June 28, 2017

Testimony of

Lloyd DeVaux

On behalf of the

Florida Bankers Association

before the

House Financial Services Committee

Subcommittee on Financial Institutions and Consumer Credit

United States House of Representatives

Testimony of Lloyd DeVaux

On behalf of the

Florida Bankers Association

before the

House Financial Services Committee

Subcommittee on Financial Institutions and Consumer Credit

United States House of Representatives

June 28, 2017

Chairman Luetkemeyer, Ranking Member Clay and members of the subcommittee, my name is Lloyd DeVaux. I am President & CEO of Sunstate Bank, which is a community bank founded in 1999 based in South Florida. My bank has $200 million in assets with three locations in Miami-Dade County.

I appreciate the opportunity to be here today to present the views of the Florida Bankers Association regarding the challenges and burdens the industry faces in complying with the demands of the Bank Secrecy Act (BSA).

Sunstate Bank has 45 employees and focuses on the needs of small businesses, consumers, real estate investors, and non-resident aliens in the communities we serve. We have approximately 3,000 business and retail deposit accounts, including demand, money market, savings and certificates of deposits, and approximately 300 loans. We also offer safekeeping services to foreigners.

As a community bank, we have seen an influx of *new* regulations over the past few years as well as *additional* requirements under *old* regulations such as the Bank Secrecy Act. Clearly, BSA compliance is an important building block for our national security, but it is founded on principles that were developed nearly 50 years ago. The world has drastically changed since the BSA was adopted in 1970; criminals keep evolving and staying one step ahead of banks and law enforcement. As the United States takes steps to combat terrorism and financial crime, now would be a good time to update the compliance requirements to develop a system suited to the twenty-first century.

In late 2013, to ensure that the bank had a robust BSA/Anti-Money Laundering (AML) compliance program, the board of Sunstate Bank made the decision to seek new management and I was hired in July, 2014. Over the next 18 months, we strengthened our BSA/AML program in all phases, including system enhancements, new policies and procedures, additional staffing, and extensive training. At the beginning of the process, to ensure that the bank was proceeding in the right direction, a significant portion of the bank's efforts involved hiring outside consultants—at annualized rates of $110,000 to $185,000 per year per consultant.

The resources devoted to compliance, especially BSA compliance, are significant for a bank of our size. Sunstate Bank employs seven people to manage its compliance program, including six full-time employees in BSA/AML and one in consumer compliance. This represents 15.5% of total staffing of 45 people, and the BSA/AML staff includes both a BSA/AML Officer and deputy BSA/AML officer. This represents a 100% increase in staffing over 2012 levels, even though the Bank has not changed significantly in size and number of customers. However, it underscores the fact that BSA compliance efforts represent a significant use of bank resources, in time, money and human capital.

Our experience is not unique. In 2007, 86% of Florida banks had five or less BSA/AML employees. Now only 62% have five or less. BSA/AML staffing has increased for many banks. While some of this is due to acquisitions, much has been driven by regulatory pressure to add more resources to BSA/AML and the regulatory risk and concern over enforcement actions.

The added costs of BSA/AML compliance—on top of the significant costs from Dodd Frank—has been significant and has led to the disappearance of many smaller institutions in Florida. Small banks have found it difficult to survive on their own due to the current regulatory environment. Many have decided to sell or merge with a larger bank. This has impacted our communities because small banks do the highest percentage of lending to small businesses.

For example, since 2007, 173 banks have disappeared. More telling, is 111 of those disappeared after Dodd Frank was enacted—a consolidation of more than 50% of all Florida banks in just the last 7 years.

What is more important about the impact that the cost of compliance is having isn't in direct costs but rather how it affects our customers and our communities. In an informal survey

conducted by the Florida Bankers Association, 91% of the banks that responded said that BSA/AML regulation has caused them to avoid certain industries, decrease business development, and lower customer retention. Many industries that are legal businesses are labeled "high risk" by regulators. This means banks must collect more customer data, conduct more analysis, provide more oversight and monitoring, and engage in more site visits—all of which translates into higher costs for the bank and for the customer. The best option, in many cases, is to not bank certain industries and certain customers, and to ask existing customers to close their account(s). From the bank's perspective, it is a simple matter of cost/benefit analysis: the economics of compliance make it unprofitable to maintain certain accounts.

Most importantly, the costs and risks associated with compliance are driving some customers outside the banking industry. This creates opportunities for an underground economy or shadow banking system to serve their needs. That has serious drawbacks which must be considered by policy-makers. First, it makes no sense to create a system that drives legitimate customers outside the formal banking system to less regulated or even unregulated providers. Second, it creates a system and series of financial transactions that may not be reported or available to law enforcement. And third, it can create a shadow financial system that is readily available for criminals and terrorists.

Overview of the BSA Program

All BSA/AML Programs must adhere to four pillars. These pillars are: (1) a strong monitoring program, (2) a periodic third-party independent review, (3) a BSA Officer responsible for overseeing the program, and (4) an effective training program across the organization that is appropriately geared to the responsibilities of each individual. And, a new fifth pillar that imposes new expectations for Customer Due Diligence is now being enforced. Failure to comply with any of these pillars is a violation of law, and whether it is by error, neglect or malfeasance, a misstep can result in a Consent Order, monetary fines, and even arrest in some cases. Should that happen, it can cause damage to the reputation and financial strength of the organization, and possibly lead to the loss of the bank's charter.

Additionally, personal legal fees and fines incurred by officers and directors to defend a BSA/AML legal action against them cannot be paid by the institution or by the institution's insurance. With a renewed focus on personal liability, *even for actions outside a compliance officer's personal control*, the reluctance by individuals to take on compliance responsibilities is increasing. Already, the personnel costs for hiring a trained and competent compliance professional have been increasing, and more banks are reporting that it is difficult to find qualified individuals to serve that role.

As mentioned above, Sunstate Bank has six people just in BSA/AML—***the largest department in the bank***. We only have ***four*** full-time lenders. That means that we have fewer staff devoted to serving customers and making loans that benefit the community than we have devoted to compliance. This is not a recipe for success. BSA/AML expenses were more than 10% of total expenses for our bank in 2016. The more we spend on compliance and regulations, the less we have to spend on service for our communities. Every $100,000 spent on compliance translates to $1,000,000 less we can lend.

To understand how this impacts the bank, it would help if I describe BSA/AML compliance, starting with the opening of a new customer account. There are a number of major activities related to BSA/AML compliance for on-boarding and monitoring a customer. The easiest way to visualize this is by following the path of a customer through the process.

New Customer scenario

BSA/AML compliance starts the minute a new customer walks through the door. Once the bank has established the type and purpose of the account the customer wants to open, it is required to properly identify the customer. The Customer Identification Program (CIP) rule requires the bank to obtain the name, date of birth, address, and an identification number of the customer and then independently verify the customer's identity. In the current environment, we must go beyond using picture IDs such as passports and driver's license. To meet the expectations of bank examiners, CIP rules encourage "banks to review more than a single document to ensure that it has a reasonable belief that it knows the customer's true identity." Other forms of identification that may be used to supplement the picture ID, are Social Security card, birth certificate, utility bills, or mortgage statements.

Once the bank has properly identified the customer and verified the customer's identity, it is expected to determine the anticipated monthly activity in the account; where deposits will come from, and where the money will go. This includes the number of transactions, and the aggregate dollar amount, by each type of transaction (checks, wires, debit card usage, ACH, internal transfers, cash, etc.). According to the banking agencies, all this information is needed to set up the customer's expected risk profile in the monitoring system. Deviations from this profile will generate alerts on a daily, weekly, and monthly basis.

Based on a number of determinants such as country of residence or countries where business is conducted, type of business, dollar and transaction volumes, expected cash activity, etc., the customer is rated as high, medium or low risk. If a customer is determined to be high risk, the bank conducts a High Risk Review (HRR) every year. For customers that have very active accounts, when the dollar volume passing through an account exceeds $3.5 million annually, the customer must be visited at their office, in the country where the business is located, by the bank every 24 months; plus the customer has to provide updated financial statements. In 2016, the Bank had to perform 157 HRRs and 50 visitations. This effort is needed solely to comply with BSA expectations.

Another requirement when the bank opens a new account is to check the OFAC (Office of Financial Asset Control) database to ensure the customer is not on the OFAC sanctions list. It is important to understand that the list of individual and entities on the OFAC lists can change almost daily. For example, in 2016, my bank received updated OFAC database lists 73 times. In order to ensure the Bank remains in compliance with OFAC requirements, the bank runs all customers and accounts, including beneficial owners, through the OFAC database every evening during the nightly batch update. Additionally, an OFAC check is done anytime a customer sends or receives a wire or ACH; purchases a monetary instrument or visits the teller. ***Despite all of this matching activity, the bank did not have a single positive OFAC match in 2016.*** However, because there are penalties for conducting a transaction with someone on the OFAC list, it is important that the bank perform this constant check.

Once an account has been established, it is then monitored daily, weekly, and monthly to ensure that the activity matches the risk profile that was created for the customer at account opening. If the activity doesn't match the profile, the monitoring system generates alerts to be

reviewed and cleared by the BSA/AML department. These alerts have to be reviewed manually by a bank employee to determine if they are in line with the profile and the nature of the business. If there is a question about whether the activity is appropriate or within the expectations for that individual's profile, a case will be opened and a full investigation conducted. Most of the time, this investigation will require research by the bank and possibly additional supporting information from the customer. If the investigation is not able to clear the transaction, the case will then be flagged for further review to determine if a suspicious activity report (SAR) should be filed to alert law enforcement. Sunstate Bank processed 7,109 alerts in 2016; which resulted in only 15 SARs being filed.

Cash and monetary instrument activities are watched closely. All aggregate cash transactions on a customer's account, in and out of the bank, on a daily basis in excess of $10,000 are reported on a Currency Transaction Report (CTR). Repetitive cash activity between $3,000 and $10,000 that triggers an alert will be investigated for structuring (purposely trying to avoid the CTR filing limit). Finally, all cash for the purpose of purchasing a monetary instrument, such as official checks, money orders, and gift cards, are logged. All BSA records, including these logs, must be kept for five years after the account is closed.

While the concept of filing a CTR seems straightforward, it can be challenging. The Financial Crimes Enforcement Network (FinCEN) requires detailed information about the customer holding the account where the funds were deposited or withdrawn. In addition, since the person who conducted the transaction may not be the account-holder, the bank also is required to collect information, including occupation or profession, about that individual as well. Finally, the bank must also identify the person(s) on whose behalf the transaction is conducted. And, compounding the challenge facing the bank is that we are expected to aggregate transactions over the course of the day to identify instances where a customer might have made multiple deposits at different locations or through different channels.

The question is whether all this effort to report large cash transactions is particularly helpful. The past FinCEN Director, Jennifer Shasky Calvery, commented that law enforcement made use of approximately 65% of CTRs on file to identify additional suspects, accounts or assets during an investigation. That means that the efforts undertaken by banks to file that information is used for supplemental purposes, not to start an investigation. Second, it means that

nearly one-third of all the CTRs filed are never used. And yet, there have never been any efforts made to identify whether there is a common trend or basis associated with these unnecessary CTRs that would let banks stop filing useless CTRs.

In the Money Laundering Suppression Act of 1994, Congress directed the Secretary of the Treasury to reduce CTR filings by 30%. Despite efforts by FinCEN, that goal has never been achieved. There have been other unsuccessful attempts to eliminate needless reports. In 2006, Congress considered the Seasoned Customer CTR Exemption Act to let banks exempt customers when the cash transaction information was identified as having little or no value to law enforcement. And, even though similar bills have been introduced since then, that format for exempting customers has never been adopted. Meanwhile, the number of CTR filings continues to rise.

Even when the process is automated, it takes time to verify that the filing is correct and complete. Knowing that fully one-third of that effort is useless for law enforcement is frustrating to us as bankers. The CTR form was the original effort for tracking money and identifying possible criminal activity but since then, use of the Suspicious Activity Reporting regime has taken center stage. Despite other, more efficient efforts to detect criminal activity, the CTR format is still in place. For example, law enforcement has access to regular checks with banks through an information sharing mechanism under the USA PATRIOT Act, section 314(a). And finally, despite these new sources of information for law enforcement, the CTR filing threshold of $10,000 which is still being used in 2017 was set in 1970; today, that same amount adjusted for inflation would be more than $64,000 in today's dollars. And so even the threshold for CTR filings is outdated. The question is whether all the time, effort and resources used to file a CTR could be better allocated to identifying and reporting truly suspicious activities.

According to the banking agencies, "Suspicious activity reporting forms the cornerstone of the BSA reporting system." Investigations and SARs can be triggered for a number of reasons, such as alerts due to deviations from expected activity, cash activities, HRRs, negative news, subpoenas, OFAC, or 314a matches, and so forth. In 2016, the Bank filed a total of 29 SARs. A decision to file a SAR is taken very seriously, and is only done after a full investigation that leads to either a conclusive finding, the inability to understand the nature of the activity, or a lack

of cooperation from the customer. A decision of whether or not to close the account is also made anytime a SAR is filed.

What's important to understand is that it takes time, effort and resources to file a SAR – or to determine not to file one when our systems create an alert. Treasury and FinCEN recognized that it takes time to put together all this information to provide the detail that's required. As a result, the filing deadline for reporting suspicious activity is 30 days after a determination has been made that suspicious activity did occur. When no suspect can be identified, that timeline increases to 60 days. And, where there is ongoing activity that was reported in a previous SAR, the bank has up to 120 days to file a follow-up SAR. The industry definitely needs that amount of time to conduct the investigation and research to submit a package for law enforcement. However, it may be that the system developed nearly 25 years ago is inappropriate in today's world.

When the United States was evaluated by the Financial Action Task Force (FATF) last year, it pointed out that the time and thresholds for filing SARs were inappropriate and should be reconsidered. A bank can determine that an activity is inappropriate or inconsistent with a customer's usual pattern of activities, but law enforcement is far better equipped to conduct the analysis and research to determine whether an activity reported as suspicious is criminal or terrorism. It would be far more efficient if a bank were allowed to file a short SAR to report a transaction that made no sense or that couldn't be explained. Although this idea needs to be explored more carefully, instead of requiring a bank to do a full-blown investigation and analysis of the activity, requiring time, effort and resources that are outside a bank's activity as a bank, it would be more appropriate to file a brief alert with as much information as available to notify law enforcement that something suspicious has occurred. This would quickly call the suspicious transaction to the attention of law enforcement and then let law enforcement agents do exactly what they are trained and qualified to do. Bankers should not be serving as un-deputized law enforcement agents.

Another element of the current BSA compliance regime was added by the USA PATRIOT Act in 2001. Section 314 is designed to encourage information to be shared from banks to law enforcement, from law enforcement to banks, and from banks to other financial institutions. Unfortunately, only one element of the information sharing mechanism Congress

anticipated is operating as intended, and that's the request from law enforcement for possible matches of a named individual and a bank customer. The Bank receives a 314a list from FinCEN bi-weekly, plus special lists when FinCEN feels it is appropriate. This list includes people and entities of interest to FinCEN in relation to an investigation involving money laundering or terrorist financing. The Bank has to check their customer and wire transaction database against this list, and inform FinCEN of any matches. The Bank received 26 bi-weekly lists and 32 special lists in 2016, and did not have a single positive match.

The feedback from law enforcement, which has been explored, has never really attained the level of usefulness that it could. At one time, FinCEN published a regular *SAR Activity Review* that identified ways that law enforcement made use of BSA data in investigations and prosecutions, but even that minimal feedback has been discontinued. Periodically, FinCEN does offer guidance in the form of advisories that identify possible red flags which indicate suspicious activity in areas such as elder financial abuse, human trafficking or other criminal enterprises. However, there is far more potential for communication from law enforcement that would help banks focus efforts and resources in ways that would be more useful to law enforcement. The partnership between law enforcement and the private sector needs to be a two-way street to succeed.

Similarly, there is a provision in that same section that encourages banks to share information with each other, but the restrictions and red tape surrounding its use make it impractical. For more than 15 years, the industry has suggested ways to encourage information sharing about possible criminal activity between banks, such as creating a directory of contacts at other financial institutions. Sadly, these have never been fully explored.

Apart from the information sharing process, there is another BSA requirement that banks must follow which has affected foreign correspondent relationships. From time-to-time, the Bank receives a notice of any foreign jurisdiction, foreign financial institution or financial entity that has been added to or removed from another list called Special Measures under 311. These are entities or jurisdictions that have been identified as not compliant with FinCEN BSA/AML guidelines and which are therefore of primary money laundering concern. The bank is required to do a historical look- back and investigate any transactions to or from any entity or foreign jurisdiction on this list. As the requirements to meet expectations have increased in recent years,

it has had a noticeable impact on foreign correspondent relationships and more and more banks have been decreasing the number of foreign correspondent accounts they maintain, in some instances simply because the costs associated with maintaining and monitoring these accounts have steadily increased. As a result, it can be increasingly difficult to wire funds internationally.

We all recognize the need and importance to stop criminals and terrorists from abusing the United States financial system. The point, though, is that the current compliance regime is out of balance. It needs to be updated and brought into the twenty-first century.

In theory, a bank's approach to BSA/AML compliance is based on risk and the unique risk profile of the bank. That overall risk profile takes into account the bank's customer base, the products and services it offers, its market area, and its strategic plan. There is a lot of agreement that regulations should be applied based on risk, but it seems that is getting increasingly lost in the application of BSA/AML expectations. Community banks are less complex and therefore less risky and should be regulated as such.

We recognize that certain elements of a BSA/AML program do not vary from bank-to-bank. For example, CTRs, structuring, and monetary instrument rules are the same for all banks and that makes sense. If a $10,000 cash transaction is potential money laundering at a $2 trillion bank, it should be considered money laundering at a $200 million bank. However, the disparities arise when it comes to risk ratings as they are applied to an individual bank and its customers. As applied by examiners, something that is considered highly risky in a small institution would be irrelevant for a larger bank. For example, if a $200 million bank is monitoring the 10% of their customers that are deemed to be that bank's highest risk customers, those same customers would not even be on the radar of a $2 trillion bank that is monitoring its 10% highest risk customers. Their 10% highest risk customers are much larger than our 10% highest risk customers. This is frustrating community banks because we are chasing $5,000 transactions and large banks are chasing $500,000 transactions. We have customers complain all the time that small banks are asking questions that larger banks never ask. The problem is that the application of the risk assessment process needs to focus on the actual risk and not graded on some arbitrary bell-curve. We need to focus on real risks, not arbitrary risks depending on where someone opens an account.

Conclusion

No banker would ever suggest that fighting money laundering and terrorist financing are not important or that we don't need regulation. We are only asking that the regulation be practical and sensible. Gilbert and Sullivan once said, "Let the punishment fit the crime." In the BSA context, we need to apply resources wisely and efficiently to combat the crime.

Dodd Frank has caused harm to communities and customers because the rules are not applied based on risk. The USA Patriot Act has also put a big burden on banks; however, it is difficult for banks to even know what should be changed. Banks produce a lot of information for the regulators, but seldom get any feedback about how the information is used, what is effective or not effective, and who is arrested and or convicted. The users of the information should be the ones to assess the value of the information provided, and suggest changes that make sense. BSA is a little like looking for a needle in a haystack. If we can decrease the size of the haystack by doing less 'low-value' activities, and focus our resources on the things that produce the more meaningful results, we will be more effective at finding the bad guys; and at a lower cost. We urge this committee to help reduce the size of the BSA haystack by working with the banking industry and the regulators to address our concerns and to update the Bank Secrecy Act to relieve unnecessary burden from financial institutions and to make the process efficient, effective and up-to-date.