

CHARTWELL COMPASS

A PUBLICATION OF CHARTWELL COMPLIANCE | CHARTWELLCOMPLIANCE.COM

MAY 2018

CHARTWELL COMPLIANCE provides a one-stop shop of consulting, testing and outsourcing services in the areas of regulatory compliance, state MSB licensing, financial crimes prevention and enterprise risk management.

EDITORIAL STAFF

Daniel A. Weiss, President and CEO
danielweiss@chartwellcompliance.com

Jonathan Abratt, Chief Operating Officer
jonathanabratt@chartwellcompliance.com

Richard Davis, Corporate Services Director
richarddavis@chartwellcompliance.com

- 2** **Chartwell Experience: Case Studies**
- 3** **Crossing the Pond? An Overview of International FinTechs Entering the U.S. Market**
Updated by Patricia Lagodzinski
- 5** **FinCEN and Beyond Evolving Regulatory Framework for Virtual Currency**
Sherry Tomac and Trish Lagodzinski
- 8** **Streamlined Licensing Process for Fintech Companies and Money Services Businesses**
Trish Lagodzinski
- 10** **Interview with Ashley Tassell, Compliance Director at FIRMA Foreign Exchange**
Richard Davis
- 12** **Canada's AML Climate Heats Up**
Matt McGuire
- 13** **Your Money Services Business Independent Review**
Karen Schirmer
- 18** **Points to Ponder**
- 20** **About Chartwell Compliance**
- 21** **Services**
- 22** **Strategic Alliances**
- 23** **Consultants**

Chartwell has been engaged on 20 plus full-country state license engagements and managed full-country approved license portfolios for roughly 16 companies which both include 6 former employers. We have handled 10-15 other licensing engagements with 20 or less states.

Relevant Skills

- ▶ State licensing
- ▶ Regulator relations
- ▶ BSA/AML/OFAC
- ▶ Consumer compliance
- ▶ Project management

Certifications

- ▶ Compliance: CAMS, CRCM, CFE
- ▶ Info Security: CISA
- ▶ Project Management: PMP
- ▶ Legal/Regulatory: J.D.



▶ Major-State License Acquisition and Maintenance and Outsourced Compliance Officer

Situation of prior unlicensed activity negotiated successfully with regulators to mitigate fines.

▶ Nationwide License Acquisition and Maintenance

Secured most licenses in under a year in a very large and complex organizational environment.

▶ Nationwide License Acquisition, Maintenance and AML Audit

Success in highly fluid internal environment and with client reps who are compliance grandmasters.

▶ Nationwide License Acquisition and Maintenance

Secured license exemptions as well; company has the industry's most high profile investors.

▶ Nationwide License Acquisition

Secured most licenses in under a year starting from absolute scratch in documentation for this NYSE-listed business.

▶ Nationwide License Acquisition and AML Audits

Completed nationwide transfer of control project with 2 private equity firms and the company in less than a year so deal could proceed. Years of AML audits in U.S. and Guatemala.

▶ Transfers of Control, AML Audits, Compliance Advisory

Nine years of experience with supporting the company during acquisitions and with audits.

▶ AML Audits, Due Diligence, Compliance and Licensing Advisory

Six years of experience with supporting the company in every area of compliance.

▶ Major-State Licensing, AML Audits, Compliance Advisory

Nine years of experience with supporting the company in every area of licensing and compliance.

▶ NY-License Situation, AML Audits, Outsourced Compliance Officer

Assisted company in obtaining NY license in a difficult situation, filled a key AML compliance role, and conducted reviews for years.

Coverage of states & connections

- ▶ Experience with all 54 states and U.S. Territories. We are very well-connected to state regulators throughout the country.

Crossing the Pond? An Overview of International FinTechs Entering the U.S. Market

Updated by Patricia Lagodzinski, Source Material Compass 2016



Technology is transforming the way purchases and payments are processed all over the world.

As technology advances, FinTech companies are opening channels within and between countries for faster and more convenient payments between individuals and institutions, including online, mobile automated, and peer-to-peer payment processing systems that handle both traditional and cryptocurrencies. FinTech companies from Europe and beyond are increasingly interested in opening channels into the lucrative U.S. market.

Legal and regulatory issues often represent an initial and ongoing hurdle to product launch and success both in Europe and in the U.S. In the U.S., financial services laws and regulatory compliance in this area can be difficult due to a complex and antiquated mix of state, federal, and international obligations. The following overview compares the environment for FinTech companies in the U.S. with the United Kingdom (U.K.)/ European Union (E.U.).

FinTech Environment – From E.U. to America

Europe has a very straightforward approach when it comes to licensing. Almost every country within the E.U. offers two types of licenses: Registered and Authorized. A Registered license allows an entity to operate from a specific country

within the EU and has a low barrier to entry. An Authorized licensed entity has 'passporting' rights, which means companies can conduct business not only in their country of origin, but also conduct business across the E.U. without having to establish offices or get licensed in other E.U. countries.

E.U. Standardized Approach

In its efforts to standardize the laws and take a pragmatic approach to foster FinTech growth, the E.U. in recent years has introduced a plethora of regulations, from standardized mobile and internet payments (PSD2) to voluntary regulatory framework on bank capital adequacy, stress testing (Basel 3), the Anti-Money Laundering Directive (AMLD), a European-wide initiative to standardize the processing of electronic payments in Euro (SEPA), harmonized regulation for investment (MiFID2), harmonized EU-wide insurance regulatory regime (Solvency2), a set of international accounting standards (IFRS) and now the soon-to-be launched e-invoicing directive requiring all 28 EU member states to use specific e-invoicing standards for all B2G e-invoices by November 27, 2018.

Both the E.U. and individual governments in Europe are using regulation to increase competition in the financial services industry. The idea is that competition will result in higher quality financial products and lower fees for consumers as well as a more robust financial system overall. Additionally, regulators in countries such as the UK, have set up centralized FinTech-specific units.

U.S. Fragmented and Obsolete Laws

Compare this to the U.S. which has 11 major federal regulatory bodies, and have yet to formulate a united approach to FinTech. Moreover, each of the U.S. fifty states, plus territories, has individual financial legislation, which makes expansion and compliance challenging for FinTech startups, as they need to get licensed separately in each state in which they want to operate.

Here are some things to consider:

- ▶ The U.S. Government is a lot more invasive on personal information vs. strong E.U. privacy laws; for example, personal financials, fingerprinting and third party investigative background checks that includes a full credit report.
- ▶ Enhanced beneficial ownership up to 100% of indirect ownership
- ▶ Money services bank accounts are not easy to obtain and have a thorough due diligence process
- ▶ States request monthly, quarterly, semi-annual and annual reports
- ▶ Monthly, quarterly and annual financials (audited U.S. GAAP)

- ▶ Demonstration of a robust BSA/ AML compliance program
- ▶ Cost of licensing - bonding, license application and fingerprinting fees, background checks
- ▶ Timing of licensing
- ▶ Outdated statutes written decades ago geared toward the traditional money remittance model such as Western Union & MoneyGram

With all that said, the U.S. is a large market and one that cannot be ignored. European FinTechs starting up in the U.S. must take a focused approach with adequate resources to build and expend in a vast market.

Market Entry Strategies – What to prepare for and what to expect

When FinTechs from the E.U. decide to make that fateful leap to enter the U.S. market, they need to be prepared for a culture shock. Some of the important things that the decision makers need to consider before they make that jump:

- ▶ The applicant must have adequate financial backup, either through a parent company or venture capitalist/private equity firms to maintain a minimum of \$1.5 million net worth at all times.
- ▶ It is possible for a company to setup a pilot program in select states. This approach can have multiple benefits such as:
 - ▶ Allowing the company to test the market with minimum cost
 - ▶ Allowing the company to test its systems and make sure they are buttoned up
 - ▶ Banks are much more receptive to beta-tested systems for both safety and commercial reasons
- ▶ Another consideration for the U.S. regulatory process is to establish a realistic and conservative business plan and pro formas – this is not your business plan/sales deck that you present to your bank for a loan. The projections in the pro formas need to be more conservative and realistic to regulators. Projected volume and financials will be used to determine bond amounts and general financial, safety and soundness, and fitness for licensure.
- ▶ In addition, location is important in all new expansions, but particularly in the diverse U.S. landscape. Where the company establishes its headquarters will determine its taxation level and ability to attract talent to run and grow the business.
- ▶ Companies need to carefully make the decision to incorporate in the U.S. versus applying as foreign company. Incorporating in the U.S. shows a strong presence and puts regulators more at ease knowing that the licensee is bound

**[The] U.S. Government
is a lot more invasive on
personal information vs
strong E.U. privacy laws.**

by U.S. laws. The state of Nevada, for example, does not allow foreign nationals to serve as control persons without a permit to work in the U.S. (visa, alien card).

In addition to licensing, license application fees, maintenance and bonding fees, the company needs to plan for additional start-up and operational costs.

Plans to Update the U.S. Regulatory Framework

To address the everchanging landscape in the money services industry, in May 2017, the Conference of State Bank Supervisors (CSBS) in the U.S. announced Vision 2020—a series of initiatives to modernize state regulation of non-banks, including financial technology firms. The goal of the initiatives is to achieve a regulatory system that makes supervision more efficient and recognizes standards across state lines – actions that will better support start-ups and enable national scale while protecting consumers and the financial system.

By 2020, state regulators will adopt an integrated, 50-state licensing and supervisory system, leveraging technology and smart regulatory policy to transform the interaction between industry, regulators and consumers. These initiatives will help bring the U.S. regulatory framework up-to date.

A pilot program to streamline the money transmitter licensing process will begin this month—April 2018. Seven states—Georgia, Illinois, Kansas, Massachusetts, Tennessee, Texas and Washington—will allow applicants to submit one application to the participating seven states at one time. The states will collaboratively review the application in a phased approach. The goal is to shorten the review process and streamline the application requirements, as possible.

Moving forward, European FinTech companies, and all international companies, need to carefully consider the trials, tribulations, and costs of the U.S. environment before taking the plunge. Prospective applicants need to remember that licenses cannot be passported from one state to another. The 50-state licensing process, even with current streamlining efforts, is burdensome and time-consuming not to mention the cost of maintaining the licenses across multiple states. However, given the enormous potential and possibilities, companies should take a chance on expanding into the lucrative U.S. and North American market. For questions, please contact Trish Lagodzinski at Trishlagodzinski@chartwell-compliance.com.

FinCEN and Beyond Evolving Regulatory Framework for Virtual Currency

By Sherry Tomac and Trish Lagodzinski

Virtual currency (VC), also known as digital currency, cryptocurrency or altcoin, has and continues to revolutionize the modern financial landscape. Bitcoin is the most widely recognized digital currency. Soaring Bitcoin prices grabbed everyone's attention as prices jumped from \$1 in early 2011 to over \$19,000 per Bitcoin in December 2017. The attention resembles the California gold rush of the 1800's.

Bitcoin issuance started in 2009 with an initial price of about 8 cents per bitcoin. That means, an initial \$100 Bitcoin investment in 2009 would have paid out over \$24M at its peak price in December 2017. Other types of cryptocurrencies, that are making waves in the marketplace include Ethereum, Litecoin, Zcash, Ripple, and Monero. Besides making some investors rich, the attention has increased curiosity, awareness and acceptance of digital currency in the marketplace.

Cryptocurrencies provide challenges to Federal, State, and International governments. There are no central authorities that control cryptocurrencies. Instead, computers "mine" digital currencies using complex algorithms. Digital currency payments can be made anonymously without banks playing the middleman. Consequently, the government does not control how digital currencies are transferred or how they are tracked. Untraceable financial transactions facilitate crime. Money laundering, drug trafficking, terrorism, and other illegal activities all benefit from moving money that is not tracked.

The legal and regulatory infrastructure is catching up with the virtual currency industry. The Commodity Futures Trading Commission (CFTC) has regulated and may continue to regulate

virtual currencies as commodities. The Securities and Exchange Commission (SEC) also requires registration of any virtual currency traded in the U.S. if it is classified as a security and of any trading platform that meets its definition of an exchange. The regulatory structure also includes tax regulations (by the Internal Revenue Service (IRS)) and Financial Crimes Enforcement Network (FinCEN) transparency regulations between financial exchanges and the individuals and corporations with whom they conduct business.



U.S. Federal Regulation

FinCEN

FinCEN was one of the first regulators to address cryptocurrency when it released interpretive guidance in March 2013 stating that an administrator or exchanger of virtual currency is a Money Services Business ("MSB").¹

These advisory rulings essentially said there is no distinction between fiat currency and digital currencies for the purposes of money transmission laws. The virtual currency administrator or

exchanger as a MSB must register with FinCEN, implement a risk-based anti-money laundering compliance program, file suspicious activity reports and currency transaction reports, obtain customer identification information, and comply with other recordkeeping requirements under the BSA unless a limitation or exemption applies.

FinCEN addressed the coordinated Federal regulatory efforts in a February 13, 2018 letter from the Drew Maloney, Assistant Secretary at the U.S. Treasury Department to U.S. Senator Ron Wyden of the Senate Committee on Finance ("FinCEN Letter"). The FinCEN Letter is a summary of FinCEN's "oversight and enforcement capabilities" regarding cryptocurrency, and it mentions regulatory concerns and prior enforcement actions. Although the FinCEN Letter does not refer explicitly to the above Bank Secrecy Act (BSA) regulation regarding MSBs, it appears to talk around the issue in the following language:

FinCEN is working closely with the Securities Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) to clarify and enforce the AML/CFT obligations of businesses engaged in Initial Coin Offering (ICO) activities that implicate the regulatory authorities of these agencies. The application of AML/CFT obligations to participants in ICOs will depend on the nature of lite financial activity involved in any particular ICO. This is a matter of the facts and circumstances of each case.

Generally, under existing regulations and interpretations, a developer that sells convertible virtual currency, including in the form of ICO coins or tokens, in exchange for another type of value that substitutes for currency is a money transmitter and must comply with anti-money laundering/counterterrorism financing (AML/CFT) requirements as a MSB. An exchange that sells ICO coins or tokens, or exchanges them for other virtual currency, fiat currency, or other value that substitutes for currency, would typically also be a money transmitter.

¹ FinCEN Guidance FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, March 18, 2013 (explaining that convertible virtual currency administrators and exchangers are money transmitters under the BSA) [FinCEN issued another advisory on January 2014 on the application of FinCEN's regulations to virtual currency mining operations [2 FinCEN Guidance FIN-2014-R001, Application of FinCEN's Regulations to Virtual Currency Mining Operations, January 30, 2014 (explaining that persons that create units of virtual currency, such as miners, and use them in the business of accepting and transmitting value are also money transmitters)].

CFTC

ICO arrangements may vary. An ICO is an offering or sale of securities or derivatives, therefore, certain participants in the ICO could fall under the authority of the SEC, which regulates brokers and dealers in securities, or under the authority of the CFTC, which regulates merchants and brokers in commodities. The AML/CFT requirements imposed by SEC or CFTC regulations would possibly apply to those ICO participants. The Department of the Treasury, including FinCEN, expects businesses involved in ICOs to meet the BSA obligations that apply to them.

The FinCEN Letter also appears to suggest that, at least in certain cases, cryptocurrency exchanges may be subject to the BSA not because they are MSBs, but because they are broker-dealers, a separate type of “financial institution” subject to the BSA.

SEC

SEC initiated enforcement actions against broker-dealers and mutual funds relating to BSA and AML-related violations, and associated private class action lawsuits, is a topic of increasing concern. Regulators may regard cryptocurrency exchanges which have registered with FinCEN under the 2013 FinCEN Guidance as MSBs also as broker-dealers.

When and whether FinCEN will exercise regulatory authority “will depend on the nature of the financial activity involved” and whether such activity constitutes money transmission under the BSA. The SEC also warned that ICOs often may represent securities subject to regulation to protect the investing public.

The SEC stated that many if not all ICOs involving cryptocurrency represent securities subject to the jurisdiction and supervision of the SEC, and already has filed several enforcement proceedings involving ICOs. The SEC also considers exchanges for cryptocurrency to also be subject to its jurisdiction. Likewise, the CFTC has asserted that cryptocurrencies are commodities subject to its jurisdiction and enforcement as well as cryptocurrency derivative products to control fraud and manipulation in the underlying cryptocurrency spot markets.

IRS

In addition to FinCEN, the SEC, and the CFC, the Internal Revenue Service (IRS) collects information on clients who conducted any transaction equal or greater than \$20,000, which paves the way for potential criminal or civil tax investigations as well as potential money laundering investigations. The Congress is also proposing to expand the definition of “financial institution” under the BSA to include issuers, redeemers and cashiers of “prepaid access devices,” digital currency,” or “any digital exchanger or tumbler of digital currency.”

The most immediate impact of a change in the BSA would be to require cross-border reporting of funds accessible through products covered by the expanded definition of “prepaid access devices” on the Report of International Transportation of Currency or Monetary Instruments (“CMIR”). Under 31 U.S.C. §5316, a person or her agent or bailee must file a CMIR, otherwise known as FinCEN Form 105, when the person knowingly transports more than \$10,000 in “monetary instruments” into or out of the United States. FinCEN’s history of pursuing foreign-located businesses suggests it may exercise its jurisdiction against foreign entities that “do business, in whole or in substantial part within the United States,” associated with ICOs.

DOJ

The Department of Justice (DOJ) has also prosecuted operators of cryptocurrency exchanges for a failure to register with FinCEN as a MSB, and FinCEN has brought civil enforcement proceedings against such exchanges for alleged failures to maintain adequate AML programs and file required Suspicious Activity Reports (“SARS”), among other alleged BSA violations.

U.S. State Regulation

State laws require money transmitters to be licensed. Every state has a list of state licensing requirements that must be satisfied regardless of physical presence in that state. Cryptocurrency companies planning to operate on-line in all states must

satisfy every one of the state’s licensing requirements. Some states have offered guidance to cryptocurrency businesses while others have taken a wait and see approach.

New York is by far the most proactive state. In 2015, the New York State Department of Financial Services established a digital currency-specific license called a “BitLicense.” BitLicense represents the first comprehensive VC regulatory regime in the United States. BitLicense reflects a concerted effort to bring VCs into mainstream financial markets by addressing the myriad of security and integrity issues inherent in the technology.

Providers of virtual currency services operating in New York (in particular, those holding custody of customers’ funds and which exchange VCs for dollars and other fiat currencies) must apply for a specially-tailored BitLicense. To maintain that license, a provider must fulfill various reporting requirements and comply with standards on anti-money laundering, cybersecurity and consumer protection. Obtaining a BitLicense is expensive, onerous and drawn out with a nearly three-year application review timeframe from submission to licensure.

Several states including Texas, Kansas, Florida have passed laws and published official guidance on the digital currency businesses. While some states have incorporated virtual currency into their definitions of monetary instruments and/or mediums of exchange, there is not a consensus on the definition of virtual currency and whether it should be treated as the functional equivalent of traditional fiat currency, or money.

Given the media attention about Bitcoin over the past year, virtual currency has become a constant theme of new state legislation. Some states are looking to regulate virtual currency as money transmission while also carving out specific licensee requirements, such as guidance on how the usual permissible investments requirements would not apply and alternatives, to disregarding the exchange of cryptocurrency from money transmission licensure if the exchange goes towards the obtainment of goods or services. For many states, cryptocurrency is not regulated as money transmission, but what is being done with that cryptocurrency is what could be, or not be, subject to regulation.

International Regulation

Australia

Regulators across the world are also moving to regulate cryptocurrency. Digital currency businesses need to comply with a kaleidoscope of various AML regulatory regimes internationally.

Australia's new legislative guidelines for the operation of cryptocurrency exchanges were introduced on April 3, 2018 and a new regulatory apparatus has formally been adopted as law mandating that digital currency exchange businesses comply with the country's AML/CTF requirements.

From now on, Australian digital currency exchange businesses will be required to register and comply with anti-money laundering/counter-terrorism financing (AML/CTF) laws. Cryptocurrency exchanges must now register and report to the Australian Transaction Reports and Analysis Centre (AUSTRAC). AUSTRAC has issued a document outlining the primary obligations of digital currency exchanges under the new guidelines.

In addition to "adopting and maintaining an AML/CTF program to identify, mitigate and manage money laundering and terrorism financing risks," Australian virtual currency exchanges must "identify" and "verify" the "identities of their customers," keep "certain records for seven years," and report "suspicious matters" and "transactions involving physical currency of \$10,000 or more" to AUSTRAC.

Europe

The European Parliament through the European Council amended the Fourth Anti-Money Laundering Directive to include measures targeting exchange platforms for virtual currencies, such as Bitcoin, as well as prepaid cards. The amendment includes a requirement to provide beneficial ownership information to authorities and "any persons that can demonstrate a legitimate interest" to access data on the beneficial owners of trusts in an effort to deter money laundering, tax evasion, and anonymous funding of terrorism.

India

In India, there is ongoing debate about how to treat digital currency, with some authorities suggesting a complete ban on digital currencies. A complete ban is unlikely; however, regulators continue to evaluate the best way to approach the burgeoning industry. Similar to the U.S., regulators may discuss whether digital currency is a currency, a commodity or a security, the role and oversight of different regulatory agencies as well as assurances that the platforms are secure.

Bitcoin exchanges in India reportedly already are following forms of traditional Know Your Customer ("KYC") rules, and are requiring confirmable identification documentation from users, such as a Permanent Account number or an Indian biometric card, which enhances AML compliance.

International

These international legislative development echo similar AML regulatory requirements in the United States that require digital currency exchangers and administrators to register with FinCEN as money services businesses, and with the various States as money transmitter businesses.

One can expect regular additions and changes to the AML/BSA requirements in developed nations as digital currency becomes more and more of an accepted form of payment for goods and services. Regulators find themselves playing catch-up because the currency changes so rapidly.

Summary

Virtual currency is here to stay, but it is an ever-changing industry. As digital currencies become more commonplace, State and Federal regulators across the United States, as well as regulators in many other countries, will need to modernize their regulatory frameworks. Due to the global nature of the industry, the world is already adapting its existing regulatory structures to the unique aspects of digital currency.

Within the U.S. individual states are working on defining if and how virtual currency should be regulated. At least 11 states have introduced or furthered proposed legislation regarding cryptocurrencies in the current 2018 legislative session. Industry and the compliance community need to keep a watchful eye on the development of new state laws defining and regulating virtual currency businesses.

Virtual currency is the wave of the future and more and more effort is being made to ensure regulatory oversight of digital currency transactions to protect consumers worldwide.

Chartwell can help you navigate this new terrain. For any questions, contact Sherry Tomac at Sherrytomac@chartwellcompliance.com or Trish Lagodzinski at Trishlagodzinski@chartwellcompliance.com.



Sherry Tomac, PMP, Sherry has over 20 years of process improvement experience using Kaizen and lean six sigma tools in operational areas of Chartwell Compliance, Western Union, First Data, and Children's Hospital Colorado. Her experience includes documentation of current and future state processes, staff training, standardization of procedures, elimination of waste, and generation of cost savings. As vice president at Chartwell Compliance, Sherry, manages a highly skilled group of compliance professionals who are skilled project managers and subject matter experts leading and/or working on high profile engagements. Sherry provides project oversight, coaching and training to the Chartwell staff and manages Kaizen process improvement activities within the organization. For more information, please contact Sherry at sherrytomac@chartwellcompliance.com.



Trish Lagodzinski, Trish has more than 20 years of experience in regulatory compliance and state and federal government contracting. As a Compliance Director at Chartwell Compliance, Trish Lagodzinski provides guidance on regulatory compliance matters dealing with state money services business licenses and associated state and federal compliance regulations for non-bank financial services companies. Trish has completed licensing and administration in all 50 states and territories. Prior to joining Chartwell, Trish served as a liaison to federal agencies, a project manager, and a business development specialist at Lockheed Martin. For more information please contact Trish Lagodzinski at trishlagodzinski@chartwellcompliance.com.

Streamlined Licensing Process for Fintech Companies and Money Services Businesses

By Trish Lagodzinski

Fintech companies—firms that leverage technology to create new business models, new delivery channels, automated decisions, and partnerships with traditional banks—perform an important role in financial services. Providing a range of financial products and services including money transmission, cryptocurrencies, debt and consumer finance services, Fintech firms have forever changed the money services industry.



Support Innovation and Startups

Allow new, innovative financial services businesses and ideas to grow and flourish.



Enable National Scale

Allow new businesses to expand nationally with as little regulatory friction as necessary.



Strengthen the Financial System

Encourage ideas that improve financial stability, provide access to underbanked communities, and grow local communities.



Uphold Important Consumer Protections

Ensure that new products and services adhere to existing consumer protection law and do not lead to predatory practices.

“Through Vision 2020, state regulators will transform the licensing process, harmonize supervision, engage fintech companies, assist state banking departments, make it easier for banks to provide services to non-banks, and make supervision more efficient for third parties.”

Charles G. Cooper, Texas Commissioner
Vision 2020 will focus on 6 major initiatives to transform state supervision of non-bank and fintech companies.

To address this everchanging landscape in the money services industry, in May 2017, the Conference of State Bank Supervisors (CSBS) announced Vision 2020—a series of initiatives to modernize state regulation of non-banks, including financial technology firms. The goal of the initiatives is to achieve a regulatory system that makes supervision more efficient and recognizes standards across state lines – actions that will better support start-ups and enable national scale while protecting consumers and the financial system.

By 2020, state regulators will adopt an integrated, 50-state licensing and supervisory system, leveraging technology and smart regulatory policy to transform the interaction between industry, regulators and consumers.

These Six Steps Outline the Plan for Modernization of the State Regulatory System.

1. The Fintech Industry Advisory Panel provides industry input to help states: modernize regulatory regimes; identify points of friction in licensing and multi-state regulation; and discuss a wide array of solutions. The panel will focus on payments and money transmission; lending; and community banks and innovation.
2. Redesigned Nationwide Multistate Licensing System (NMLS) – the common platform for state regulation – will transform the licensing process thru data/analytics; automate most new applicants; and enable states to focus more on higher-risk cases while streamlining state regulation on a multi-state basis.
3. Harmonize Multi-State Supervision by establishing model approaches enhancing uniformity in examinations; facilitating best practices; and identifying and reporting non-bank violations. CSBS is also building a new technology platform for state exams.
4. Assist State Banking Departments, through education programs, analytics and stronger standards, CSBS is helping state departments: identify their weaknesses; put expertise where it is most needed; update supervisory processes; compare and learn from other states; and validate higher performance thru accreditation.
5. Enable Banks to Service Non-Banks, through enhanced industry awareness campaigns to address de-risking practices -- where banks are cautious about doing business with non-banks – CSBS is increasing industry awareness that strong regulatory regimes exist for compliance with laws for money laundering, the Bank Secrecy Act, and cybersecurity.

1

Fintech advisory panel

Identify pain points and possible solutions

2

Redesign NMLS

Enhance re-tech to automate multi-state licensing and streamline supervision

3

Harmonize multi-state supervision

Adopt best practices and drive towards uniform examinations

4

Assist state banking departments

Automate exam process, introduce better analytics, adopt higher standards

5

Redesign NMLS

Attack de-risking and dispel uncertainties of regulatory regimes for BSA-AML

6

Improve third-party supervision

Support federal legislation that improves state-federal coordination

6. Improve Third Party Supervision through CSBS support of federal legislation to amend the Bank Services Company Act to allow state and federal regulators to better coordinate supervision of TSPs and, in turn, produce an easier supervisory experience for Fintechs and other non-banks.

Streamlined Money Transmitter Licensing Pilot

At the tenth annual NMLS Conference and Training in February 2018 in New Orleans, CSBS unveiled two of the key elements of Vision 2020—the redesign of the Nationwide Multistate Licensing System (NMLS) and the harmonization of multi-state supervision.

A pilot program that incorporates both of those elements will begin sometime in April 2018 (exact date to be determined) where the initial 7 states—Georgia, Illinois, Kansas, Massachusetts, Tennessee, Texas and Washington—will begin to test the new money transmitter application process as follows:

- ▶ A money transmitter license applicant submits an application on NMLS. The application will be assigned to one of the seven states in a two-phase process. The Phase I state licensing fee is paid at the time of application submission.
- ▶ The applicant then pays the license application fees for all the seven states.
- ▶ Phase I—the state that is assigned the application reviews the general information—MU1 and MU2s and any other information in NMLS. After 25 days, if approved by the designated reviewing state, the applicant will be approved to submit the application to the other states. If the applicant

passes the Phase I review, the results will be communicated to the Phase II states and the states will begin their state-specific reviews. The licensing fee will be paid to those states at that time.

- ▶ Phase II—When Phase I is completed and the applicant is approved to proceed, the applicant submits all the state-specific items to NMLS/the other states in Phase II, as specified in the state applications including each state's licensing fees.

- ▶ Applicant Requirements: The applicant must be in NMLS and have a complete NMLS record with business plan, financials, Officers MU2s and background checks, IT, cybersecurity, business plan, BSA/AML compliance documents, and all of the baseline information. All of the information will be shared through NMLS. A certain level of financial review will occur at Phase One. Note: Texas **requires** audited financials for all applicants. The states are still discussing information security requirements.

The actual review process will be streamlined and “harmonized.” It is not “passporting” licenses between states because the applicant will not be automatically issued multiple licenses. States will still ask for the state-specific requirements in Phase II. The goal is to create a more uniform licensing process, but to allow states to keep their state-specific regulatory requirements.

The process as described above is being refined and it has not been formalized officially or in writing. The process already exists through NMLS and the states' laws and rules – the participating states are trying to better coordinate the timing of applications to multiple states.



Ashley Tassell, Compliance Director at Firma Foreign Exchange, specializes in AML/CTF Compliance and Financial Services Licensing for Canada, Australia, New Zealand, the United Kingdom and the United States with a central focus on Compliance Regime Creation and Development, including; legal and regulatory research, document writing for policy, procedure, manuals, risk assessments, business process creation and improvement.

Interview with Ashley Tassell, Compliance Director at FIRMA Foreign Exchange

By Richard Davis

Please tell us a bit about Firma Foreign Exchange and its services

AT: FIRMA helps small to mid-size businesses access the global market by assisting them with their foreign exchange and payment needs. What started as a small company out of Edmonton, Alberta Canada, is now a global company with offices across Canada, and in the United Kingdom, Australia, New Zealand and the United States.

Describe what you like most about your current position

AT: I like the opportunity to grow as the company grows. When I started, I was focused mainly on compliance with Anti Money Laundering regulations throughout Firma's offices around the world. As laws have changed, and Firma itself has branched out, I've been involved in everything from setting up licensing in various locations, to compliance with Anti-Spam, Privacy, Bribery, Cybersecurity, and various other laws that have come into play.

How do you see the company changing in the next two years, and how do you see yourself being a part of that change?

AT: As a compliance professional, you know that nothing stays constant for very long. There are always changes, both internally and externally that will make your life interesting. FIRMA is a growing company, and with that growth comes new opportunities and challenges. I am fortunate that the current ownership and management ensures that compliance is a consideration no matter what change occurs at Firma.

What is the biggest challenge you or the company is facing right now?

AT: Right now, Firma is embracing a growth strategy, which involves exploring different ways of meeting our client's needs. This means that there needs to be a lot of research and heavy lifting from all departments, and compliance is not exempt from this effort. I've done a lot of work lately, looking at different products, services, delivery channels, and locations, to determine compliance costs and requirements.

The best piece of advice that you have ever received?

AT: My parents would always tell me that I could be anything I wanted to be...with a heavy dose of reality, by also saying that I would have to work hard for it. It's taught me to not impose rules on myself on what I could or could not achieve, to think outside of the box and understand that the box is just a human construct. If I worked at something hard enough, and long enough, I could eventually get what I wanted.

Note that I'm still trying to figure out how to be a rock star, pro athlete and Batman...but mostly Batman.

Who has inspired you the most throughout your life?

AT: Everyone has that little voice in the back of their heads, often it sounds like their mother, father, or spouse. Mine for some reason sounds like the drill sergeant from Full Metal Jacket. Not sure where it comes from, but it provides the kick in the pants I sometimes need to get off the couch, get out of my comfort zone, and take at least one step forward.

Did you ever have a nick name?

AT: I'm just old enough to be named Ashley before it became popular as a girl's name. To avoid the obvious "I thought Ashley was a girl's name" scenario, I often go by Ash.

Nick names while growing up, were anything that rhymed; Smash, Bash, Crash... I must have been a bit clumsy.

What was your favorite age?

AT: Would it be too much to ask to have everything that I have now, my family, my career, yet get by body from my early twenties...and my hair?

If given a chance, who would you like to be for a day?

AT: To steal a quote "Always be yourself, unless you can be Batman, then always be Batman".

People would be surprised if they knew?

AT: My university degree is in film and media studies. I have a certificate in graphic design. I taught English in Japan for

three years...generally that my background is not what you would expect from a compliance professional.

People usually ask how I ended up in Compliance with my background. I often tell them that I started my university career by studying business but I found that it wasn't challenging for me, so I went with something else. When it came to a career though, business pays better than art, so I worked my way to where I am through hard work and experience.

What did you want to be when growing up?

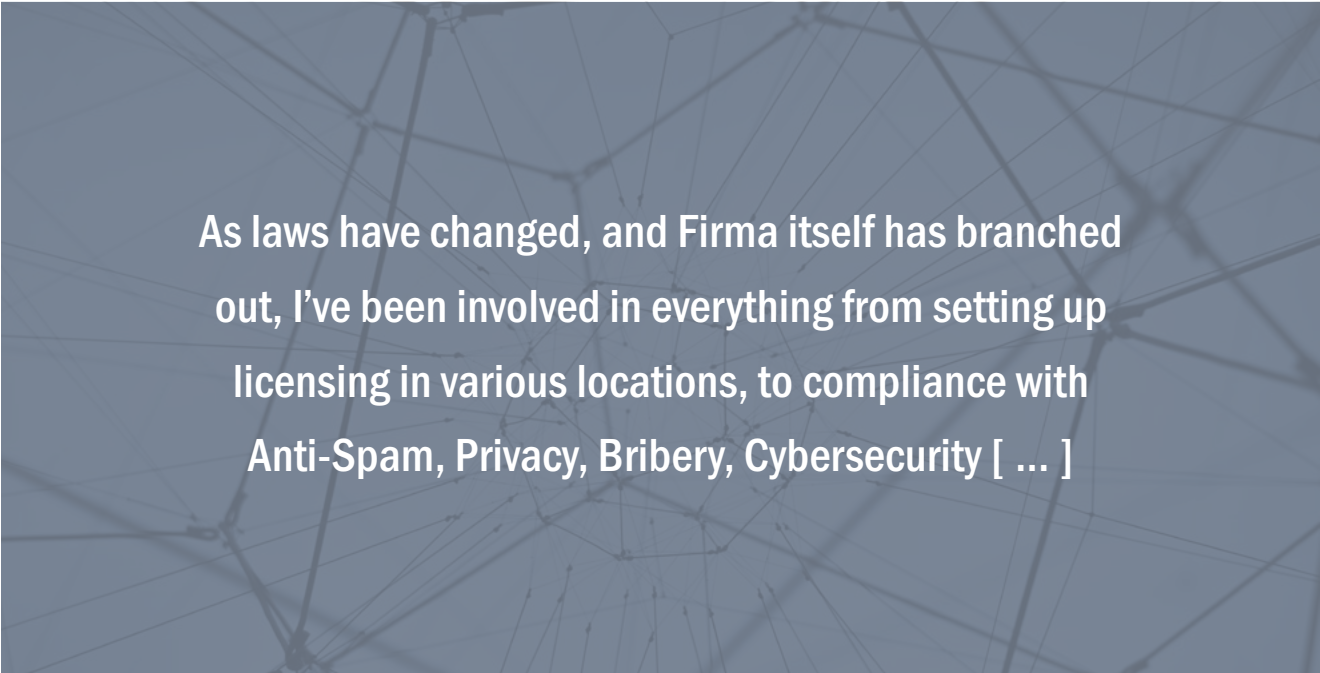
AT: When I was young, I had this thing about being a doctor. That idea remained my motivation for a few years until I realized that being a doctor involved dealing with a lot of disturbing things about the human body. I highly applaud those people who can deal with the constant questions about whether or not a wart looks cancerous, however its not for me. Doctors are much stronger people that I'll ever wish to become.

What's the weirdest thing you've ever eaten?

AT: I have two young kids, a four year old and a one year old. My four year old and I were eating Doritos with whipped cream last week. It was her idea...but not a bad one.

What book did you read last?

AT: I don't get a lot of reading done, other than kids books, therefore I lack any inspirational reading recommendations for this article. Sesame Street's "The Monster at the End of This Book", and Dr. Seuss' "Oh, the Places You'll Go!" are classics though.



As laws have changed, and Firma itself has branched out, I've been involved in everything from setting up licensing in various locations, to compliance with Anti-Spam, Privacy, Bribery, Cybersecurity [...]

Canada's AML Climate Heats Up

By Matt McGuire

Nearly 20 years after its implementation, parliamentary committees conducting a mandatory 5-year review of Canada's AML regime have uncovered reports criticizing major banks for their lax suspicious transaction reporting practices. It is posited that those practices and weaknesses in enforcement and prosecution have hampered Canada's abilities to seize and forfeit criminal proceeds. The review five years before found significant weaknesses, with an average of only 11 money laundering prosecutions a year for public annual spend of nearly CAD 100 million. Hope may be found in the appointment of FINTRAC's new Director, Nada Semaan, a veteran of the Canada Border Services Agency, and FINTRAC's reinstated program to levy administrative monetary penalties.

Immediately preceding the committee hearings, Canada's Finance Department proposed vast changes to the regime as a means to frame the review. Some of those changes were designed to address FATF-identified weaknesses, including issues in enforcement, the vulnerabilities of the legal profession (which won the right to exemptions from AML responsibility in our Supreme Court), other high-risk businesses and professions not covered by our legislation, and significant issues with beneficial ownership standards.

Finance has proposed the inclusion of new classes of entities which would have responsibilities under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), including those involved in: white label ATM operation; parti-mutuel betting and horse racing; mortgage and title insurance; land registration; non-federally regulated mortgage lending; finance, leasing and factoring; armored cars; and high value goods dealers (such automobiles, boats, yachts, art and antiques, and jewelry houses).

To bring lawyers into the fold of the PCMLTFA, Finance has proposed a new class of reporting entity called "Company Service Providers", which would apply to any providers assisting with onshore or offshore company or partnership formation, registered business addresses, acting or arranging for director or nominee shareholders, managing financial affairs or, annual filings.

Also proposed was the expansion of cross-border currency reporting requirements (CBCR). Currently, there are no PCMLTFA reporting requirements for diamonds, gold or other precious metals, prepaid payment products crossing

Canada's borders, all of which are being considered for inclusion in the CBCR regime.

For alignment with FATF standards, Finance has proposed an expansion of the PEP definition, the sectors to which the determination requirements would apply, and mandatory PEP determinations for beneficial owners.

American AML professionals will be used to criminal prohibitions against structuring transactions to avoid reporting, record-keeping and identification requirements. No such prohibition exists in Canada, yet, but is being proposed, along with rules prohibiting reporting entities from designing products or services for those purposes.

MSBs and the Canadian MSB Association applauded the


acknowledgement by Finance of the challenge faced by de-risking, which it asserts arises from the "...mistaken belief that financial institutions must know your customer's customer". No potential solutions are offered, but input is solicited by the comment deadline of April 30, 2018.

Canada has made renewed commitments to improve the beneficial ownership situation in the country, through coordination with the provinces. Previous guidance rejecting attestation as a valid

means of beneficial ownership determination is expected to be relaxed in the coming months, at least until a viable alternative is made available by the government.

If history is a guide, proposed changes pursued by Finance may take up to three years to come into force.

Still pending are Canada's long-awaited regulations enabling laws passed in 2014 for "Dealers in Virtual Currency". As a consequence, many crypto companies are in limbo, without the ability to register as money services businesses, and the ire that draws from their financial service providers.



Still pending are Canada's long-awaited regulations enabling laws passed in 2014 for "Dealers in Virtual Currency".



Matt McGuire is a Financial Crime Risk Management Expert based in Canada with the AML shop. He is an internationally recognized expert in anti-money laundering (AML) and counter-terrorist financing (CTF). He has been assisting financial institutions to assess and reduce financial crime and related regulatory risks for fifteen years. He has served as an advisor to the UN as well as Canadian and foreign governments on development of their laws and financial intelligence functions.



Your Money Services Business Independent Review

By Karen Schirmer

Money Services Businesses (“MSB”) know that one of the four pillars of the Bank Secrecy Act (“BSA”) is to have its BSA/AML Compliance Program (hereinafter the “Program”) tested periodically by a qualified, independent party.

The BSA/AML Independent Review (the “Review”) provides valuable feedback to the MSB about the state of its AML Compliance Program, and it is also a document that is requested as part of regulatory examinations and bank-partner oversight. The purpose of this article is to share insights from a Reviewer’s perspective in order to help MSBs prepare for upcoming Reviews. Keep in mind that these insights do not reflect observations from any one client, but rather, are general observations that are cumulative over time.

In the beginning ...

The FFIEC has provided guidance that says a Review is “an evaluation of the overall adequacy and effectiveness of the BSA/AML Compliance Program including policies, procedures, and processes.” It is the Reviewer’s job to evaluate that the Program is designed and implemented to meet the applicable BSA requirements and that the Program is tailored to the MSB’s AML risk profile. Reviewers take this mandate seriously and use the time before, during, and after their on-site review to gather as much information as possible to make copious observations, identify findings, and make best practices recommendations. The initial request for documents provides a roadmap as to what will be reviewed and tested. In fact, much of

the review takes place prior to the on-site. As such, the company’s AML Compliance Officer should take the time to fully review and understand the entire request list and ask clarifying questions as necessary. Providing thorough responses, and current and well organized documents that cover the review period gives the Reviewer more confidence that the Program is being actively managed. The Reviewer generally performs transaction testing and the transaction data is requested as early in the process as possible. The Reviewer determines the most appropriate testing method and works with the MSB on the sampling concepts commensurate with the risks, and the best way to produce the data in a secure manner that identifies the relevant fields and can be easily queried.

Reviews involving multiple products

A Reviewer needs to have a clear understanding of the products and services that are offered under the Program. Many companies have multiple product offerings wherein some of these offerings are regulated under the BSA while others may not be. Further, some MSBs choose to cover their regulated and nonregulated products under one

Program, while others only cover the regulated products. Be prepared to educate the Reviewer through product descriptions, business plans, funds and data flows, legal memorandums, regulatory guidance, and other materials that explain how the products operate and how they are managed under BSA.

Program best practices

The Program is often in the form of a manual that is maintained by the AML Compliance Officer and his/her team and approved by the Board of Directors. However, the Program belongs to all employees and sets the tone for the MSB's culture of compliance. FinCEN's 2014-A007 advisory provided valuable feedback that, while AML sanctions are specific to individual institutional practices or lack thereof, the common thread among sanctioned companies (large and small) has been that they lacked a strong culture of compliance promoted from the top down. We, at Chartwell, recommend that the Program be shared with all employees. An effective way to accomplish it is by providing each employee with a copy of the Program as part of the training process and/or making the Program accessible on an intranet site and obtaining an employee acknowledgment.

Strengthen your program

1. Practical steps to strengthen your written Program:

- ▶ Include a description of all applicable BSA requirements in the Program manual. This demonstrates to the regulators the company's knowledge of its responsibilities and commitments. Further, if the requirements are not stated, there is a greater chance that there may be gaps in the corresponding procedures and controls.

- ▶ Include roles and responsibilities of board of directors, senior management, compliance officer, and employees, in the Program manual. Doing so establishes stronger accountability and engagement at all levels.

- ▶ The Program may describe multiple levels of procedures and

training; however, the detailed Standard Operating Procedures (SOPs) are best maintained separate from the Program to allow for changes without the need for Board approval. SOPs are most effective when they contain sufficient detail to know who, does what, when, with what frequency, and how. Procedural documents should be dated and trained to appropriate personnel. Reviewers test to make sure that procedures are being followed so that the practice mirrors what is documented. It is sometimes the case that when procedures are included in the Program and not provided to employees as separate documents, the implementing operations team is not aware of the procedures in the Program.

- ▶ For MSBs with non-U.S. parent companies, it is best that the U.S. entity has its own Program rather than combine the two. Bank partners and regulators consider it a best practice.



2. Compliance Officer:

All MSBs must have a designated AML Compliance Officer ("CO"), and regulatory guidance clarifies that the CO should be appointed by the MSB's Board of Directors ("BOD"). The appointment can be documented in a resolution of the BOD or included in the minutes of a BOD meeting. Your CO must have sufficient AML experience and receive ongoing AML training. Also, some states have experience requirements for the AML Compliance Officer position. Check your organizational structure to make sure your CO has:

- ▶ Sufficient independence from business decisions;

► Access to the BOD; AND

► Sufficient systems, authority and resources to implement an effective program.

3. Policies and Procedures:

Policies and Procedures are in writing and a best practice is to have three levels:

► High-level policies and procedures of the Program;

► Detailed SOPs for operational teams such as procedures for investigations and enhanced due diligence; and

► Desktop procedures that are job-specific and may contain forms or screenshots of system pages with detailed instructions.

Other useful tips include:

► For each regulatory requirement, there should be a procedure with assigned accountability. For instance, while the Customer Identification Program (“CIP”) is a regulatory requirement, a member of the company’s underwriting team may perform the identification verification tasks. The underwriting team should be designated as the control owners for the CIP requirement.

► Chartwell highly recommends a Quality Assurance procedure for each regulatory control. For instance, suspicious activity monitoring is a control. Provide procedures for timing and documenting of investigations, making determinations and reporting. Sample and test decisions on a periodic basis depending on volume to assure that procedural steps are being followed and properly documented.

► Include exception procedures so that employees understand acceptable deviations from procedures and know the escalation process.

► Each procedure should have a change history page, owner, approver, date approved, effective date if different from approved date, and either training or communication

date. Documenting this information provides Reviewers and Regulators the opportunity to see how procedures have changed to adequately sample and test the Program.

4. Risk Assessment best practices:

A company’s Risk Assessment must be tailored to the distinct products/services and unique industry of that company. While that may sound obvious, sometimes the Risk Assessment is too generic, and, as such, the company may not have sufficient risk mitigations in place. The tips below provide ways to develop or enhance your AML Risk Assessment process:

► The methodology for calculating risk should be clearly explained in your written Risk Assessment.

► Your Risk Assessment should be reviewed and approved by the Board of Directors initially and periodically.

► Your Risk Assessment is a living document. Occasionally, an MSB may not want to acknowledge “high risk” elements within its Risk Assessment for fear that bank partners or regulators will interpret high risk as a weakness. We suggest a different perspective in acknowledging high risk elements within your Program. When you work through the risk assessment process, you have the opportunity to identify risks, which provides the ability to implement appropriate resources and systems. When you document this process and discuss implemented mitigation factors, you actually demonstrate the strength of your Program to bank partners and regulators. Testing and subsequent adjustments to residual risk levels further demonstrate the depth of your Program as well as the comprehensiveness of your risk assessment process.

5. Data Testing (Suspicious Activity Monitoring, Customer Identification Program, Due Diligence):

► Be prepared to provide data for data testing, which may be applicable to any procedure, requirement, or control. Raw data is requested for various purposes: to test various limits;

to see if suspicious activity rules hit; to look for patterns; to test recordkeeping requirements; to test data integrity; or, to test due diligence procedures, etc.

► Know your CIP requirements – set up and review any third-party systems as your vendor may not know the requirements for your products. CIP dictates what to collect for customer identification. The proof of CIP and its verification has to comply with the recordkeeping requirements as well.

A company’s Risk Assessment must be tailored to the distinct products/services and unique industry of that company. While that may sound obvious, sometimes the Risk Assessment is too generic, and, as such, the company may not have sufficient risk mitigations in place.

► Do you have a gap between what you say you are going to collect/verify for due diligence and what is actually collected? Remember, credit risk and knowing your customers are different. If a particular verification step is optional, say so in the procedure.

► Suspicious activity rules and alerts should be analyzed for effectiveness. Some companies get too many alerts and have a long backlog for reviews.

Other companies' rules rarely generate an alert, and therefore the parameters may need to be refined.

► Investigation steps and standard documentation language should be established and sampled to make sure the procedures are followed and documentation is consistent.

6. Third Party Oversight:

Oversight Programs for third parties that are instrumental in the sales, operations, or controls for your business are essential. Third parties may include Agents, Independent Sales Organizations, Foreign Correspondent Financial Institutions, contractors, vendors, and more. The initial due diligence must

be done consistently, whether the third party is large and well known or a small operation. If the third party has a role in meeting your regulatory obligations, make sure that a thorough and consistent review is done based on risk and at least annually.

7. Suspicious Activity Reports ("SARs"):

As we all are aware, an improvement regarding SAR elements in the narrative section is always ongoing. Here is a useful tip: develop a SAR narrative template that provides a flow for how to organize the critical facts, circumstances, parties, and dates. Succinct chronologies are necessary; so, highlight what happened, when, roles of the key parties, identification numbers and

dollar amounts, and why the activity is deemed to be suspicious. Without this structure, there is a tendency to leave out important details, convey speculation instead of facts, and use internal acronyms or phrases that are likely unfamiliar to the party reviewing the filed SAR. Program Reviewers, state, and federal examiners test the 30-day filing deadline. It is a best practice to include data in the investigative notes and in the SAR that explains when the activity became suspicious. The requirement states that a SAR must be filed with FinCEN no later than 30 calendar days from the date of the "initial detection" of facts that may constitute a basis for filing a SAR. The time period for filing a SAR starts when an MSB, during its review, or based on other available information, has firm reason to suspect that the activity or transactions under review meet one or more of the definitions of suspicious activity. The phrase "initial detection" should not be interpreted to mean the moment a transaction is highlighted for review as well as the date on which the transaction occurs. There are a variety of legitimate transactions that could raise suspicion simply because they are inconsistent with a customer's historically "normal" activity. As such, each MSB should set and communicate its decision-making standards and the initial detection date should be included in its SAR and back-up documentation.

8. Training:

Most MSB's provide to its employees good, basic AML training on at least an annual basis. The following list provides suggestions for improving your AML Training content and recordkeeping:

- Include all relevant BSA requirements in the training.
- Tailor the examples to your MSB's product offerings. If your company purchases an off-the-shelf AML training module, make sure you can tailor the content. Too many trainings use examples of suspicious activity for products, such as money transmission or sale of money orders, when those products are not offered.
- Include in the training all relevant instructions (e.g. where to locate



the Program, Standard Operating Procedures, compliance forms, what to do if something suspicious is detected, relevant time frames, and how to contact the AML Compliance Officer, etc.).

- ▶ Incorporating a test of the training content is a best practice. Use quality assurance testing to validate that the questions cover the important points for the audience, and that the questions and answers (if multiple choice) are clearly written.

- ▶ Review your training audience each year. Some companies train all employees. Others select departments, and leave out key personnel such as senior managers, and Board members. Anyone who “touches” a regulated product in the course of performing their duties should be included in the AML training audience. This may include finance, operations, IT and other shared services.

- ▶ Training records must be maintained for 5 years. Training records include the course content, attendance records, hire date and test scores if applicable. If your company’s policy says that new hires are trained within a certain timeframe from date of hire, an internal control should be set up to assure that the training occurs timely. Training records should be maintained in a location including all Program records and not in an individual’s files.

- ▶ Human Resources and senior management must support the completion of AML training as a performance matter.

9. OFAC:

OFAC laws, rules, and regulations are separate and distinct from the BSA. While a BSA Program must include OFAC compliance, it may be appropriate to have a separate OFAC Program and OFAC Risk Assessment, since OFAC applies to all dealings of U.S. Persons and not just to those within the scope of the BSA. OFAC reports must be timely filed and maintained for five years. Companies frequently have good systems for initial screenings, but fail to screen certain databases, such

as employee lists, against updates. As most MSBs use some type of interdiction software or proprietary screening method, it is very important to test OFAC controls regularly. The following is a short list of tests you can perform:

- ▶ Test the filter using names from the SDN and other lists, including AKAs, and common misspellings.

- ▶ Test your data integrity. For instance, does your system pull in titles (i.e. Dr. or Mr.) that would cause you to miss a potential match? Does your system limit characters such that names would be cut off? Are abbreviations used inconsistently?

- ▶ Test your blocking controls to make sure that once a transaction is blocked

for OFAC reasons, it cannot be released without the proper authorization (usually AML Compliance or Legal).

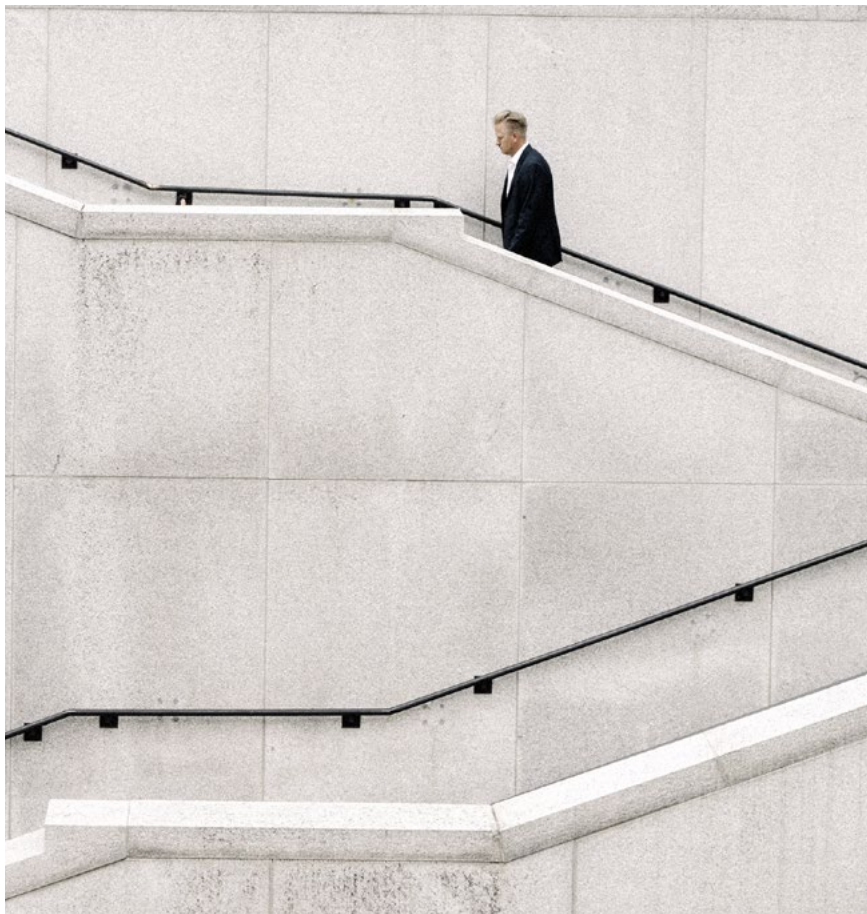
- ▶ When the OFAC list is updated, test to make sure that the updates (adds and deletions) were made.

10. Other:

Know your BSA requirements and be prepared to show proof of compliance, which may include CTRs, FBARS, CMIRs and others not specifically addressed in this article. In summary, each Review is unique in its own way. Chartwell’s goal is to provide Independent Reviews that not only meet the BSA requirement, but also provide valuable feedback and best practices to improve the AML Compliance Program.



Karen Schirmer has over 18 years of experience directing Compliance teams, and drafting programs that identify requirements, risks, controls and methods of control validations. During her work as Compliance Director for Western Union, Inc. and Integrated Payments Systems Inc., she conducted independent reviews, and coordinated regulatory examinations. As part of the First Data leadership team for 10 years, she drafted and directed the operations of the 2012-2013 Global Corporate Compliance Program. For more information, please contact Karen at info@chartwellcompliance.com.





Points to Ponder

Regulations & Rules + Interpretations & Applications

Virtual Currencies Are Commodities, Us Judge Rules

Virtual currencies like bitcoin can be regulated as commodities by the U.S. Commodity Futures Trading Commission, a federal judge ruled in March 2018. U.S. District Judge Jack Weinstein in Brooklyn ruled that the CFTC had standing to bring a fraud lawsuit against New York resident Patrick McDonnell and his company Coin Drop Markets, allowing the case to go forward. Weinstein also entered a preliminary injunction barring McDonnell and Coin Drop Markets from engaging in commodity transactions. McDonnell, who is representing himself, declined to comment on the decision. The CFTC, which is tasked with regulating commodity, futures and derivatives markets, first determined that virtual currencies, also known as cryptocurrencies, are commodities in 2015.

Weinstein upheld that determination, saying it was supported by the plain meaning of the word “commodity” and that the CFTC had broad leeway to interpret the federal law regulating commodities. In its lawsuit, announced in January, the CFTC said that since about January 2017, McDonnell and his company fraudulently offered customers virtual currency trading advice.

Icos Likely Subject To Money Transfer Laws: Fincen

Initial coin offering (ICO) operators have long known that they risked running afoul of US securities laws. However, a newly released letter drafted by an official with the Department of the Treasury suggests that ICOs may also be subject to criminal statutes governing money transfer businesses. The letter, which was addressed to Senator Ron Wyden (D-OR) and dated February 13th released on April 3rd, 2018, said that companies that sell “convertible virtual currency” must comply with bank secrecy and know-your-customer guidelines, rules which were put in place to combat money laundering and terrorism financing.

From the letter:

“Generally, under existing regulations and interpretations, a developer that sells convertible virtual currency, including in the form of ICO coins or tokens, in exchange for another type of value that substitutes for currency is a money transmitter and must comply with AML/CFT requirements that apply to this type of MSB [money services business].”

Peter Van Valkenburgh, director of research at Coin Center, wrote in a blog post that he believes this interpretation of the Bank Secrecy Act is “highly consequential” and raises “major licensing problem for ICOs.” In his view, any ICO that involved US residents (as issuers or investors) and failed to register with the Financial Crimes and Enforcement Network (FinCEN) — a Treasury bureau tasked with preventing and investigating financial crimes — could be charged under 18 U.S.C § 1960, a federal felony criminal

statute that carries a maximum sentence of five years in prison. If broadly interpreted, Van Valkenburgh said that this statute could be enforced retroactively and render employees of, and investors in, the business culpable as well.

Generally, under existing regulations and interpretations, a developer that sells convertible virtual currency, including in the form of ICO coins or tokens, in exchange for another type of value that substitutes for currency is a money transmitter

State Bank Supervisors Release New Tool To Help Financial Firms Manage Risk

A new tool to help money services businesses better manage Bank Secrecy Act/Anti-Money Laundering (BSA/AML) risk was introduced by state regulators in February 2018.

The BSA/AML Self-Assessment Tool, developed by the Conference of State Bank Supervisors (CSBS), is designed to reduce uncertainty surrounding BSA/AML compliance. Further, it will lead to more transparency and address risk mitigation practices within the financial sector.

“BSA/AML requirements are vital to thwarting financial crimes, and money services businesses play a major role in minimizing risk,” Albert Forkner, commissioner of the Wyoming Division of Banking and CSBS chairman, said. “State regulators are committed to helping supervised institutions develop and communicate their BSA/AML risk management programs.”

The BSA/AML Self-Assessment Tool is part of CSBS's commitment to de-risk the state regulatory system that oversees banking and non-depository financial institutions. The regulators' focus is on consumer protection, safety and soundness and BSA/AML compliance.

"By helping financial institutions understand and communicate their BSA/AML risk management program in a way that can be easily customized to each institution's risk profile, we are making BSA/AML compliance more efficient and raising the industry's overall compliance level," Forkner said.

State Regulators: Money Services Businesses Do Not Deserve To Be Victims Of De-Risking

State regulators are committed to the responsible oversight of money service business (MSBs) and creating new solutions to keep pace with emerging and evolving risks that may impact the industry.

These actions address a major concern: MSBs are too often the victim of de-risking – a practice in which MSBs are shut out of banking services, said Bryan Schneider, Secretary of the Illinois Department of Financial and Professional Regulation, at a hearing before the U.S. House of Representatives Subcommittee on Financial Institutions and Consumer Credit.

Schneider, who also chairs the Conference of State Bank Supervisors (CSBS) Emerging Payments and Innovation Task Force, noted that state regulators are not just holding MSBs accountable; through CSBS they also are taking the following action: Tracking MSB transactions through CSBS's nationwide licensing system, which shows MSBs were on pace to handle over \$1 trillion in transactions during 2017; Providing self-assessment tools for MSBs to reduce uncertainty surrounding compliance, increase transparency and address de-risking; Soliciting industry input and solutions on financial technology through an advisory panel to help state supervisors streamline and solve licensing and regulation friction points; and Creating a new technology platform designed to transform state examinations and help states respond to increasingly borderless financial markets.

New Study Of Payment Types Lifecycle

Secure Payments Task Force announced its publication of Payment Lifecycles and Security Profiles, educational materials regarding the lifecycles, security characteristics and relevant laws and regulations for most common payments in March 2018. The materials were developed through the collaborative efforts of 200+ task force participants with diverse payments background and security expertise. Payment Lifecycles and Security Profiles can help financial institutions better understand the lifecycle of various payment types and potential improvement opportunities to help strengthen their payment security practices. Payment Lifecycles and Security Profiles provide perspectives related to:

- ▶ The lifecycles of the most common payment types, covering enrollment, transaction flow and reconciliation
- ▶ Security methods, identity management controls and sensitive data occurring at each step in the payment lifecycle
- ▶ Relevant laws and regulations, and other references, as well as challenges and improvement opportunities related to each payment type

CFPB Updated Prepaid Rule Resources


The CFPB posted a notice on March 13, 2018, that it had updated its Small Entity Compliance Guide and the Guide to Preparing the Short Form Disclosure for Prepaid Accounts. The guidance documents and other resources for compliance with the rule (which now becomes effective April 1, 2019), are located on the CFPB's Implementation and Guidance page for the Prepaid Rule.

FTC Annual Survey Of Consumer Complaints

The Federal Trade Commission released the results of its annual survey of complaints reported by consumers in March 2018. While the number of complaints about fraud from consumers dropped in 2017, consumers reported losing more money than they did in 2016, according to the Commission's 2017 Consumer Sentinel Network Data Book. Although reports about debt collection declined between 2016 and 2017, it remained the top consumer complaint category, making up about 23 percent of all complaints. The high number of debt collection reports was due in part to reports submitted by a data contributor that collects complaints via a mobile app. Identity theft was the second biggest category, making up nearly 14 percent of all the consumer complaints. Credit card fraud was the most common type of identity theft reported by consumers. Tax fraud was the second most common type of identity theft reported despite falling by 46 percent from 2016. The FTC also posted blog articles with the top frauds of 2017 and a recap of the consumer complaint data.

Disclaimer: For informational purposes only and not to be relied upon as legal advice.

Chartwell Compliance Shows You the Way



One state regulator with a reputation for strictness, attested to the conscientiousness and efficiency of the Chartwell Compliance team by stating: "I would also like to take this opportunity to say thank you so much for submitting such a complete and thorough application. It is extremely rare (it has actually only happened one other time in the history of our division regulating money transmitters) that we receive an application that does not require us to ask the applicant for additional information!"

"I'm glad I made the decision of getting the services of Chartwell Compliance.

Knowledgeable, open to questions or concerns and more than willing to go the extra mile. I should have hired them long ago."

NYC Credit & Funding, Inc

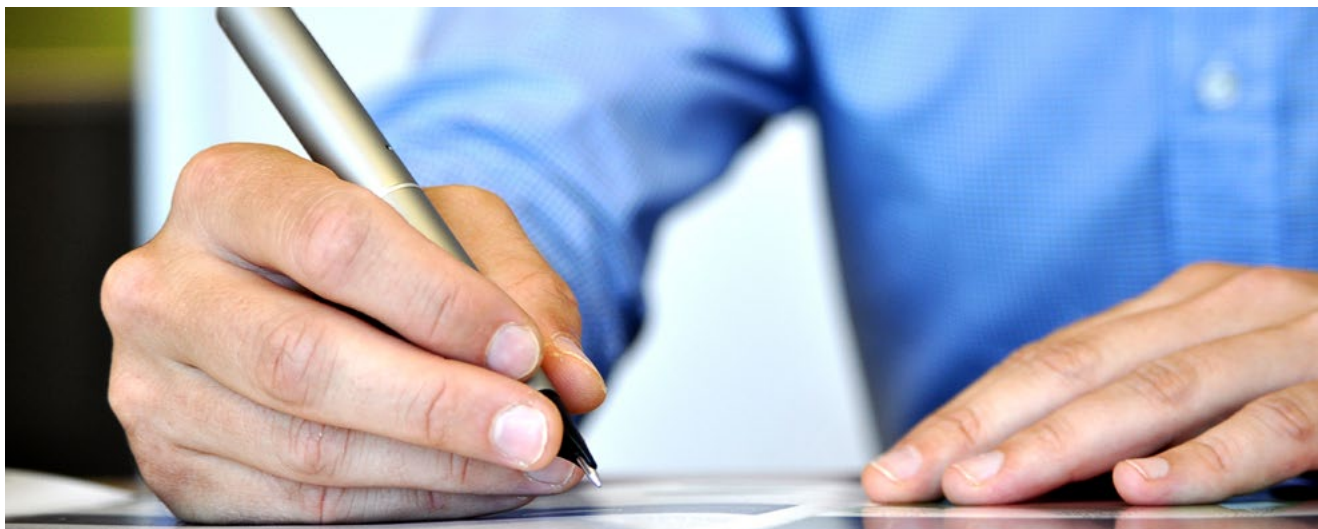
Chartwell Compliance offers all-in-one integrated regulatory compliance and risk management consulting, testing, audit and examinations, and outsourcing services. We serve bank and non-bank financial service providers that are striving to do business successfully in the midst of unprecedented regulatory upheaval.

Chartwell Compliance is attuned to emerging trends, new regulations and rules, and issues relating to the financial services industry. Our consultants believe every client is critically important; and, along with high service delivery standards, coupled with a smaller firm's pricing, allow Chartwell to deliver a value unmatched in the marketplace.

The people of Chartwell have a practical, real-world understanding of regulatory compliance, enterprise risk management, and financial crimes. Chartwell consultants have gained their real-world understanding through numerous years of work as regulators, law enforcement officials, and operators in the financial industry. This allows us to translate compliance in practical ways helping our clients maintain fee revenue; lower operating costs, and proactively anticipate the desires and requirements of a diverse range of agencies and regulators in charge of supervising financial institutions.

Chartwell Compliance, as an all-in-one consulting firm, allows our clients to avoid the burden of managing multiple vendor relationships, making it possible for our clients to realize economies of scale. In addition, our clients gain further value from having a partner with experience and expertise encompassing compliance, risk, and corporate planning. Our consultants are passionate about their areas of expertise and equally comfortable as testers, trainers, or mentors to our clients.

Services



REGULATORY COMPLIANCE Chartwell Compliance provides consulting across nearly the entire range of rules and regulations affecting bank and non-bank financial institutions. Our regulatory subject matter expertise includes but is not limited to: Enforcement action solutions; Bank Secrecy Act (“BSA”); Office of Foreign Assets Control (“OFAC”); Loan Compliance (commercial, consumer, real estate); Deposit Compliance, Home Mortgage Disclosure Act (“HMDA”); Secure and Fair Enforcement for Mortgage Licensing Act (“SAFE”); Unfair, Deceptive or Abusive Acts or Practices Act (“UDAAP”); social media; capital requirements; Community Reinvestment Act (“CRA”); state and federal regulations for money services businesses, stored value, and payment systems.

BSA/OFAC, AML, FRAUD & CORRUPTION Chartwell Compliance brings together some of the country’s most prominent authorities in Anti-Money Laundering and Combating the Financing of Terrorism (“AML/ CFT”) financial crimes and fraud prevention. Chartwell Compliance’s proficiencies include: Counter terrorism financing; anti-money laundering; asset forfeiture and recovery; fraud prevention (corporate and mortgage); Foreign Corrupt Practices Act and the UK Bribery Act; forensic

accounting; foreign government advisory on AML/CFT regulatory regimes. Chartwell Compliance provides a wide variety of related services including: Training and seminars; enforcement action solutions; comprehensive look back reviews; policy and procedure development; independent reviews; risk assessments; investigations and due diligence, expert witness services; and non-legal opinions.

STATE MONEY SERVICES BUSINESS LICENSING Chartwell Compliance assists money services businesses such as prepaid access providers, currency exchangers, check-cashing companies, e-wallet service providers, and mobile technology companies in applying for and maintaining state licensure requirements. We offer first-hand experience, reasonable non-legal pricing and additional value in being able to assist clients with related areas such as AML compliance and corporate planning. Chartwell Compliance provides services tailored to fit the specific needs of each MSB including: preparation and submission of state license applications: FinCEN/FINTRAC registrations; administration of existing state license portfolios including renewals, periodic reporting, and other requirements; assistance with state regulatory exams and related remedial work;

and non-legal regulatory opinion relative to licensing and regulatory requirements.

DUE DILIGENCE AND INVESTIGATIONS The team of former senior law enforcement and regulatory officials and private sector executives of Chartwell Compliance permits Chartwell to undertake due diligence and investigation activities in a range of areas in the U.S. and overseas. We also offer assistance to institutional investors and other companies conducting corporate due diligence on investment, merger, and acquisition targets.

OPERATIONS & GOVERNANCE Many Chartwell Compliance consultants have experience in corporate operations, planning and leadership. Chartwell Compliance provides consulting services in all of these areas, as well as, providing clients with services such as: Assessments and recommendations; enterprise wide risk assessments; key indicator dashboards; policies and procedures; employee training; board of directors training, and other services.

Strategic Alliances

Chartwell Compliance welcomes relationships that deepen the value provided to our mutual customers. In particular, Chartwell Compliance has a select number of strategic partnerships with leading service and software providers in the financial sector seeking a trusted source for referrals, thought leadership and feedback on new products from the perspective of regulators, law enforcement officials and former practitioners. Some of our alliances include:

- **Fiserv, Inc.** (NASDAQ: FISV) is the leading global provider of information management and electronic commerce systems for the financial services industry.
- **BankersEdge** is the online training partner of choice for hundreds of financial institutions nationwide, with a library of over 300 courses that span regulatory compliance, financial skills and professional development.
- **Bankers' Bank of the West** provides high-quality products and services as well as deep industry expertise to more than 300 community bank clients in the western states and Great Plains region.
- **Thomson Reuters** is the world's leading source of intelligent information for businesses and professionals.
- With its finger on the pulse of the financial services, real estate and IT industries, **OnCourse Learning** provides best-in-class education and compliance solutions that help people get started and succeed in their chosen professions.
- Consistently ranked as number one in the space, **NICE Actimize** experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance.
- **First Manhattan Consulting Group** provides strategy, risk management, and marketing services to financial institutions across the globe.
- **IdentityMind** version 2.0 supercharges your compliance. We use digital identities and machine learning to provide a higher fidelity risk-based compliance approach. Our platform continually adjusts a user's risk profile based on their actions, behavior, comparisons with other users, SAR filings and more. The result is more accurate compliance efforts.



Resellers

Owned by Reed Elsevier, **Accuity** is part of BankersAccuity, the global standard for payment efficiency and compliance solutions. Accuity is a leading provider of global payment routing data, AML screening data and software and professional services that allow organizations, across multiple industries, to maximize efficiency and facilitate compliance of their transactions. Accuity maintains authoritative and comprehensive databases globally with a reputation built on the accuracy and quality of our data, products and services.



Consultants

Our team is cross-certified in regulatory compliance, anti-money laundering, testing, information technology and security, and fraud. The diversified experience of our consultants provides our clients with access to experienced examiners, operators, and regulatory policy makers in both the banking and non-banking segments of the financial services market, including some of the most talented and seasoned professionals in emerging payments compliance. This vast, multi-disciplinary experience allows us to help our clients design and implement compliance and risk management programs and practices properly calibrated to address both the current and prospective regulatory environment in an effective manner. As a result, our clients' products and services can be launched more quickly and remain appropriately priced, usable, compliant, and of high value to end users.

Our group includes some of the industry's foremost authorities on regulatory compliance, information security, licensing, and fraud such as:

- ▶ Average of 20 years of experience per professional
- ▶ Former executives and managers from MSBs such as Western Union, First Data/Integrated Payment Systems, MoneyGram, Sigue, and Microfinance International
- ▶ Former senior compliance and risk managers for state and nationally chartered banks
- ▶ Former Chief of the Federal Bureau of Investigation's Financial Crimes and Terrorist Financing Sections
- ▶ Former Office of the Comptroller of the Currency (OCC) Assistant Director of Enforcement
- ▶ Certified AML (CAMS) and regulatory compliance manager certifications (CRCM), PMP
- ▶ Extensive experience working in or with start-ups
- ▶ Long-standing relationships between many team members
- ▶ Certified Identity Theft Risk Management Specialist (CITRMS)



Value Propositions

- One of the best AML/CFT, financial crimes and state license consultancies in the world
- One of North America's best MSB and emerging payments compliance consulting firms
- Very well-rounded practitioners experience
- Nimble, specialized and affordable
- Significantly lower cost, more services, and more practitioners experience
- Entrepreneurial and highly responsive
- End-to-end services and outsourcing
- Free distribution of quarterly technical publication, Chartwell *Compass*
- Strong human and software project administration backbone to keep on time and on budget.

Awards & Honors

Chartwell has been recognized not only for its superior services and dedication to client relationships but also for its commitment to investing in and developing a unique workplace. The backbone of Chartwell success is its expert team that truly embody the Chartwell brand.



Gettysburg Leadership Training



Kaizen training in Japan



Gettysburg Leadership Training



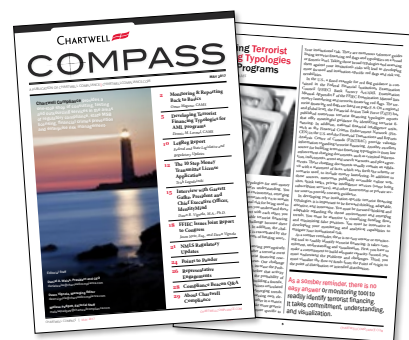
A special thank you to all contributors of Compass. Without your support, our publication would not be what it is today and would not have a readership of over 20,000 subscribers. If you have an article or an idea to submit, please contact Richard Davis richarddavis@chartwellcompliance.com

Request your complementary digital subscription of the Chartwell *Compass* today!

compass@chartwellcompliance.com

Start receiving the latest on financial institution regulatory compliance, financial crime prevention, and risk management issues.

Chartwell grants permission to all subscribers to freely distribute this publication.



CHARTWELL 
REGULATORY COMPLIANCE & RISK MANAGEMENT

6701 Democracy Blvd. Suite 300, Bethesda, MD 20817 | 800.541.6744 | chartwellcompliance.com |



Chartwell *Compass* is intended to provide education and general information on regulatory compliance, reasonable management practices and corresponding legal issues. This publication does not attempt to offer solutions to individual problems and the content is not offered as legal advice. Questions concerning individual legal issues should be addressed to the attorney of your choice.