

**Testimony of Tracy Woodrow
Bank Secrecy Act Officer/Anti-Money Laundering Director
M&T Bank Corporation**

**Before the Committee on Banking, Housing, and Urban Affairs
Subcommittee on
National Security and International Trade and Finance**

*Combating Money Laundering and Other Forms of Illicit Finance: How
Criminal Organizations Launder Money and Innovative Techniques for
Fighting Them*

June 20, 2018

Chairman Sasse, Ranking Member Donnelly, and members of the Subcommittee, thank you for holding today's hearing to discuss the U.S. anti-money laundering and combating the financing of terrorism regime and its impact on the way U.S. banks employ technology to counter illicit financial activity. My name is Tracy Woodrow and I am a Senior Vice President, Bank Secrecy Act Officer and Anti-Money Laundering Director at M&T Bank. M&T Bank is a U.S. regional bank with approximately 780 domestic banking offices in eight states and the District of Columbia. Since 2013, I've overseen the bank's AML/CFT and sanctions compliance efforts. I also chair a working group at The Clearing House¹ that is analyzing the resources banks devote to AML/CFT and sanctions compliance. We are seeking to understand whether the current legal and regulatory regime is effectively addressing present-day illicit finance risks and enabling banks to use their resources to proactively identify illicit activity. I will present some of the findings from this working group during my testimony as well as some insights regarding the resources M&T devotes to such efforts.²

As M&T's BSA/AML Officer, I lead a team of over 300 professionals who are dedicated to the cause of detecting and deterring money laundering and terrorist financing, while ensuring that our customers can conduct transactions in a safe, secure and private manner. We use a variety of standard tools in this fight, including rules-based monitoring, customer screening, enhanced due diligence for higher risk customers, and tips sent to us from fellow bank employees. In addition, we are beginning to use more modern, innovative tools. For example, we are using flexible data analytics to understand emerging risks and patterns of similar suspicious behaviors across customer groups. In some cases, we are working directly with law enforcement to identify red flags that may indicate suspicious activity in the communities we serve and have achieved great success in cases where we have worked collaboratively with law enforcement to thwart criminal activity. We are also exploring the use of automation, artificial intelligence and shared utilities across financial institutions as tools which may allow us to better assess huge amounts of data and identify unusual financial transactions.

While we have achieved significant success in the fight against money laundering, which in some cases has led to the detection of illicit finance and ultimately criminal convictions, I believe that the financial industry can be even more effective. Increased

¹ The Clearing House is a banking association and payments company in the United States and is currently owned by 25 large commercial banks. The Association is a non-partisan advocacy organization dedicated to contributing quality research, analysis and data to the public policy debate.

² The Clearing House has conducted a survey of its members that is intended to provide an empirical basis upon which to assess current BSA/AML/OFAC requirements. TCH expects to release the results of that survey shortly.

effectiveness can be achieved if we are given the tools and flexibility to increase innovation, focus on the most serious risks and collaborate closely with law enforcement and peer institutions. Criminal actors who seek to use the U.S. financial system to do harm in our communities are well financed, highly motivated and agile. To effectively combat this threat, we must continue to evolve and strengthen our anti-money laundering regime. We must re-evaluate the expectations placed on financial institutions so that we do not inadvertently place a higher value on the ability to precisely and comprehensively document the evaluation of routine transactions than we place on the ability to provide meaningful information to law enforcement.

As you are aware, the Bank Secrecy Act was passed by Congress in 1970 and has been added to, but not significantly reformed, by the legislature since. The Act requires financial institutions to provide law enforcement with leads that are of a “high degree of usefulness”³ while also setting basic requirements for AML/CFT programs at financial institutions, including (i) the development of internal policies, procedures and controls; (ii) designation of a BSA or compliance officer; (iii) ongoing training requirements; and (iv) a robust audit or independent review function. The Act also introduced the requirement to file Currency Transaction Reports (“CTRs”) on cash transactions over \$10,000. Legislation enacted since the Bank Secrecy Act, including the USA PATRIOT Act, have added requirements to file reports on suspicious transactions (“SARs”), verify the identity of bank customers and to conduct enhanced due diligence on a subset of those customers—notably correspondent banks, private banking clients, foreign senior political officials and other customer categories that have been deemed higher risk. Most recently, the requirement to identify ultimate beneficial owners of legal entity customers has been added through regulation.

Criminal organizations move money through the financial system in many ways. They use all forms of finance including cash, ACH, wires, investments and trade finance — and now, even emerging technologies such as virtual currencies and person-to-person funds transmittal applications. They use shell companies to hide identities or to create the false impression of legitimate business activity. They use front companies and money mules to hide the real people behind the transactions. With so many varied and ever-changing techniques to move illicit funds, it is critical that financial institutions, law enforcement and banking regulators never become complacent or satisfied with yesterday’s methods of identifying this activity.

³ See 31 U.S.C. § 5311 which states that “[i]t is the purpose of this subchapter [the BSA] to require certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism.”

It is also important to ensure that financial institutions are using their compliance resources efficiently and effectively. Under the current regime, banks like M&T are required to perform extensive evaluations of customers and transactions. We are required to carefully document every aspect of these evaluations and to compile large amounts of supporting documentation, even where it is determined that no suspicious activity is present. This focus on documentation of that which is not suspicious results in a huge amount of resources devoted to satisfying the intense focus of our regulators to such matters, resources that could be used to further the mission of detecting illicit activity.

Each year M&T files thousands of SARs⁴ and tens of thousands of CTRs⁵. However, feedback from law enforcement regarding the quality or usefulness of these filings is rare. At my institution, we receive post-SAR filing follow up requests for information on a SAR (such as a subpoena or other legal process) from law enforcement about 5% of the time. Follow up on CTR filings almost never occurs. Results of a survey recently conducted by The Clearing House indicate that our experience is not unique. In discussions with some law enforcement agencies, it appears that the lack of consistent agency policy or legislative authorization makes law enforcement reluctant to provide feedback on SAR filings, possibly due to concerns about the confidential nature of SARs, and there is no official mechanism through which to provide feedback.⁶ Thus, it is difficult to know whether our filings provide law enforcement with leads that are of a “high degree of usefulness,” as required by the statute. Therefore, we are compelled to calibrate our monitoring systems to the only tangible data we have — our decision to file a SAR. As a result, we fine-tune our systems to reflect our own work product, rather than to reflect law enforcement’s priorities.

Let me give you an example of the resources M&T expends on its SAR filings. We use both automated and manual processes to monitor for suspicious activity, which trigger tens of thousands of alerts each year that are investigated further by AML compliance employees, who ultimately make a determination to either close out the alert or designate

⁴ In 2017, U.S. depository institutions such as banks, thrifts, savings and loans and credit unions alone filed 916,353 SARs. Many more were filed by non-bank financial institutions such as money services businesses, casinos and securities firms. See “SAR Stats,” available at: <https://www.fincen.gov/fcn/Reports/SARStats>. Accessed June 14, 2018.

⁵ From 2012-2014, the average number of CTRs received per year by FinCEN was 15,283,950. See FATF Anti-money laundering and counter-terrorist financing measures, Mutual Evaluation of the United States, December 2016, pg. 54; available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016>.

⁶ Disclosure of the existence of a SAR to unauthorized persons may result in criminal penalties. 31 U.S.C. §5322. While this prohibition should not apply to a communication between a bank that filed a SAR and law enforcement as they are both authorized persons, the strict nature of the SAR confidentiality rule leads some to err on the side of caution in the absence of explicit permission.

it as a case in need of further review. If an alert becomes a case, resources will then be devoted to investigating the case which, depending on the activity under investigation, could take anywhere from a few hours to a few weeks to conclude. Once an investigation is complete, we make a determination to either file a SAR or document our decision not to file a SAR. Of the thousands of cases we investigate, only 39% become SARs. However, each investigation must be meticulously documented to meet regulatory expectations. On average, an investigation consists of seven pages of narrative text and 50 attachments, which average 250-280 pages total, regardless of whether that investigation results in a SAR.⁷

This is why I believe it is essential for policymakers to reform the AML/CFT regime so that institutions are able to deploy resources more efficiently and improve efforts to provide useful information to law enforcement, national security and intelligence officials. This change should be founded on greater coordination and communication between the public and private sector. The U.S. Department of the Treasury should establish annual priorities for the regime, which could in turn form the basis for financial institution supervision and exams. Within this effort, it could also rationalize the broad reporting requirements implemented under the BSA, which would allow institutions to further tailor the resources they deploy to AML/CFT priorities. In addition, greater information sharing between law enforcement and financial institutions would allow institutions to calibrate their monitoring systems and to detect suspicious activity that is meaningful to law enforcement. Furthermore, institutions should have the legal and regulatory flexibility to explore innovative technological solutions to AML/CFT compliance, either individually or in concert with their peers. Finally, Congress should consider changes to beneficial ownership rules in order to facilitate more transparency and the collection of consistent data to prevent companies from obscuring their ownership, thereby providing them with the means to hide illicit proceeds. I will address each of these recommendations in the remainder of my testimony.

Treasury Should Set Priorities for, and Rationalize, the Regime

As I noted previously, The Clearing House recently surveyed its members to better understand the resources institutions are devoting to AML/CFT compliance in the United States. Of the 19 TCH members surveyed (with assets ranging from 50 billion to over 500 billion dollars), 17 institutions employ a total of over 14,000 individuals, with 14 institutions collectively spending nearly \$2.4 billion on AML/CFT compliance. With all of these resources invested in compliance, 18 institutions reported that they collectively

⁷ Attachments to an investigation may include copies of account statements, results of internet and database searches on the customer and transaction counterparties, secretary of state filings for legal entities and documents evidencing transaction reviews.

filed more than 640,000 SARs and 17 institutions indicated that they filed 5.2 million CTRs in 2017. Furthermore, a median of 14 respondents indicated some form of law enforcement contact (including subpoenas, national security letters or requests for SAR backup documentation) on only 4% of the SARs they filed in 2017, whereas 10 institutions reported hearing from law enforcement on roughly 0.44% of the CTRs they filed.

Institutions of all sizes are devoting substantial resources to AML/CFT compliance, yet, in the current regime, little feedback is provided to determine whether those efforts are useful or reflect law enforcement's priorities. Moreover, the absence of specific measures of effectiveness, has led some to focus on the auditability of procedures and level of documentation of decisions as an inexact proxy for effectiveness, which encourages financial institutions to invest heavily in activities that reduce criticism of records, rather than in activities aimed at identifying suspicious activity in innovative ways.

Furthermore, U.S. financial institutions often have more than one regulator examining their AML program, with each individual regulator having their own priorities and viewpoints. At M&T alone, we have five regulators that evaluate us for compliance with AML laws and regulations. This is why it is important for Treasury, working with law enforcement, to establish a process for prioritizing the matters investigated by financial institutions subject to the BSA. This prioritization effort would convene relevant public sector actors that are the end users of the BSA information financial institutions provide to the government—notably law enforcement, national security and intelligence officials, regulators and other stakeholders, with the resulting priorities forming the basis for AML/CFT examinations at covered institutions. Such a process would further encourage banks to devote resources to activities that proactively address regime priorities, rather than focusing their resources on proxies like auditability and documentation. It would also ensure greater AML exam consistency across financial institutions and amongst examining agencies. I understand that FinCEN, a division of the Treasury Department, has begun to have these discussions with relevant stakeholders, an effort that should be encouraged and expanded.

In addition, the Treasury Department, in consultation with law enforcement and the federal banking agencies, should conduct a review of the current BSA/AML reporting regime with the goal of de-prioritizing the investigation and reporting of activity of limited law enforcement or national security consequence to allow financial institutions to reallocate resources to higher value AML/CFT efforts. Analysis of how SAR data is actually used by law enforcement could lead to the streamlining and automation of data submissions, rather than the current highly manual and cumbersome reporting process for some types of suspicious activity. This review is possible because FinCEN has data that

banks do not have — namely, information as to what SARs are accessed by law enforcement and at what frequency. Such a review could also investigate how to modernize, tailor and clarify BSA reporting requirements while increasing law enforcement feedback within the system. For example, the review may find that provision of data to law enforcement in a streamlined format, rather than the narrative format required by the SAR form, may actually be more useful as law enforcement increasingly uses modern tools to “data mine” the SAR database, rather than performing manual SAR reviews. Thus, a data-driven review of SAR usefulness may both enable institutions to better calibrate their monitoring system to provide law enforcement with higher value information and provide that information in a more efficient and useful manner. Again, I understand that FinCEN is working on such an analysis and I hope that the results will be shared with a broad group of constituents so that meaningful and workable changes can be identified and implemented.

The Public and Private Sector Should Exchange More Information

As this hearing is meant to focus on barriers to successful illicit threat identification and mitigation, it is important to highlight that one of the greatest barriers to an effective regime is the lack of communication between the public and private sector—notably between law enforcement and financial institutions. I have already described how feedback from law enforcement with respect to SAR filings can help financial institutions to better target their transaction monitoring toward better identifying suspicious activity. Financial institutions can also use investigative data provided by law enforcement such as IP addresses, geographic locations, names of suspected foreign shell companies and other items to develop targeted leads on potential suspicious activity.

There are examples of this type of information sharing in the U.S., but the examples tend to be ad hoc and not consistently applied across financial institutions.⁸ For example, some law enforcement agencies and prosecutor’s offices have held industry outreach conferences with select banks to share high-level information from recent cases as examples of certain typologies of illicit finance. FinCEN has issued periodic Advisories to notify financial institutions of high-level red flags associated with some kinds of criminal activity. FinCEN has also recently embarked on an effort to share more detailed

⁸ The UK’s Joint Money Laundering and Intelligence Taskforce (JMLIT) and Canada’s Project Protect are two international examples of such efforts. For more information on JMLIT, Project Protect and other public-private sector information sharing partnerships, see Nick J Maxwell and David Artingstall, *The Role of Financial Information-Sharing Partnerships in the Disruption of Financial Crime*, Occasional Paper, Royal United Services Institute for Defence and Security Studies, October 2017, available at rusi.org/sites/default/files/201710_rusi_the_role_of_fisps_in_the_disruption_of_crime_maxwell_aringstall_web_2.pdf.

information with some banks in the U.S., through a program called “FinCEN Exchange.” In addition, law enforcement agencies can seek information regarding specific AML/CFT suspects through the USA PATRIOT Act’s 314(a) provisions and other legal means. However, there remains a need for greater and more routine sharing and collaboration between the industry and law enforcement to better address the illicit finance risks facing our country. More routine sharing of specific and actionable information to a broader set of financial institutions could improve the effectiveness of the entire regime. Expansion of 314(a) to allow broader secure and confidential sharing with participant banks, which should be able to voluntarily participate based upon their risk profile and individual circumstances, would facilitate this communication.

Financial Institutions Should have the Flexibility to Adopt Innovative Technologies

In addition to setting AML/CFT priorities, rationalizing regulatory requirements, and improving public-private sector information sharing, it is important for institutions of all sizes to be able to embrace the innovative technologies available to them to better detect and report on suspicious activity. We must be cognizant of the fact that money laundering happens at banks of all sizes with differing levels of resources and sophistication. We also know that illicit finance often moves between multiple financial institutions as criminal actors work to complicate and conceal the money trail. Therefore any effort to encourage technological innovation within the industry should be flexible enough for institutions of all sizes to investigate them further — whether through a shared utility model or as an individual investor.

Congress should explore whether expansion of the “safe harbor” language within Section 314(b) of the USA PATRIOT Act, which presently provides a legal pathway for financial institutions to share information on potential money laundering or terrorist financing investigations with each other in certain circumstances, could facilitate these efforts.⁹ Explicitly allowing banks to share information with each other under 314(b) for the purpose of working to detect potential suspicious activity would help to ensure that such efforts do not encounter legal or regulatory hurdles to innovation.

Congress Should Pass Beneficial Ownership Legislation

Finally, I support Congressional efforts to establish a nationwide framework for the collection of beneficial ownership information by a trusted government body and to provide that data to qualified financial institutions and law enforcement. During my time

⁹ Section 314b of the USA PATRIOT Act allows participant financial institutions to share information “regarding individuals, entities and organizations engaged in or reasonably suspected based on credible evidence of engaging in terrorist acts or money laundering activities.” This permission to share confidential information is known as a “safe harbor.”

at M&T, my team has investigated instances where shell companies appear to have been used to attempt to obfuscate the real actors behind transactions to move funds secretly to illicit actors. Based upon discussions with law enforcement and former prosecutors, shell companies are routinely used for this purpose. While the new CDD rule requires banks to ask their legal entity customers to certify as to their ownership, banks cannot independently verify that the information provided is accurate. A nationwide secure database of ownership information would be a useful investigative tool.

Conclusion

AML/CFT reform is needed to make the U.S. regime more effective and to allow institutions, like M&T, to redeploy or invest their limited resources in efforts and technology that will allow them to provide information that is of greater utility to law enforcement. I applaud the Subcommittee's interest in this important topic. Discussions such as these will assist in allowing banks to continue to support law enforcement's efforts to keep our communities safe and to cut off the flow of illicit funds through the U.S. financial system. I thank you for the opportunity to testify and look forward to your questions.