requirements, which grants them a safe harbor, if the third party were to mess up, or it can go all the way to outsource the entire AML compliance program.

It's obviously very important in any contract for this scope to be outlined.

Another important indicator or another important issue is performance indicators, such as how is a financial institution going to monitor the third party? Will there be targets that the recipient of the outsourced work needs to meet? And what happens if the goals are not met?

Owen Bonheimer: If I might mention, Bill, that looking back at the E*Trade and the Crowell, Weedon case that we looked at, the SEC was considering did the practices follow the policy, and did the policy describe the practices?

And so if you're monitoring the outsourced party to see what they're doing, that's especially important, because if they're not doing what you think they're doing then it could be found that your customer identification program policy statement is inaccurate, because you're not actually describing what's really going on.

Bill Gordon: And in that case the institution itself would get the primary blame laid on it, and so that is something that clearly everyone involved in AML outsourcing should try to avoid.

We also need to look at a transition plan, both when the contract is first going into effect and when the contract is ending. We need to have a plan in place for how the responsibilities will be transitioned between the outsourcer and the recipient of the work.

Oftentimes, due to complexities of AML compliance this can't be done in one day. There will most likely need to be training, and in the training sense we need to think about who is going to provide this training. Will the outsourcer train the recipient of the work on the specifics of that work?

Obviously, the institution itself is likely, as I noted before, in a position to be more knowledgeable of the ins and outs and the intricacies of its plan than any third-party source.

You'll also want a compliance certification program in place. You'll want the outsourcer to certify that they are complying with certain laws, certain relevant laws. Obviously, AML is one of them. The (SEPA) also comes to mind, and there's just a lot of intricate international laws that we really need to make sure that any institution and any third-party outsource works are thinking about.

Now, another thing we need to think about is changes in control. Are there plans in case the outsourcer needs to temporarily or permanently take back some level of control? I think we all can imagine a situation in which the outsourcer is just not doing its job properly, either their software isn't getting it right, the training hasn't been appropriate, or they're just not doing their job. The institution remains primary responsibility, and there needs to be a method of the institution taking back control.

Also, terminations, how will the contract end? Can it be terminated unilaterally by either party? Will compensation then be owing to either party?

And, finally, but maybe most importantly, audit rights. If the government comes in and investigates you, the institution, you're going to want to have the ability to go to a third party outsourcer or outsourcee and look at their books, see what they've done, see what their efforts were.

And with that, hopefully, we've saved enough time for a few questions.

Owen Bonheimer: And I see there is one question that asks is the clearing house in the last example before Bill started discussing outsourcing, is the clearing house a financial institution?

And for that we can go to the financial crimes and enforcement work ruling, the example we gave was from a ruling, FIN 2008 R008, and there the FinCEN treated the clearing house as a financial institution for purposes of the Bank Secrecy Act, but it also was interpreting a particular rule under the Bank Secrecy Act called the Correspondent Account Rule.

And so it was clarifying how the clearing firm had to treat the broker. And in some sense that arrangement could almost be thought of as outsourcing, where the clearing firm is, in essence, outsourcing the account opening function, and the customer identification procedures to the introducing broker.

And in that case, though, the particular arrangement between the two was formalized through an agreement and an understanding that was put in writing and had other features described in the release.

And based on that the FinCEN determines that what was being established was a correspondent account for the broker in the clearing firm, and because it was a correspondent account the

appropriate due diligence by the clearing firm was on the broker itself and not necessarily on the customers of the broker.

Now, I see there's another question here. I don't know if you can scroll up a little bit so I can see the…

Owen Bonheimer: Oh, Brennan, do you have that?

Brennan Holland: Yes, I've got the questions here. There are a couple. Which one are you…

Owen Bonheimer: (I'm)…

Brennan Holland: Let me – there's one question that has to do with compliance, and it asks in terms of compliance is it enough to say that an outsourcee must comply with all applicable laws or do the specific laws need to be stated?

And that would be a matter of contract law, I would imagine. If you've got a contract with an outsourcer you've got to be careful in any case that you have appropriate protections.

There are questions not only of liability and how the liability flows, and you can I guess mitigate some of that through – requiring bonds and that kind of thing, and making sure that your outsourcing vendor is solvent, but there may be safety and soundness concerns, as well. Can you guys just briefly address that?

Owen Bonheimer: Well, I think the outsourcer is best protected if the legal obligations and procedures are reduced to writing and very detailed to the extent that they're easily understood by the party doing the outsourcing.

If the responsibility for even identifying which laws are applicable is left to the outsource party, the outsourcee uses the term, then that creates some risk for the financial instituting if the – if there's not compliance or the outsourcee doesn't understand which laws are applicable then the financial institution could remain liable. So specifying the applicable laws and the applicable procedures I think would be preferable in the outsource contract.

Bill Gordon: And one of the problems remaining is that even in the contract, if everything is specified to a "T" and the third party still doesn't do his job properly, the institution is going to get blamed.

Owen Bonheimer: Yes, and you can imagine in these – you outsource and the third party is not conducting the work correctly, if there's not oversight then you could get like in the SEC case the government officials will come out and pronounce the case and relate the concerns they have to terrorism.

Even though in E*Trade and Crowell, Weedon there was no evidence that any of the people opening the account were engaged in any sort of terrorist activity, the enforcement officials tried and couched the actions in terms of antiterrorism policy, which has the effect of associating the financial institution on the wrong side of the fight against terrorism, which I think has reputational concerns, even if there's still a safe harbor from liability it creates reputational risk.

Brennan Holland: Absolutely. Well, gentlemen, we're going to have to wrap up here. We're at the top of the hour. But Owen and Bill, we appreciate very much your presentation today. And I'd like to thank Steptoe firm for sponsoring our webcast today.

Once again, let me remind you that the audio file for this webcast will be available on the ACC Web site for – about three hours from now and will be archived there.

And I'd like to thank you, all, for attending our webcast. If you have any remaining questions you can direct those to our speakers. I'm sure they'd be more than happy to answer e-mails, and their addresses are found in the bios, there on the left-hand side of your screen.

And also please don't forget to complete the survey to let us know what you think of this. And we would love suggestions, as well, on topics that would be interesting and relevant to your membership.

Our regular November meeting for the Financial Services Committee is going to be canceled – is canceled, but we are going to meet in December at – on December 10 at 3:00 pm Eastern. So we've rescheduled our December meeting to – so that it won't conflict with the Christmas holidays. And we look forward to having you participate in that then, and we thank you for joining us today. You may now log-off.

END