alessa

iCOMPLY

Definitions, Obligations and Best Practices

What Financial Institutions Need to Know About Cryptocurrency

Adoption of cryptocurrency has seen a remarkable increase over the last few years - growing to an overall market capitalization of over $150 billion[1] in less than 10 years. The new market has resulted in new types of businesses that financial markets have never seen before. Collectively referred to as Virtual Asset Service Providers (VASPs), these include cryptocurrency exchanges, digital wallets, custodial services, and Bitcoin ATMs.

While many traditional banks and other financial services businesses have taken a wait-and-see approach, the explosive growth of this industry is requiring these institutions to take a more active role and determine how best to enter the market while still maintaining a risk-based approach to anti-money laundering (AML), know your customer (KYC), and Bank Secrecy Act (BSA) compliance.

Defining Digital, Virtual and Cryptocurrency

While often used interchangeably, digital currency, virtual currency, and cryptocurrency each mean slightly different things.

Digital currency is a broad term for any payment method that exists only in electronic form and is not tangible.[2] A virtual currency is a subset of digital currency and is a digital representation of value, issued by private developers and denominated in their own unit of account.[3]

Crypto currency (or cryptocurrency) is a type of virtual currency that uses cryptographic protocols to secure the currency. Cryptocurrency bundles up transactions into blocks and uses various cryptographic protocols (based on the individual cryptocurrency) to establish the correctness and permanence of each block. After the block has been verified, it is added to the end of a blockchain.

While these terms differ slightly, from a regulatory compliance perspective, they can be treated as one-and-the-same, as many people, and some regulators, use these terms interchangeably and they require similar due diligence when evaluating the risks associated with each.

[1] *https://coinmarketcap.com/charts/*
[2] *https://www.techopedia.com/definition/6702/digital-currency*
[3] *https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf*

Types of Cryptocurrencies

Bitcoin was the first mass-adopted cryptocurrency and still maintains over 50 per cent market dominance. However, it is only one of thousands and not all cryptocurrencies are the same. Looking at the cryptocurrency landscape, there are fewer than 15 with a market capitalization of over $1 billion and fewer than 850 with a market capitalization of over $1 million.

Each cryptocurrency serves a different market or use case:

Bitcoin is the largest, most used, and first major cryptocurrency. While there have been a number of technologies built to expand the usage of Bitcoin, it is fundamentally a currency. There have been a number of splits of Bitcoin referred to as hard forks (when a cryptocurrency splits in two and they become two totally different currencies from the activation block forward) that have separated from Bitcoin. These include Bitcoin Cash, Bitcoin SV, Bitcoin Gold, Bitcoin Diamond, etc. Litecoin was an early hard fork from Bitcoin that served to reduce transaction costs. These are classified as **Conventional** cryptocurrencies. While some organizations have built "layer 2" technologies to expand the functionality of these conventional cryptocurrencies, their primary use is to function as a replacement for traditional currency.

Ethereum is the second largest cryptocurrency and serves as both a currency (Ether) and a computing network. Programs, called **Smart Contracts**, run on the Ethereum network. While these can be used as conventional cryptocurrencies, they can also be used to store and trade digital representations of real-world goods, such as equities, commodities and real estate.

Ripple is being used by traditional FIs to send bank-to-bank remittances. It and other services are referred to as **Settlement Networks.**

Monero and **zCash** both serve as highly anonymous networks or **Privacy Cryptocurrencies or Private Coins.** Unlike most other cryptocurrencies, these use complex math to anonymize the ledger, making it difficult or impossible to determine who is transacting. Privacy coins are used by individuals who value anonymity of transactions and users.

Stable Coins, such as **Tether, TrueUSD, Paxos, GeminiCoin, and Dai**, attempt to tie the value of the cryptocurrency to a traditional, fiat currency (such as the US Dollar) or some other commodity. They provide an easy mechanism to switch between cryptocurrencies and fiat currency value.

Each type of cryptocurrency, and each cryptocurrency within each type, poses unique risks. These include the anonymity of transactions (making tracing those transactions difficult or impossible) as well as risks of a currency being hacked.

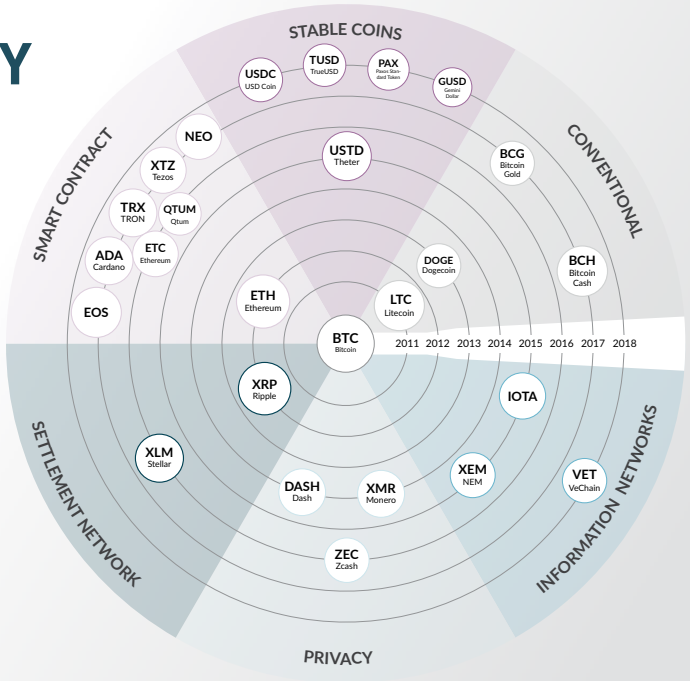
In the same way that financial institutions manage geopolitical risk, where each country is risk-ranked, the same approach should be taken with cryptocurrencies, monitoring and identifying risk of each cryptocurrency and making decisions on engaging with those cryptocurrencies.

CRYPTOCURRENCY LANDSCAPE

Top 10 Cryptocurrencies by Market Capitalization

Bitcoin	USD	$181.9 Billion
Ethereum	USD	$22.9 Billion
Ripple	USD	$13.7 Billion
Litecoin	USD	$5.9 Billion
Bitcoin Cash	USD	$5.5 Billion
Tether	USD	$4.0 Billion
EOS	USD	$3.8 Billion
TRON	USD	$1.9 Billion
Stellar	USD	$1.7 Billiion
Cardano	USD	$1.5 Billion

*Data source from coinmarketcap.com, July 2019



Cryptocurrency Businesses or VASPs

Along with the advent of cryptocurrency there has been the creation of an entirely new industry of businesses to serve these new markets. Called virtual asset service providers (VASPs), each of these pose new challenges for individuals and businesses transacting with them, and most require regulatory compliance.

Fiat-to-Crypto Exchange

Fiat-to-Crypto exchanges provide users the ability to exchange fiat currency (USD, EUR, CAD, etc.) for cryptocurrency. These exchanges allow users to send and receive cryptocurrency and make deposits and withdrawals in fiat currency. In many jurisdictions, fiat-to-crypto exchanges must be registered with their local Financial Intelligence Unit (FIU) as a money services business (MSB).

Crypto-to-Crypto Exchange

Some exchanges do not provide direct access to fiat currencies, but rather serve as a method to exchange one type of cryptocurrency for another. These exchanges often provide access to a greater number of cryptocurrencies.

Decentralized Exchanges (DeX)

Decentralized, or peer-to-peer, exchanges do not use a central authority to facilitate transactions and do not store any cryptocurrency on local servers. Rather, they serve as a means of connecting buyers and sellers who then transact directly or through proxy tokens. Because there is no central authority, DeXs do not require users to register or provide any details to a central authority. For many, this provides a level of anonymity and security that its users prefer. DeXs do not provide for any registration or any Know Your Customer (KYC) or Anti-Money Laundering (AML) compliance.

Custodial Services

While cryptocurrency provides users the ability to store their private keys, many users choose to use a service to store their keys. Centralized exchanges provide this feature for their users as do a number of online wallet services. As these services hold and transmit funds, they often have to register with appropriate FIUs as MSBs.

ICOs/STOs

ICOs (Initial Coin Offerings) and STOs (Security Token Offerings) are both mechanisms for businesses to raise money through the issuance of digital tokens. Those tokens can represent a utility such as a pre-purchase of a product (ICO) or a security (STO). In 2018 almost $8 billion[4] was raised through ICOs and STOs. Depending on the type of offering, the issuer may need to register with securities regulators, such as the SEC in the United States.

Others

With an industry as large as cryptocurrency, there are many other types of businesses that may come into contact with traditional FIs. Each one may represent unique risks and may or may not have a similar counterpart in traditional markets. These include peer-to-peer lending services, Over the Counter (OTC) trading platforms, gambling services and Bitcoin ATMs.

As part of their overall risk-based approach to cryptocurrencies, financial institutions must understand the type of business when determining whether to onboard the business as a client and/or whether to transact with that business. For example, Mixing Services are a type of VASP that serves to obfuscate the transaction source or destination. These are high-risk businesses that are frequently used to launder money through the blockchain.

[4] *https://www.icodata.io/stats/2018*

What are the Regulators Saying?

Despite calls for the adoption of global AML standards for cryptocurrency trading, no such uniform rules have yet emerged.

Over the last 12-24 months, regulators across the globe have been reaching out to industry leaders in both traditional finance and cryptocurrency to determine how to develop and maintain proper protections for all players in these new markets. This includes regulators covering taxes (IRS), commodities (CFTC), securities (SEC), currency (OCC), corporate law (DFS in New York and Florida) as well as BSA/AML compliance (FinCEN).

There has been some convergence toward the Financial Action Task Force (FATF) view that cryptocurrency payment service providers should be subject to the same obligations as their non-crypto-counterparts. However, the level of legality of cryptocurrency ranges significantly from country-to-country and even state-to-state. In Canada, for example, many major banks do not permit transacting with cryptocurrency[5]. In China[6] the government has completely banned cryptocurrency miners and exchanges. In New York cryptocurrency business must apply and receive a Bitlicense before they can conduct business.

Other jurisdictions, such as Switzerland, Singapore, Luxembourg, Malta and Gibraltar, have seen cryptocurrency as a new opportunity to grow their financial sector.

Many of these jurisdictions have issued rules or guidance on the matter and have concluded that the commercial exchange of cryptocurrency for fiat currency (including through Virtual Currency Exchanges (VCEs)) should be subject to KYC, AML, and securities obligations.

Where cryptocurrency and crypto-related businesses (virtual asset service providers) are legal, the general guidance, as provided by SEC Chairman Jay Clayton[7] is:

> *"...replacing a traditional corporate interest recorded in a central ledger with an enterprise interest recorded through a blockchain entry on a distributed ledger may change the form of the transaction, but it does not change the substance."*

Said another way, it is not the *form* that a security, commodity, or currency takes, but rather the function. The rules should be implemented the same way regardless of the type of currency.

---

[5] *https://www.investopedia.com/news/canada-banks-ban-users-buying-cryptocurrency/*

[6] *https://www.loc.gov/law/help/cryptocurrency/china.php*

[7] *https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11*

FinCEN Provides Further Clarification on Regulations for Virtual Asset Service Providers

On May 9th, 2019, FinCEN released interpretive guidance on how existing regulations impact cryptocurrencies, which are referred to as convertible virtual currencies. While the "guidance does not establish any new regulatory expectations or requirements," it does clarify existing regulations and the obligations of many crypto businesses.

The guidance serves to explain which types of businesses must register as Money Services Businesses (MSBs) and thereby comply with FinCEN MSB regulations, including compliance with the Bank Secrecy Act (BSA).

Compliance with the BSA requires businesses to screen their customers, third party relationships, and transactions to mitigate money laundering or terrorist financing risk. These regulations also require the filing of Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs) when those risks are identified.

The guidance does not however cover regulatory obligations associated with securities, commodities, taxes, or other possible government regulations which are managed by other government entities such as the SEC, OCC, CFTC, IRS, and others.

FinCEN's policy on what constitutes an MSB is clear: "whether a person qualifies as an MSB subject to BSA regulation depends on the person's activities and not its formal business status." Put more simply, it is the function of the business, not the form it takes or the name it is given. The same policy applies to all types of currencies: money is considered "currency, funds, or other value that substitutes for currency."

FinCEN has clarified that organizations that do business "in whole or in substantial part within the United States," are subject to BSA regulations, even if they have no physical presence in the United States. This will make it more difficult for companies headquartered overseas to skirt AML obligations if they are doing business in the US. However there are cases where an individual or business may not be subject to MSB requirements, and that is if they perform certain MSB activities, but do so infrequently and not for gain or profit.

Key Takeaways from FinCEN's Guidance

- **Exchanges,** whether crypto-to-crypto or fiat-to-crypto, must register as an MSB and comply with the BSA (including having a complete AML program and SAR/CTR reporting).
- **Hosted wallets** are services where the provider manages private keys and is responsible for backup and security. They must comply fully with BSA requirements. Unhosted wallet providers, such as deployed software or most hardware wallets, are not required to comply with BSA and FinCEN AML requirements.
- **Cryptocurrency ATM providers** must comply with BSA and FinCEN AML requirements.
- **DApps** (decentralized apps such as Ethereum Smart Contracts) may or may not be required to comply with the BSA depending on whether the DApp performs money transmission (31 CFR § 1010.100(ff)(5)(i)(A)).
- **Privacy Coins** (zCash, Monero, etc.) and anonymization services (such as mixers or tumblers) must comply with BSA and FinCEN AML requirements.
- **Cryptocurrency Payment Processors** (also known as fiat gateways) do not qualify for the BSA exemptions provided to fiat payment processors as they may process payments from individual wallets, unlike fiat payment processors who only process payments from financial institutions through credit card payments or bank transfers. Because of this, cryptocurrency payment processors must comply with BSA and FinCEN AML requirements.
- **Decentralized Exchanges** (DeX) do not need to comply with BSA and FinCEN AML requirements as long as the DeX does not facilitate the transfer of funds or hold any user funds.
- **Mining Pools** may have to comply with BSA and FinCEN AML requirements if the pool hosts the wallets that receive the proceeds of the mining. If there is no wallet hosting provided by the mining pool, they most likely do not have to comply with BSA/AML requirements.
- **Token Offerings (**Initial Coin Offerings, Initial Exchange Offerings, Security Token Offerings, et al) provide the most complex scenarios for determining AML/BSA requirements. Based on the organization, type of the issuer, intermediary, or investor, the FinCEN obligations may align more closely with a bank, broker-dealer, futures commission merchant, commodity dealer, or mutual fund. These types of institutions have different AML/BSA requirements and will differ from those of an MSB.

Organizations issuing ICOs should work closely with trusted issuance vendors, accountants, and lawyers to determine what is required for regulatory compliance based on the type of issuance and potential investor pool.

While the guidance does clearly outline how the U.S. Department of the Treasury views many virtual asset business models, it does not cover all possible crypto businesses. It is important to consider that just because a business does not fall neatly into one of the categories described does not mean it can avoid FinCEN compliance obligations. Where things may be unclear, the business should reach out to an experienced compliance lawyer or reach out directly to FinCEN.

What Should Financial Institutions Do?

Inconsistent regulations is nothing new for AML/BSA professionals. While FATF provides global guidance, each jurisdiction provides its own rules. This can be seen significantly in the jurisdiction-to-jurisdiction variations in Politically Exposed Persons (PEPs) screening requirements.

As with traditional AML/BSA screening, compliance teams must take a risk-based approach to cryptocurrency. The challenges posed by cryptocurrency require new methods to mitigate new risks.

Risk profile each cryptocurrency

Historically, financial institutions have treated all cryptocurrencies as one-and-the-same. This does not reflect the reality of cryptocurrency. Each cryptocurrency poses unique risk. As an example:

- **What is the level of privacy of the cryptocurrency?**

Certain cryptocurrencies, such as Monero, zCash, and Dash, provide significant privacy and anonymity for their users. Individuals use these currencies to ensure their transaction and account privacy. While this does not imply their activities are illicit or illegal, greater privacy implies greater risk for financial institutions. Understanding the different cryptocurrencies and their level of risk is as critical as and can be more difficult than understanding geopolitical risk.

- **What is the hacking risk of the cryptocurrency?**

While established cryptocurrencies like Bitcoin and Ethereum have large networks that protect them from individuals or groups that may try to take over the currency, that is not the case for smaller currencies.Depending on the technical implementation, the market capitalization and the size of the network, certain cryptocurrencies may be easy to manipulate, potentially causing significant losses for its users.

Use blockchain forensics tools

In addition to traditional transaction monitoring, institutions must monitor the transactions of their customers and other 3rd parties on the blockchain. While the patterns may be similar between traditional finance and cryptocurrency, the methods used to identify these patterns are quite different.

While blockchain technology provides new challenges for AML/BSA compliance, the public ledger of many cryptocurrencies such as Bitcoin, Ethereum, Dash and Neo allows a level of transaction visibility that is not possible in traditional finance. Using blockchain forensics tools, compliance teams can analyze the transaction history and connections for any wallet address. This provides an incredibly valuable tool in analyzing the risk of an individual based on their transaction history and transaction proximity to high risk wallets, such as dark markets.

Exchange security standards

With significant hacks and cryptocurrency exchange failures[8], such as QuadrigaCX[9], many traditional financial institutions are wary of transacting with VASPs[10]. Traditional FIs do not want to permit their customers to engage with high risk business that may reflect poorly on the FI. Financial Institutions can play an important role in pushing for implementation of IT security standards for cryptocurrency businesses. FIs must also ensure all cryptocurrency businesses that they transact with meet industry standards for KYC and AML. Due to the varied jurisdictions used by many crypto businesses, FIs must understand the KYC/AML policies in these jurisdictions and take a risk-based approach when engaging in business with different crypto-businesses.

ICOs and VASPs that failed to implement compliance

Regulators are monitoring and regulating cryptocurrency businesses and fines, penalties, and enforcement actions are on the rise:

- **2015:** Ripple Labs was assessed a $700,000 civil money penalty for willfully violating several requirements of the Bank Secrecy Act (BSA) by acting as a money services business (MSB) and selling its virtual currency, known as XRP, without registering with FinCEN, and by failing to implement and maintain an adequate anti-money laundering (AML) program designed to protect its products from use by money launderers or terrorist financiers.
- **2017:** Russian exchange BTC-e was handed a $100 million civil fine by FinCEN for failing to comply with AML rules. According to FinCEN, the company was also complicit in AML rules, in their facilitation of digital transactions involving "ransomware, computer hacking, identity theft, tax refund fraud schemes, public corruption, and drug trafficking."
- **2018: The** Securities and Exchange Commission (SEC) settled charges with both CarrierEQ Inc. (Airfox) and Paragon Coin Inc. for ICO securities offering registration violations. Airfox raised approximately $15 million worth of digital assets to finance its development of a token-denominated "ecosystem" starting with a mobile application that would allow users in emerging markets to earn tokens and exchange them for data by interacting with advertisements. Paragon, an online entity, raised approximately $12 million worth of digital assets to develop and implement its business plan to add blockchain technology to the cannabis industry and work toward the legalization of cannabis.
- **2019:** The SEC sued Kik Interactive, claiming it illegally raised $100 million through an initial coin offering in 2017 without registering its offering as securities.
- **2019:** IoT security firm Atonomi faces a $25 million class-action lawsuit for failing to register their ICO with the SEC.

[8] *https://www.zdnet.com/article/2018s-most-high-profile-cryptocurrency-catastrophes-ico-failures-and-cyberattacks/*
[9] *https://www.bloomberg.com/news/articles/2019-03-01/quadriga-has-6-cold-wallets-but-they-don-t-hold-any-crypto*
[10] *https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html*

Risk scenarios to watch for

As with all financial vehicles, cryptocurrency poses AML and CFT risk. These risks can be divided into two areas: those that align with traditional AML and those that are unique to cryptocurrency.

For traditional AML risks, these will include both predicate offences, such as fraud, bribery, terrorist financing, organized crime, human trafficking, and counterfeiting; as well as transaction monitoring risk such as structuring and high value transactions.

There are a number of risks, however, that are unique to cryptocurrency such as:

- use of dark web sites
- use of PunyCode URLs
- cryptocurrency giveaways
- pump-and-dumps
- use of mixing services and many others

Additionally, many VASPs must be registered as MSBs (Money Services Businesses) with FinCEN. FIs receiving or sending transactions to and from VASPs should ensure those VASPs are properly registered.

Conclusion

The cryptocurrency market continues to grow and expand, with new businesses and cryptocurrency MSBs opening up almost daily. One third of all cryptocurrency exchanges have opened since the beginning of 2018, and this trend is unlikely to slow. With adoption of these new financial vehicles growing and new users coming on-board every day, financial institutions need to engage in this new industry while managing the associated risk.

When evaluating the risk associated with a particular cryptocurrency, compliance officers have new challenges and new risks to consider and manage.

1. As regulations across jurisdictions are still evolving, extra attention must be paid on what regulators require for compliance.

2. For those operating in the U.S., FinCEN has issued clarification for virtual asset providers and some types of businesses need to follow BSA and FinCEN AML requirements while others are exempt under special cases. Compliance officers should work with their legal counsel and directly with the regulators to understand their obligations.

3. Risk profile each cryptocurrency as each poses unique risk.

4. In addition to traditional transaction monitoring, institutions must monitor the transactions of their customers and other third parties on the blockchain. While the patterns may be similar between traditional finance and cryptocurrency, the methods used to identify these patterns are quite different.

5. Ensure all cryptocurrency businesses that they transact with meet industry standards for KYC and AML.

6. Watch for additional risks that are unique to cryptocurrency including the use of dark web sites, PunyCode URLs, mixing services and many others.

7. Rely on technology that is designed to analyze blockchain transactions to mitigate risks associated with cryptocurrencies.

KYC and Compliant Token Issuance by iComply Investor Services

iComply Investor Services Inc. (iComply) is an award-winning software company focused on reducing regulatory friction in the capital markets. With powerful data, verification, and tokenization solutions, iComply helps companies overcome the cost and complexity of multi-jurisdictional compliance to effectively access new markets.

End-to-End Compliance for Smart Assets: Efficiently onboard investors in seconds with robust, global KYC & AML, enhanced due diligence, accreditation and liveness. Issue smart assets and maintain compliance across jurisdictions to dramatically reduce human error, costs and regulatory friction. Trusted by legal, accounting and fintech vendors in over 100 countries for real estate, funds, equity, debt and digital assets.

Country-by-Country Screening: iComplyKYC brings the powerful KYC/AML features from our flagship PREFACTO Platform for use in digitally onboarding customers.

Cryptocurrency Exchanges, Fintech Platforms, and Financial Institutions can now access world-leading KYC, AML, and BSA compliance, along with blockchain forensics in a simple, secure, and straightforward REST API.

Powerful Client Onboarding: iComply allows exchanges, broker-dealers, money service businesses, and fintech platforms to efficiently onboard new individuals and corporations based on the requirements of their local jurisdiction. iComply's suite of turn key solutions include identity verification, document authentication, accredited investor verification, blockchain forensics, and more. Simplify the implementation of your compliance program via API, SDK, or easy to deploy "copy and paste" widgets for your platform.

To learn more about how iComply can help automate your compliance requirements, visit **https://icomplyis.com**

AML Compliance with Alessa

Alessa provides all the anti-money laundering (AML) capabilities that banks, money services businesses (MSBs), FinTechs, casinos and other regulated industries need – all within one platform. Capabilities of the product include:

Customer Due Diligence: To support KYC, CDD, and EDD processes, Alessa combines data from onboarding, transaction monitoring, and other core systems with identity verification and risk intelligence data to provide updated risk profiles and scores that are based on activities and relationships.

Sanctions Screening: Alessa screens individuals and businesses against multiple lists including PEPs, negative news, OFAC, and other sanctions lists. Screening can be done in native characters and in real time, periodically or on demand.

Transaction Monitoring: Alessa can analyze every transaction in real time and, using an extensive library of analytics and scenarios, generate alerts for suspicious activities. These are sent to the appropriate personnel via text or email for investigation and/or reporting.

Regulatory Reporting: All suspicious activity alerts include data needed for regulatory reports. Once it is determined that a Suspicious Transaction Report or a Suspicious Activity Report needs to be filed, Alessa can auto-populate (and electronically file) as many as 70% of these reports. Alessa can also automate as much as 100% of CTRs.

Risk Scoring: Alessa uses data from various sources, including sanctions lists, to provide an assessment of the risks of doing business with an individual or business. The solution also periodically reviews an organization's customer base and updates their risk level based on their activity and third-party data.

Configurable: With Alessa, organizations can select the functionality they need or the complete solution. Permission-based functionality allows different users to access only the information they need to perform their responsibilities, and data can be maintained in the cloud or on-premise, ensuring compliance with regulations.

Data Management: Alessa accesses data from any platform, including ERPs, bespoke applications, and core business systems. The data is then cleansed and aggregated to increase its accuracy, and cross-referenced to reveal big-picture insights. Better data means better insights.

Investigation Tools: Alessa offers dynamic workflows to guide processes and investigations. Enterprise search capabilities allow for easy searching of data within internal and external sources, while case management offers a collaborative approach to investigations, compliance, and decision making.

Metrics & Insights: Alessa offers configurable dashboards that track key metrics and allow compliance staff to drill down into the alerts. Advanced analytics allow for sound decision-making and actions to be taken based on comprehensive information and insights.

To learn more about how Alessa can help with your AML compliance activities, visit **alessa.caseware.com**

About CaseWare RCM

CaseWare RCM Inc. is the maker of Alessa, a financial crime detection, prevention and management solution. With deployments in more than 20 countries in banking, insurance, FinTech, gaming, manufacturing, retail and more, Alessa is the only platform organizations need to identify high-risk activities and stay ahead of compliance. To learn more about how Alessa can help your organization ensure compliance, detect complex fraud schemes, and prevent waste, abuse and misuse, visit us at **www.alessa.com.**

150 Isabella Street, Suite 800,
Ottawa, ON K1S 1V7, Canada

1-844-265-2508

alessa@caseware.com

www.alessa.com

alessa