Information Sharing—Strengthening Our AML/CTF Program
Richard T. Wells, CAMS-FCI®
OUTLINE

Executive Summary

I. USA PATRIOT ACT Section 314 (a) & (b) Defined
   A. What is in it for me (Financial Institution)
   B. Financial Crimes Enforcement Network 314 registry
      1. Where do I go?
      2. How do I register?
      3. What can I share?
   C. The technical side of the information sharing program within an FI

II. Current state of information sharing within an FI
   A. Existence of Suspicious Activity Reports (SARs)
   B. Enterprise Solution to Narrow Regulation

III. The How
   A. How a Financial Institution Establishes and Maintains Information Sharing
   B. A Case Study

Conclusion
Executive Summary

The focus of this paper is to leverage the USA PATRIOT Act Section 314(a) and (b), and to improve the reader’s anti-money laundering/counter-terrorist financing (AML/CTF) program with a focus on the importance of not just building but maintaining relationships with law enforcement (LE) and regulators. The goal is to display the importance of information sharing between financial institutions (FIs), as well as between LE, regulators and FIs, specifically pertaining to financial intelligence in connection with money laundering and/or terrorist financing investigations. This will be accomplished by defining the USA PATRIOT Act Section 314(a) and (b) and by emphasizing what the current state is. A redacted case example that spanned two years and uncovered a large network of trade-based money laundering (TBML) and Black Market Peso Exchange (BMPE) will be showcased. The data and information gathering (research) of this white paper will be from the laws and regulations, as well as the professional organizations/groups that have written on this topic. It must be emphasized, to stay ahead of the illicit actors determined to infiltrate our financial systems and spread their crimes, we must continue to talk about current laws and regulations, and how the private sector is affected by those laws and regulations and come together to discuss how we can evolve the information sharing process. It cannot be stressed enough that we cannot stop the sharing of critical investigative information within the private sector, between the private and public sector, and we must discuss furthering the information sharing to reach outside of U.S. borders to thwart illicit actors from compromising our institutions.

Author Biography

A brief summary of the author’s relevant background includes a combined 23 years of military, LE and banking. The author was a subject-matter expert, trained and certified as an anti-terrorism instructor and was sent abroad to train other militaries in the history of terrorism, terrorism operations, hostage survival, base and home defense, and others. Following his service he became a LE officer and specialized in violent crimes. This provided years of experience at street level crimes, including, but not limited to, drugs, gangs, assaults, weapons offenses and others. Since joining the private sector, the author has worked in banking in the financial crimes profession, specifically focusing on AML/CTF. The author has extensive training and has logged numerous hours interviewing and interrogating through both formal training, as well as practical application, while with LE and to some degree with banking. The author has also gathered extensive evidence, prepared case work, and testified before grand juries, and state and federal level courts. The author has provided training within the FI along with IRS/DEA and local agencies. The author has an extensive portfolio of case work, both in terrorist financing investigations and money laundering investigations where the specified unlawful activities (SUA)s included, but were not limited to, Medicare/Medicaid fraud, other insurance fraud, bust-out schemes, Ponzi schemes, pyramid schemes, narcotics trafficking, weapons trafficking, human trafficking, hawala networks and unlawful internet gambling. Money laundering investigation typologies that the author has directly investigated with LE and other FIs include, but are not limited to, the BMPE, TBML, tax evasion and others. Not one of the author’s “significant cases” would have risen to the levels they did without the critical “information sharing” piece from other FIs and from LE.

USA PATRIOT ACT Section 314 (a) and (b) Defined

According to the Financial Crimes Enforcement Network (FinCEN):

“Section 314 helps law enforcement identify, disrupt, and prevent terrorist acts and money laundering activities by encouraging further cooperation among law enforcement, regulators, and financial institutions to share information regarding those suspected of being involved in terrorism or money laundering.”¹

“USA PATRIOT Act Section 314(a) requires the Secretary of the Treasury to adopt regulations to encourage regulatory and law enforcement authorities to share with financial institutions information regarding individuals, entities, and

organizations engaged in or reasonably suspected, based on credible evidence, of engaging in terrorist acts or money laundering activities.”

“USA PATRIOT Act Section 314(b) permits financial institutions, upon providing notice to the United States Department of the Treasury, to share information with one another in order to identify and report to the federal government activities that may involve money laundering or terrorist activity.”

What is in it for me (financial institution)?

When we think of environments that are isolated from the rest of the world, such as certain countries we are all too familiar with, we are left to only imagine the lack of understanding, lack of sharing, poverty, education and loneliness the citizens within those environments must go through and feel. We also have to think of businesses that have not opened their doors through communications with other businesses in their respective industries or even to its customers in a customer friendly sense. Have those countries or companies thrived? Do we hear about them or read about their successes? If it were not for the USA PATRIOT ACT and its Section 314 with regards to cooperative efforts to deter money laundering—encouragement of information sharing—would we as LE, regulators or FIs be sharing information to further aid in the thwarting of financial crimes, specifically money laundering and terrorist financing? Sometimes we need to take a step back and ask ourselves what is in the best interest of—not just our specific roles within the institutions we are employed—but what is in the best interest of our firms, our local governments, federal governments and our nation? What is in the best interest of the global economy? Most importantly, what is best for the social good?

We all are very aware of the devastating impact that terrorist financing has: murder (life [family, friends, co-workers and neighbors] taken by the hands of others), kidnapping, maiming (severe debilitating injuries), psychological traumas (fear, loneliness, anxiety), and the economic impact from extortion, bribery and corruption. The impact on our nations and the global economy from the laundering of ill-gotten gains can crush smaller nations, can impact large cities, counties, states and drive poverty, narcotics addictions, human trafficking, slavery (work related and sexual related), as well as elevate the wrong people to power. How do we strengthen the fight against terrorist financing and money laundering? The answer is right in front of us: through the proper and timely sharing of information pertinent to capture the most relevant facts we can to aid in the stand against the criminal underworld. This information sharing has to be done internally (i.e., within the firms/institutions we work both domestically and internationally, if applicable), between FIs (banks) and the non-bank financial institutions (e.g., casinos, money services businesses [MSBs], payment processors, dealers in precious metals, insurance companies and hedge funds), LE and regulators.

The United States’ 107th Congress signed Public Law 107-56 titled Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. A smaller, but very important, portion of this law, Section 314, helped design our current flow of information between LE, regulators and FIs. This is one of those “appropriate tools” congress was targeting. However, how it is being used is another story. Only recently has there been a greater number of FIs (banks and non-banks) using the tool to disrupt money laundering or to clear a case investigation as non-suspicious due to adequate information satisfying the institutions’ questions to transactions that may initially mimic typologies to money laundering. In addition, non-bank financial institutions (NBFIs) are gaining ground on registering with FinCEN to participate in the sharing of information pursuant to money laundering or terrorist financing investigations.

---

Very recent remarks by Stephanie Booker, FinCEN’s associate director for enforcement, were captured by FinCEN from the June 18, 2015 Bank Secrecy Act (BSA) Conference held in Las Vegas, Nevada:

“Over the last year, FinCEN has also seen an increase in information sharing between casinos and card clubs through the 314(b) program. The 314(b) program now includes 98 casinos and card clubs. Information sharing across financial institutions can play a critical role in helping these institutions achieve their BSA/AML goals. Casinos and card clubs that participate in 314(b) are able to communicate with other 314(b) participants, even if those other institutions are not other casinos.”

“The 314(b) program is a powerful tool for providing financial institutions with a more comprehensive view of potential money laundering or terrorist financing activity that involves multiple institutions. We strongly encourage all financial institutions to consider participation in the 314(b) program.”

**FinCEN 314(b) registry**

**Where do I go?**

FIs can go to [http://www.fincen.gov/statutes_regs/patriot/section314b.html](http://www.fincen.gov/statutes_regs/patriot/section314b.html) and review the requirements to register and the requirements to renew registration annually. This registration identifies a point of contact within your firm for other firms to connect with when the transactional flows begins with your firm or is received into your firm. This is also where you or your appointed analyst/investigator within your firm can go to verify the existence of a registry and the appropriate point of contact to respond to information sharing request(s) or to initiate information sharing request(s).

**How do I register?**

It is as simple as completing a half page form providing specific information for FinCEN such as the FI’s name, FI’s tax payer identification number, primary federal regulator, FI’s mailing address, contact name, contact title, email address of contact, telephone number of contact, and fax number of contact. The more involved part of registering is ensuring you have documented procedures and processes in place to ensure the information shared is secured, the information shared is within laws and regulations, and to ensure employees are trained on the importance of the sharing of information pursuant to money laundering or terrorist financing investigations and more specifically what to share.

**What can I share?**

Per FIN-2009-G002, FinCEN Guidance dated June 16, 2009, “Information related to SUAs (specified unlawful activities, [which includes an array of fraudulent and other criminal activities]) may be shared appropriately within the 314(b) safe harbor to the extent that the FI suspects that the transaction may involve the proceeds of one or more SUAs and the purpose of the permitted information sharing under the 314(b) rule is to identify and report activities that the FI ‘suspects may involve possible terrorist activity or money laundering.’” In essence, share the information that would help your FI make a

---


6 [http://www.fincen.gov/statutes_regs/patriot/section314b.html](http://www.fincen.gov/statutes_regs/patriot/section314b.html) FinCEN Section 314(b). Financial Institution Notification Form. Quick Links: Mandatory E-Filing FAQs; 314(a) Information Sharing List; 314(a) Facts and Figures; 314(b) Fact Sheet; 314(b) Registration Forms; Change Your Point of Contact 314(a)...

7 FinCEN: Notification for Purposes of Section 314(b) of the USA PATRIOT Act and 31 CFR 1010.540 (Form).

determination of whether the activity is potentially suspicious or not. This includes, but may not be limited to, customer information such as name, address, employment (source of funds), personal identifiers (which helps reverse search systems for data accuracy, as well as capture potential misstatements made by a customer at account opening or during the relationship), transactions associated with the flow of funds to or from the asking institution, and source of funds or use of funds for those transactions (typically capturing routines or potential patterns that may be related to the red flags of money laundering or terrorist financing as defined by the BSA Exam Manual Appendix F).9

The Technical Side of the Information Sharing Program within an FI

Establishing appropriate processes and procedures with regards to the sharing of information pursuant to the USA PATRIOT Act Section 314 (a) and (b) is critical within your FI. Within those procedures, clear steps should be documented on the handling, documenting and secure storing of the information both as a receiver and a sender. In addition, periodic training should be provided to analyst/investigators that are responsible for the information sharing process. Emphasizing the importance of sharing that information for both sides of that call or correspondence in order to be able to document and form a fact based opinion off the relevant transactional and customer information data shared.

Information Sharing within a Financial Institution—Cross Borders

USA PATRIOT Act Section 314(b) targets information sharing between FIs within the U.S.’ jurisdictional control and provides safe harbor to those firms as long as they do so in good faith of money laundering or terrorist financing investigations. However, as the world has become globally connected, the law, regulations and guidance provided by FinCEN do not permit a single FI to share critical SAR filing information between the U.S. entities of its company and its foreign counterparts or subsidiaries. It has been proven time and time again, that SAR information is critical to LE. That same information is critically important for a FI to share across borders within the confines of a tightly controlled environment in order for compliance officers in neighboring or cross ocean jurisdictions to conduct a full and thorough investigation on those parties involved in the U.S. SAR or counterparties in their respective jurisdictions that are part of the transactional flow for the money laundering or terrorist financing investigation to play out.

Existence of SARs

In March of 2009, FinCEN provided guidance for information sharing regarding SAR information and the existence of a SAR within a FI and across its affiliates within the boundaries of the U.S. This was and is critical for FIs to affectively monitor and report money laundering and aid in the reduction of money laundering and terrorist financing risks to those firms. In addition, it was acknowledged that coordination with international financial intelligence units (FIUs) was being done to discuss and work with the complex issues of being able to share that same information across international borders.10

Enterprise Effort to Broaden a Narrow Regulation

It would be ideal for U.S. FIs to share SAR information within its own firm, to include its affiliates or subsidiaries, across international borders with the compliance teams in the respective international jurisdictions. For the most part it is widely known that firms place weight (or additional scoring for varying risk indicators) on SARs pertaining to a customer and its account(s). This scoring not only impacts system generated events or alerts that lead to cases, but also impacts analyst/investigators decision-making process on whether to file a SAR, subsequent or continuing activity type SARs, and when weighing the compliance risks posed to the firm that are captured in those SARs.

---

A solution for U.S. FIs is to be able to share that critical SAR information across its borders when the FI has appropriate processes and controls in place to tightly manage the confidentiality around the SAR and SAR data. This will aid compliance and risk officers in the respective foreign regions to weigh-in on the global relationship with the customer or weigh-in on the domestic relationship with the customer that poses higher risk due to the customer’s transactional originators and/or beneficiaries. In other words, who their customer is doing business with. This will also allow for better compliance risk management controls by tracking potential money laundering or terrorist financing typologies across international borders. If a SAR or suspicious transaction report (STR) is warranted within the international respective jurisdiction as a result of information learned from cross-border U.S. SAR information, the local jurisdictions may gain transparency sooner rather than later. This will also help the Egmont Group’s efforts in its information sharing program with the respective international FIUs.\(^1\)

The current laws and regulations are somewhat ambiguous to the defining of the sharing of information within a single FI across boundaries. More clear guidance and additional governmental leverage to define or re-define the information sharing need across boundaries would greatly enhance the private and public sectors’ fight against money laundering and terrorist financing. This would also prove extremely valuable for the timeliness of that information sharing by getting it into the respective LE’s hands to aid in their investigations.

In 1999, the U.S. Attorney’s Bulletin dedicated to money laundering enforcement efforts covered an interview with Gerald E. McDowell. McDowell stated, “We recognize that the gathering and coordinated sharing of investigative information is a critical component to money laundering cases. Information is currently kept too compartmentalized. We need to improve information sharing efforts.”\(^12\)

Advancing forward, the 2001 USA PATRIOT Act was signed into law and provided the U.S. government (LE and regulators) the ability to share information with FIs and for FIs to share information with each other—all pursuant to money laundering or terrorist financing investigations. In 2003 and 2004, John J. Byrne testified before the House Financial Services Subcommittee for the American Bankers Association (ABA).\(^13\) This testimony proved valuable to the industry, for both the government and private sectors. The testimony sought a number of improvements—of particular was the improvement of the 314(a) process on behalf of the government, as well as the information sharing from the government to the private sector with regards to SAR guidance. The testimony in 2004 proved the growth of the relationship between the private sector and the government and helped hone the 314(a) process to what it is today.

As of April 2015, FinCEN published the FinCEN's 314(a) Fact Sheet, which provides LE, regulators and the private sector specific data as a result of the 314(a) program.\(^14\) However, the 314(b) program (encouragement of information sharing between FIs)
could use more specific efforts within the private sector using the government sector as a mediator in helping each other understand our roles and responsibilities to create an overall stronger process to the program.

It is widely known and clearly obvious to the regulated communities (FIs and governmental bodies) that neither money laundering nor terrorist financing is done in a vacuum. To be successful at the placement, layering and integration phases of money laundering, launderers must set up cross-border networks that infiltrate FIs and exploit the very nature of their existence. If launderers move across borders freely, sharing critical information with each other to impact the volume and speed at which they launder funds, then why do we not move closer to closing in on them? Why do we not allow U.S. FIs to share critical SAR information with their international counterparts? It is believed the efforts taken on by ABA may be needed once again, like what was done in 2004—and that is to encourage our government to move in an even more transparent (although still controlled) way by working towards permitting U.S. firms to share that SAR with their compliance counterparts across borders.

Dennis Lormel, retired FBI agent and a foremost expert on money laundering and terrorist financing, summed it up nicely in the conclusion piece of his 2011 paper titled “Perspectives, Partnerships and Innovation.”

“Since the bad guys are not constrained by boundaries when it comes to fraud and money laundering, it’s incumbent that law enforcement and the financial services sector share the responsibility to contain and disrupt their criminal activity. The more proactive and coordinated law enforcement and industry are the more likely they are to deter the bad guys. The combination of perspectives, partnerships and innovation would provide the framework needed to stem the tide of fraud and money laundering.”

A model conceptualizing information sharing being at the central focal point for statutes, regulation and enforcement action.

The How: How a Financial Institution Establishes and Maintains Information Sharing (Communication) with Law Enforcement, Other Financial Institutions and Regulators (the Non-Technical Side)

Any reputable business, whether private or public, will tell you that the number one reason they are successful is because of their people. Not the product, not the inventions, but the people behind it all. From the customer service representative on the phone to the front facing sales person all the way up to the leadership. Without strong, committed and flexible people, the products, services and ideas will not move forward. There is no difference with regards to the importance of producing

---

and selling goods and services to be a successful and profitable company with the importance of gathering and sharing critical investigative information to thwart money laundering and terrorist financing. How do we decide to participate in the “encouragement of information sharing” portion of the USA PATRIOT Act is up to us. Each FI is provided with the flexibility of information sharing pursuant to the investigation of potential money laundering or terrorist financing. How is your FI participating in that powerful law? Do they have a central point of contact transferring/transcribing that information or do they allow analyst/investigators to have direct communication with other analyst/investigators on the receiving or sending end of a 314(b) request? Do they allow AML/CTF or financial crimes analyst/investigators to speak direction with LE during the course of both the internal (FI) and external (LE) investigation?

It can be argued that if the emphasis was placed in the USA PATRIOT Act encouraging the sharing of information, it would seem to be the right thing to do for the social good. So, how do we go about implementing or improving our information sharing program within our FIs? The first step would be to research www.FinCEN.gov and the USA PATRIOT Act. Secondly get out and talk about it. Yes, get out and talk to other FIs whether by picking up the phone or attending conferences. Ask the questions: How do you share? What do you share? When do you share critical potential money laundering or terrorist financing investigative information with other FIs or with LE? Ask your regulators and LE and do not forget to look internally to ask persons within your own organization.

**A Case Study: (One Business/One Individual) Grew to Over 40 Entities (Businesses and Individuals) and Spanned the Globe (TBML uncovered by 314 (a) and subsequent 314 (b)**

A 314(a) request is initiated by LE (two federal agencies working together). FinCEN sends their 314(a) lists to FIs. Multiple FIs respond with their respective “yes” or “no” for the entities these two agencies are investigating for alleged money laundering. One FI’s process involving all incoming LE requests is to initiate a case investigation by entering LE requests into their internal systems, which triggers an event that processes and pulls all pertinent data through their automated systems. As data compiles, the entities (x2) create a case each (one for the business and one for the individual). It is also the FI’s process to initiate contact with the requesting agency/agent that is listed as the point of contact for a particular 314(a) request, as well as Grand Jury Subpoena’s, and other forms of contact by LE.

Though the case management system built two separate cases, the investigators (internal financial crimes analysts) realize the cases are related due to know your customer (KYC) data on file. The individual is the business’ authorized signer, point of contact and president of the company. A prior SAR was already filed on the business entity that was opened with the FI in South Carolina; however, the report showed an incorporation filing in Michigan. The investigators decide to merge the cases together and work as a single case. They engage LE. LE appreciates the call; however, as often encountered between initial conversations between FIs and LE, an initial reluctance to share information found mostly because of the unknowns (lack of initial trust with regards to “who is on the other line.”)

As the case investigation progresses both on the LE side and on the FI side, additional calls are made and LE becomes very appreciative of the diligence that the FI investigator is taking to stay in contact and provide additional information through SARs that the LE did not have. The FI’s case grows as they begin looking closer at the rapid movement of funds passing through the business. The business entity is receiving large even dollar checks through the remote deposit system and is rapidly being moved out of the account, first as large even dollar checks clearing in South America jurisdictions and then migrating to large even dollar wire transfers to South America and Asia.

The FI takes a closer look at the initial filing and who initially funded the account. A couple of businesses stood out and subsequent 314(b)’s were sent to the respective U.S. FIs that housed their relationships. It was uncovered that a couple large even dollar checks that were sent by the other businesses were, in fact, owned by the same individual that owned the business with this current FI. All with different names, different industry types and incorporated in different states. Furthermore, it was found that those businesses closed their relationship with those FIs within nine to 18 months of opening the relationship with the FIs.
As additional SARs were filed, each SAR warranted a call with the original LE that initiated the 314(a) and the ongoing investigation. The LE agent and the FI investigator began sharing more information “real time” as soon as a new case popped up and new SARs were being filed. The LE also engaged more freely when new leads came their way. This proved very beneficial as the FI was uncovering a web of existing and closed relationships with the initial entity; however, the money trail was getting more complex to follow as most of it was leaving U.S. jurisdiction; thus, not allowing the sharing of information internationally through the FIs.

During the course of the investigation, the initial FI customer (target of LE’s investigation) closed the individual and business account. Trail stops. Transaction outflows are going overseas leaving no U.S. bank to lead LE too. LE catches a break a few months later as a result of an illegal entry into the country by the alleged money launderer’s girlfriend. LE learns she was sent in to open a business in her name. Bingo—the girlfriend to the initial 314(a) target and her business are with the FI, which was opened in California. The trail picks back up. Same typology, checks in wires out; however, this time a significant transaction was captured between the girlfriend’s new business and a business relationship in Florida, which also happens to be with the same FI.

As the FI looks into this Florida business it uncovered that multiple SARs have been filed on it and it connected it to other businesses in Florida that are also with the FI. The web of businesses and individuals and their respective accounts grow substantially. Additional 314(b)s are initiated to share the information with other financial institutions, as well as to gather data on the transactions that are sent to them or received by them involving these businesses, which now appear to be shell companies as the transactions are clearly outlining unrelated industries.

LE receives the additional SARs, looks into the relationship in Florida and relays back to the FI that this is the break they needed. The Florida entity that all transactions are now pointing to seems to be the hub point for the money laundering that is originating out of South America. LE initiates multiple account seizures and conducts simultaneous search warrants on the business’ and individuals locations. LE relays back to the FI that received a full confession from the Florida entity (an accountant by trade and supposed lawyer from South America), which confessed to a complex money laundering ring that was moving money for a South America FI that was allegedly laundering for a Columbian drug cartel.

In the end, through the extensive information sharing that was initiated by a single 314(a), followed by multiple case investigations that resulted in connecting prior SAR filings, the creation of new SAR filings, the building and maintaining of the relationships between the LE and the FI, and the FI initiating multiple 314(b)’s to other FIs, a complex money laundering network was brought down. Within the one FI, over 40 entities (individuals and businesses) were found to be set up as front companies for the laundering of funds from South America. The typology also consisted of sending those funds to Asia after a series of checks and wires passed through the U.S. accounts to purchase goods from Asia to be allegedly sold in South America on the black market, which allegedly returned the funds in pesos to a Columbian drug cartel (also known as the BMPE).

Upon hearing LE’s success, the FI terminated over 40 relationships and closed over 60 accounts. The FI debriefed extensively and learned that connecting the relationships and accounts would not have been possible without the cooperative information sharing between LE and the FI’s financial crimes unit, and between the FI and other FIs that received or sent some of those transactions through the 314(b) process. The information sharing in this case brought justice to those involved within the U.S., and further work was initiated between U.S. authorities and foreign counterparts. The FI mitigated significant risks, as well. If the process and procedures were not in place to participate, train, document and safely maintain the confidentiality around the information received and provided to both LE and other FIs, the firm may still be carrying those relationships and accounts, and the laundering of illicit proceeds may have gone on for quite some time.

Conclusion

The intent of this paper was to provide the reader with some background to laws and regulations that protect FIs when it pertains to the sharing of critical investigative information, whether that information is shared between financial institutions
in the private sector or with LE and regulators. The reader was walked through Sections 314(a) and (b) of the USA PATRIOT Act, how to register with FinCEN, the technical side of the information sharing process and most importantly what, how and why to share information with regards to money laundering and terrorist financing investigations. A subject-matter expert in the field of terrorist financing and other white-collar crimes that also involve money laundering stated:

“When financial institutions participate in Section 314(b) information sharing, they have an opportunity to obtain information regarding customers who pose concerns to them. It enables them to go back in the direction of the source of funds and get closer to the origin and to go forward to the use, and get closer to the point of distribution. This information, which is provided by other participating financial institutions, can assist in making decisions to file suspicious activity reports (SARs). It will also provide better details to include in SAR narratives. Better quality SARs provides law enforcement with better opportunity to develop investigative evidence.”

In his 2012 paper, that same author pulled a direct quote from the then FinCEN Director James H. Fries, Jr: “The more information bankers and brokers can share the more the integrity of our financial system will be protected and law enforcement can gain additional sources of valuable information.”

---
