Gary M. Shiffman, Ph.D.

"An Economist's View on Technology in the future of BSA/AML"

Before the Subcommittee on National Security, International Development, and Monetary Policy

House Committee on Financial Services

United States House of Representatives

March 13, 2019

Introduction

Distinguished Members of the Subcommittee, thank you for the opportunity to appear before you today to discuss the important topic of countering financial crime.

I am an Economist who focuses on technology, behavioral science, and people who do bad things such as money laundering, human and drug trafficking, terrorism, fraud, and corruption. I am the CEO of Giant Oak, a software company focusing on making screening easy. I teach courses at Georgetown University on organized violence. I am also a Navy Gulf War veteran and I have served in a federal law enforcement agency.

I have no interest in AML compliance for compliance sake; I tell you about my background to emphasize this point. I come to the sub-committee today as a technologist to argue that we can and must do better at combatting money laundering, trafficking, terrorism, and other illicit acts.

Background

Our current AML regime requires radical reform. We are inefficient. According to the United Nations, "The estimated amount of money laundered globally in one year is 2 - 5% of global GDP".[i]

At the same time, spending to combat money laundering and the financing of terrorism (AML/CFT) exceeds $7 billion[ii] in the US and $25 billion[iii] globally. However, of the approximately 2 million Suspicious Activity Reports (SARs) generated by today's AML systems for FinCEN, less than 5% provide value.

In short, it appears we have an AML regime that compels the industry to spend billions of dollars, generates mostly useless data, and counters less than 1% of the problem.

We must do better. We can begin by harnessing available technologies and focusing them on supporting our law enforcement and national security professionals.

Machine Learning

When I say technology, I refer primarily to Machine Learning (ML), Artificial Intelligence (AI), and the application of behavioral science to data analytics. I define Machine Learning as the training of computers to identify patterns in data.

If you imagine a spreadsheet with millions of rows and columns, it is not hard to believe that patterns exist somewhere in the data, but because our human eyes and brains cannot find those patterns, none of us will ever again live in a world without Machine Learning.

By utilizing Machine Learning, we can teach computers to find and reveal the patterns for us.

Any future AML regime must include Machine Learning, and a future BSA/AML regime without without Machine Learning seems unbelievable. So what shall we do?

How to Create the Best *Machine* to Detect and Deter Financial Crime

To build the best *machine* to detect and deter financial crime, one needs good training data. Machines are literal. If you teach it to play chess, it will not learn to play checkers. The best *machine* on the planet for AML will be built by training it on the best AML data.

If we apply this to financial crimes, the vulnerabilities and opportunities are obvious: government agencies know which SARs provided the best quality information, but the banks do not, so they cannot train their tools properly.

The few banks using Machine Learning for AML today train their *machines* on previous years' SAR data. If more than 95% of past SARs were wrong, then these banks simply perpetuate inaccuracies (just more efficiently). However, with feedback from law enforcement, systems can learn and improve. This is where we need to bring the AML regime.

Call to Action

I do not want to end without raising a word of caution. Computers are powerful tools that can do both good and bad. As far back as the 1968 Stanley Kubrick and Arthur C. Clarke film *2001: A Space Odyssey*, we humans have understood the need to harness the computer.

To ensure we maintain the balance between risks and rewards of advancing technologies, I suggest three core principles for the subcommittee to consider as part of any reform or legislative proposal:

1. Encourage information sharing between law enforcement, financial institutions, and regulators. This will enable the sharing of priorities and training data for Machine Learning. This will also help regulators better judge the quality of the data

generated, and not just the volume. It will also provide tools for measuring biases in data.
2. Avoid opaque solutions where humans cannot understand the internal processes or outcomes of the *machines*.
3. Keep humans in the loop; let machines sort and filter data, but let humans adjudicate good vs. bad and right vs. wrong.

Closing

To close, Machine Learning already pervades our lives. Technology will increasingly enable regulated financial institutions to identify threats with increasingly precise measurements that will enhance security, protect privacy, and promote financial inclusion.

We spend billions today to generate mostly useless data and miss 99% of global financial crime. Law enforcement knows that better systems based upon existing technologies are available to generate good data and keep us all safer and more secure.

Thank you for your time, and I'm happy to answer any questions you may have.

---

[i] https://www.unodc.org/unodc/en/money-laundering/globalization.html
[ii] https://www.theclearinghouse.org/banking-perspectives/2016/2016-q3-banking-perspectives/departments/by-the-numbers-aml
[iii] https://www.prnewswire.com/news-releases/anti-money-laundering-compliance-costs-us-financial-services-firms-25-3-billion-per-year-according-to-lexisnexis-risk-solutions-300728586.html