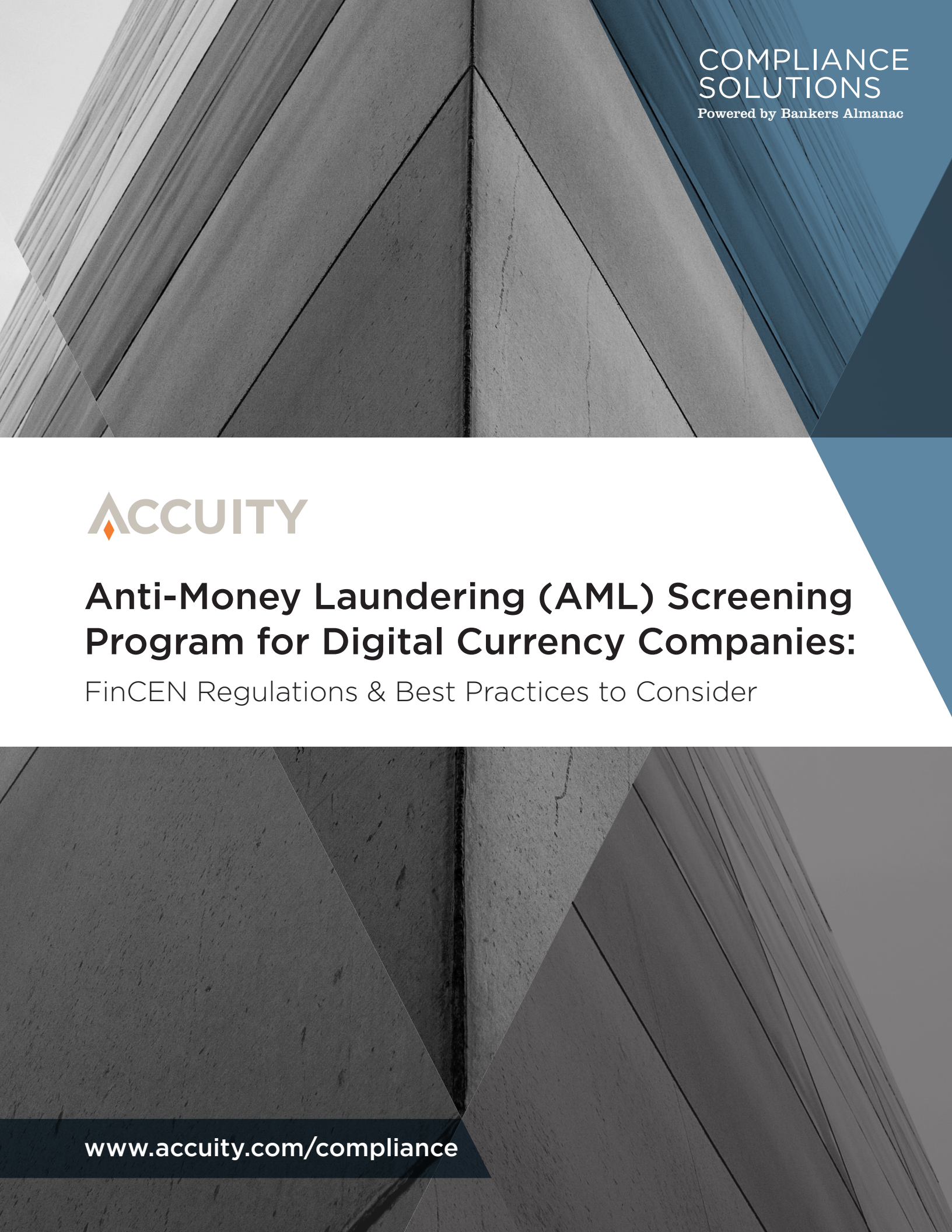


COMPLIANCE SOLUTIONS
Powered by Bankers Almanac

ACCUITY

Anti-Money Laundering (AML) Screening Program for Digital Currency Companies:

FinCEN Regulations & Best Practices to Consider

www.accuity.com/compliance

Index

Introduction—The Rise of Digital Currencies

With the number of digital currencies rapidly increasing due to a large amount of venture funding—over 600 currencies to date—governments are beginning to realize the current and future significance of digital currencies in the financial sector.

The centralized nature of the world of finance has already begun to slowly disintegrate with the rise of the Internet and the inefficiencies of the banking system (led by a double entry system of accounting created over 500 years ago), and are eventually going to be replaced by more efficient systems. Lower transaction costs, faster settlement, and ease of cross-border payments, are just a few of the many ways the decentralized nature of digital currencies can create a more efficient way to transfer money and value. Thousands of retailers across the globe have taken notice and now accept some form of digital currency. Which begs the question—why aren't more people beginning to use them?

600+

currencies to date

Outside of price fluctuation, the greatest knock on digital currencies is the anonymity surrounding them. There has been a great deal of adverse media surrounding digital currency, from Mt. Gox to Silk Road, and this has caused widespread distrust. Much of society is beginning to dismiss digital currencies as something that can be easily stolen, or worse, a currency that only drug traffickers, human traffickers, or terrorists use to hide their suspicious transactions. This dismissal is occurring before people ever learn about the blockchain technology behind digital currencies and the benefits this technology can provide the financial sector and beyond. Since the concept of digital currency is still largely in its infancy, this is a critical stage to begin to dispel the negative perceptions held by most.

To achieve widespread adoption of digital currencies a great deal of trust will be required—the same amount of trust society bestows in fiat currencies—and that trust cannot be built until the negative perceptions are lessened. Trust is not only important to get people to exchange their fiat currency for digital currency but also key in garnering strategic banking partnerships.

Federal governments create sanctions list (watch lists) to help aid in stopping the flow of money to drug traffickers, human traffickers, and terrorists. Screening owners of your digital currency (whether it is a client who buys it or any transaction you process on behalf of clients) against sanctions lists will allow you to stop the flow of money to sanctioned individuals.

Eliminating the anonymity by screening clients will help build trust and the feeling of security that many in society lack in what they view as a decentralized, and therefore unsafe, currency. Thus, to dispel society's concern about the anonymity of digital currencies and build the trust needed for widespread adoption, it is important for digital currency companies to put an Anti-Money Laundering (AML) screening program in place.

> "Since the concept of digital currency is still largely in its infancy, this is a critical stage to begin to dispel the negative perceptions held by most."

Why Did AML Screening **Become Important?**

Following the terror attacks that marked the dawn of the 21st century, AML screening programs in banks were heavily improved to detect funding to drug traffickers, human traffickers, and terrorists.

As a result, there are now hundreds of watch lists worldwide, totaling millions of names, from 'political exposed persons', to 'state-owned companies', to 'dual-use materials'. The sanctions on Libya during the Arab Spring on certain African leaders and more recent sanctions on Russia clearly demonstrate that sanction programs now form an integral part of governments' foreign policies, replacing military action wherever possible. Within the current world context, it is clear that this trend will continue and probably accelerate in the future.

With regard to the practical implementation of sanctions, anyone processing transactions of any form of currency are de facto gatekeepers of the financial system. As such, they have been enrolled by authorities for their essential role in checking identities, both at account opening or when transactions are processed. Most companies seek to protect their own reputation, and therefore perform their own preventive checks during an AML screening process.

In an era of increased scrutiny and judgments for anti-corruption, AML screening is a significant concern that keeps executives, the board, legal counsel, and compliance professionals up at night due to crippling fines and severe jail time for non-compliance. Digital currency companies, especially those in their infancy, cannot afford ad hoc approaches to anti-bribery and corruption. Established processes must be in place to prevent corruption from happening to please not only regulators but also owners of digital currency. The ability to demonstrate an established AML screening program can significantly reduce the penalties and reputational damage imposed upon a firm if wrongdoing was discovered.

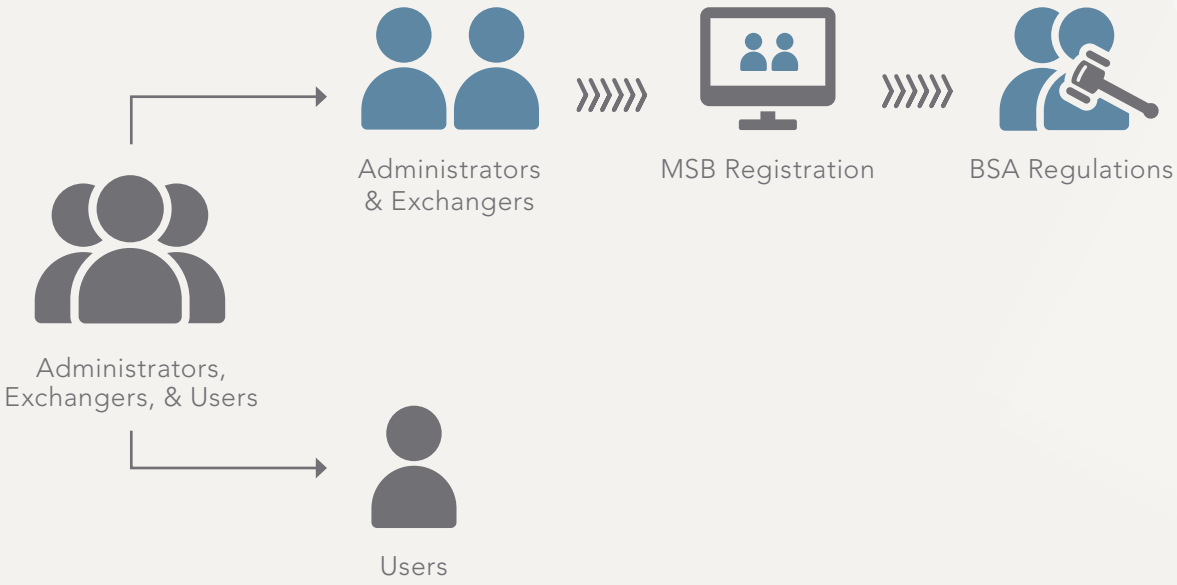
FinCEN Regulation: What Digital Currency Companies Do They Apply To?

According to United State Treasury's Financial Crimes Enforcement Network (FinCEN) regulation FIN-2013-G001, any person that is "creating, obtaining, distributing, exchanging, accepting, or transmitting" any form of digital currency must register as a Money Service Business (MSB) and therefore is subject to Bank Secrecy Act (BSA) regulations.

Within the FIN-2013-G001 regulation, FinCEN proceeds to break down different persons associated with digital currency as "users," "administrators," and "exchangers," while it clearly states that only administers and exchangers are required to register as a MSB and adhere to BSA regulations.

Users of digital currencies are merely people that buy digital currency to purchase either goods or services and are not subject to BSA regulation, while administrators and exchangers of digital currency fall under the (broad FinCEN) definition of a money transmitter MSB and therefore are subject to

FIN-2013-G001 Regulation



BSA regulations. Exchangers are those who are in the business of exchanging digital currencies for real currency, other virtual currency, or anything of value that easily substitutes to currency. This means that all brokers and dealers of digital currency or e-precious metals and brokers and dealers of centralized or decentralized convertible digital currencies are subject to BSA regulation. Administrators are those who have the power to issue or withdraw a digital currency from circulation. This means that all companies using blockchain or any other form of technology to issue or withdraw a digital currency are subject to BSA regulation.

FinCEN determines that all MSBs must fill out FinCEN form 107 to register as a MSB within 180 days of being established, and that registration must be renewed every two years. As part of being a MSB you must adhere to all BSA policies, which includes having a documented AML screening program. This white paper will go on to discuss not only the importance of having an AML screening program in place for digital currency exchangers and administrators, but will also serve as a guide to what a proper AML screening program looks like.

Ripple Labs: The Value of an AML Screening Program

Ripple Labs, a San Francisco based digital currency and payment network company, was fined $700,000 by the United State Treasury's Financial Crimes Enforcement Network (FinCEN) for violating the Bank Secrecy Act (BSA).

In addition to the monetary fine, Ripple Labs has to hire independent auditors to review their AML screening program (put in place after the fine) every two years until 2020. Many believe that the fine was steep for a start-up in largely undefined fin-tech space, but historical patterns of AML fines have proven that fines are much more substantial when violations are not willfully reported through Suspicious Activity Reports (SARS) and when no AML screening processes are in place, as was the case with Ripple Labs. If Ripple would have adhered to BSA regulations for a MSB that are clearly outlined in the FIN-2013-G001 regulation, the fines and reputational damage could have been avoided altogether.

The fine stemmed from a few **wrongdoings by Ripple Labs:**

- **They failed to establish themselves with FinCEN as a MSB** while being an administrator of digital currencies.
- **They failed to have an AML screening program in place** prior to and subsequent of March 2013 (when FinCEN's regulations on digital currencies were put in place).
- **They processed a few transactions for suspicious persons**, including a $250,000 transaction for a person who pleaded guilty to selling explosives on eBay.

The fine itself is only the tip of the iceberg, as Ripple Labs now has to look back at all past transactions, implement a transaction monitoring solution, change its protocol to collect more information on its customers, and train employees on AML regulations. Not to mention, the negative media surrounding the company subsequent the fine could dissuade potential investors and strategic bank partners going forward.

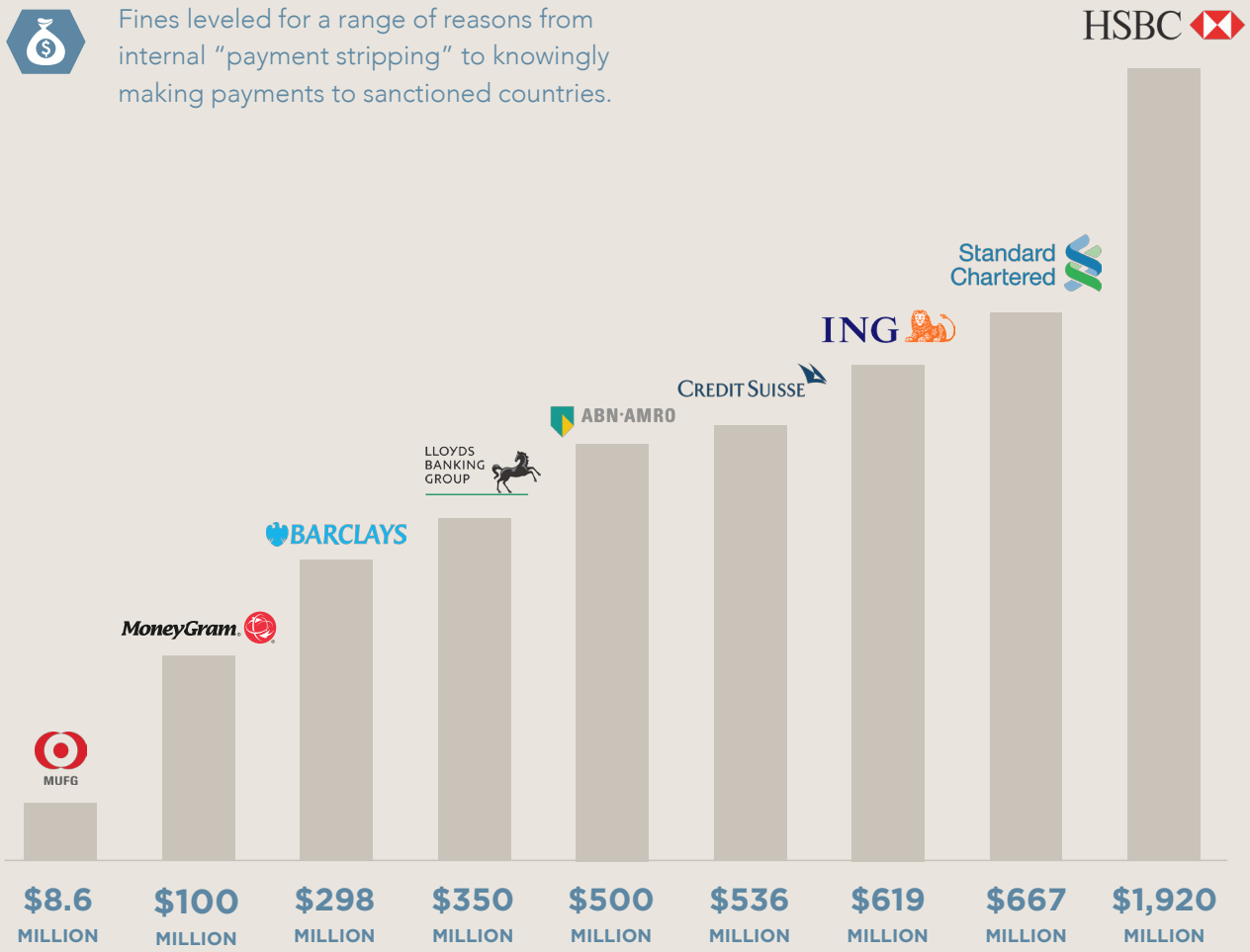
This served as the shot over the bow from FinCEN towards digital currency administrators and exchangers. MSBs, whether registered or not, need to have a proper AML screening program in place to ensure they do violate the BSA. Although this is a non-revenue generation function of a business, the cost of not having a proper AML screening program in place can be much higher due to fines and reputational damage incurred. Going forward, successful digital currency companies will view a proper AML screening program as an opportunity to do the right thing, ensuring their reputation is upheld and their business is protected now and in the future.

"The fine itself is only the tip of the iceberg, as Ripple Labs now has to look back at all past transactions, implement a transaction monitoring solution, change its protocol to collect more information on its customers, and train employees on AML regulations. Not to mention, the negative media surrounding the company subsequent the fine could dissuade potential investors and strategic bank partners going forward."

In the past couple of years, there have been over $2 billion in fines from FinCEN alone. Both the number and size of fines continues to grow on a yearly basis. The fine total doesn't begin to do justice to the cost of remediation and reputational damage incurred by the companies that were fined. To the right is a graph that highlights just a few of the major fines from the past couple of years:

Bank fines for AML violations scale with the severity of the violation

Fines leveled for a range of reasons from internal "payment stripping" to knowingly making payments to sanctioned countries.



(FINES IN $ USD MILLION)

What Does a Proper AML Screening Program **Look Like?**

Policy and Procedure

Sanctions programs may not specifically require a company to establish a Policy and Procedures manual. However, the lack of such a manual during a regulatory investigation can lead to severe consequences. Sample monetary penalties such as those from the United States Treasury's Financial Crimes Enforcement Network (FinCEN) can range up to $ 10,000,000 for each Bank Secrecy Act (BSA) violation and prison terms of up to 30 years can be imposed. Often times, the presence of a Policy and Procedures manual during an investigation can provide relief to such penalties if in fact there is one imposed. Refer to United States Sentencing Commission, Guidelines Manual, 8A1.2, Application Note 3(k) (2001).

Risk Profile

Building a company (and therefore customer) risk profile is essential to the establishment of a successful AML screening program. FinCEN and similar regulatory bodies suggest a risk based approach commensurate with the organization's BSA risk profile. This risk profile is typically based on products, services, customers and geographic locations. If an organization conducts business in countries that are considered high risk, while inherently not a BSA violation, the existence of a documented risk profile and having a proper customer identification and AML screening program in place are considerations during an examination.

People

A core element of an AML screening program is the staff responsible for implementing this program. Regulators require all levels of staff to be adequately trained on detecting and reporting suspicious activity within their organizations. Keeping adequate records and demonstrating to regulatory authorities that an effective training program is in place is essential. Another aspect is the appointment of a Compliance Officer whose responsibility is to ensure the AML sanctions program is in place and is effective through independent testing and verification.

Information

Proper client and transaction records that can be used as a basis for effective FinCEN screening is another important element. It is also key to consider the quality of the AML watch list(s) to be used for the screening process as well. The established FinCEN risk profile can heavily influence the robustness of the required screening. Invariably due to the nature of the AML watch lists put out by federal governments and other regulatory bodies, false positive matches are typically generated as a result of a screening process.

Not only do you want to ensure good quality client and transaction data, you also want to screen against a watch list with additional data enhancements to increase your chance of creating a match against entities on AML watch lists. Screening good quality client and transaction data against a sophisticated and enhanced watch list will reduce the volume of false positives, leading to the reduction of manual review and operational costs.

The elements described above, coupled with the selection of a well-known, robust screening technology solution, all combine to create **a successful AML screening program.**

Example

Let's take the example of a company in the US that issues or withdraws digital currency from circulation or exchanges digital currency for other forms of currency.

As of March 2013, the United States Treasury's Financial Crimes Enforcement Network (FinCEN) determined that those companies are required to register as a Money Services Business (MSB). All MSBs are obligated to develop an AML screening program as part of the guidelines set forth by the FinCEN to ensure adherence to the Bank Secrecy Act (BSA) guidelines.

FinCEN requires MSBs to have a proper AML screening or Know Your Customer (KYC) program in place, and requires client and transaction data to be actively screened against AML watch lists to prevent the flow of money to drug traffickers, human traffickers, and terrorists. As part of the KYC program, MSBs need to screen against the sanctions list put out by the United States Treasury's Office of Foreign Asset Controls (OFAC). All facets of the MSB's business, from all clients who are sold digital currency to all parties processed on a transaction (regardless of dollar value), must be screened against the OFAC list. MSBs in the United States also have an obligation to comply with international regulations outside of the United States if they deal significantly in international business. For example, they must be mindful of various regulations such as the EU's 4th AML Directive, which requires MSBs to monitor for anti-bribery and anti-corruption if they have operations in the EU or correspond heavily in the region. This would require a KYC program that screened clients against a Politically Exposed Persons (PEPs) list, since persons with political exposure are at a higher risk for bribery and corruption.

The following are examples of sanctions violations:

Processing a cross-border transaction going to a construction project in Beirut, Lebanon, in which a beneficiary of the project is linked to an organization that has ties to Al-Qaeda.

Selling digital currency to anyone in the EU without identifying if they are a Politically Exposed Person (PEP).

New account openings for individuals linked to sanctioned entities found on the OFAC list.

The purpose of these examples is to highlight the need for an AML screening program for any institution to develop procedures that screen not only the customer itself but other parties in a transaction.

How Can Technology **Help You Achieve** an Efficient AML Screening Program?

Compliance must be an active part of culture and processes to prevent and detect corruption, bribery, and fraud. AML screening programs that monitor for anti-bribery and anti-corruption must be monitored, maintained, and nurtured.

Regulations and watch lists are constantly updating and keeping up on these regulations is nearly impossible without the help of a trusted data provider. To contextualize this, the OFAC list has over 40,000 names and aliases, updates a few times weekly, and has a 20% increase in names and aliases annually. The challenge is establishing corruption prevention and detection activities that move the firm from an ad hoc reactive mode to one that actively manages, monitors, detects, and prevents corruption risk. This requires the firm to implement technology to manage AML compliance. Recent examples of fines totaling billions (listed earlier) have demonstrated that regulators take sanction breaches seriously. This leaves MSBs squeezed between the risk of huge penalties and the unbearable cost of manually investigating hundreds of thousands of persons and companies.

OFAC List

40k

Names & Aliases

Updates a Few Times Weekly

+20%

Names & Aliases Annualy

Technology facilitates a firm's ability to manage and monitor AML compliance by enabling and automating activities, information, processes, and reporting. **The use of technology for compliance delivers processes that are:**

Efficient

Compliance technology lowers cost, reduces redundancy, and improves human capital efficiencies. This is done through delivering accountability and automated electronic reporting that is burdensome in manual and document centric lookup approaches.

Accurate

Compliance technology delivers consistent and accurate information about the state of AML initiatives to assess exposure. Information is accurate, current to rapidly changing regulations, and readily available.

Agile

Compliance technology improves decision making and business performance through increased insight and business intelligence, so the business can achieve objectives while avoiding loss.

Automated

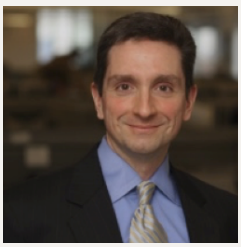
Compliance technology can automatically screen all of your client and transaction related data in real-time without manually entering any information for screening. This will lead to proactive decisions about the status of a client or transaction with a clear, consolidated, electronic audit trail to prove it.

Key Contributors

Jameson McRae

Product Manager for Risk & Compliance Solutions, Accuity

Jameson is the Product Manager for the Risk & Compliance Solutions line for Accuity in North and South America. He is a key member to the product marketing teams and professional services engagements which advise multinational institutions. He specializes in bringing technical knowledge, subject matter expertise, and communication skills together in order to overcome common industry challenges and expedite business development. Jameson is accustomed to and effective in leading high-profile consulting engagements for the world's largest firms. Accuity is a global provider of payments and compliance solutions with clients in the Financial Services and Corporate sectors, including banks, shipping and manufacturing firms, money services businesses, and insurance companies.



Ron Quaranta

Chairman of the Wall Street Blockchain Alliance

Ron is an accomplished executive and entrepreneur, with 25 years of experience in the financial services and technology sectors. He currently serves as Chairman of the Wall Street Blockchain Alliance, an advocacy group whose mission is to guide and promote comprehensive adoption of blockchain technology across financial markets. He also serves as Chief Executive Officer of Digital Currency Labs, a financial technology and strategic advisory firm focused on bridging the gap between the emerging world of digital currencies and Wall Street. Prior to this, Ron served as CEO of DerivaTrust Technologies, a pioneering software and communications provider of secure transaction and information platforms for financial market participants. Before this he held a variety of roles at Thomson Reuters, the global news and information firm, culminating as Global Head of Trading Analytics.

GETTING STARTED
Email: **customerservice@accuity.com**
or go to **www.accuity.com/payments**

12.10.15