

COMPASS

A PUBLICATION OF CHARTWELL COMPLIANCE | CHARTWELLCOMPLIANCE.COM

OCTOBER 2022

Chartwell Compliance
delivers powerful solutions to
complex regulatory, licensing, and
compliance challenges experienced
by fintech and financial services
companies. Chartwell has served
nearly 600 firms ranging from
Fortune 50 to fintech's biggest
unicorns throughout the world.



- 3** **Secretary of State Did You Know**
By Karen Elliott
- 4** **Buy Now Pay Later Licensing**
By Dustin Stephans
- 5** **Permissible Investments Plain Talk**
By John Laramie
- 6** **Virtual Currency – What has FinCEN
Been Doing**
By Russ Morin
- 8** **Truth in Crypto Lending**
By Lauren Ceniviva
- 9** **How to Catch a (Domestic) Terrorist**
By Monica Morales
- 11** **Does Fraud have an Age Limit**
By Juan Saa

- 13** **Compliance with a Founder's Mentality**
By Martin Patterson
- 14** **Locational Data and Fraud Monitoring**
By Erik Kemme
- 15** **NMLS Corner**
- 17** **Chartwell Shows You the Way**
- 19** **Services**
- 20** **Strategic Alliances**
- 21** **Chartwell Announcements**

EDITORIAL STAFF:

Daniel A. Weiss. Chairman and Chief Executive Officer,
dweiss@chartwellcompliance.com;

Jonathan Abratt, President and Chief Operating Officer,
jabratt@chartwellcompliance.com;

Richard Davis, Corporate Services Director,
rdavis@chartwellcompliance.com

Chartwell Futures: Blue-Ocean Talent Development, Team Building and Transformation

Chartwell Futures is a collection of programs aimed at sparking personal transformation in ways that have helped make Chartwell Compliance what it is today, winner of multiple industry awards for talent development, culture, and innovation.

Futures experiences provide an enabling environment in awe-inspiring locations where participants can truly appreciate and enjoy the amazing activities and environment, whether it is a coral reef, battlefield, musical, or focused museum tour. These experiences enable participants to be truly present in the moment with one another and better establish lifelong mentorships, professional contacts, and friendships.

Our experiences are augmented by live, webinar-based courses (which in the future we also hope to offer in-person in some cities). These interactive skills classes cover less commonly addressed topics such as fundamentals of emotional intelligence and nonverbal communication; employing kaizen at work and at home; taking and leading action as a social or business entrepreneur; and thinking and writing critically.

Futures also offers a combination of our experiences and courses to companies who are looking to outsource all or a part of their corporate retreat delivery or training and development programs. We integrate elements of our various offerings customized option to fit an organization's needs and to create unique team experiences into a company's corporate retreat or training and development program. The outcome of these custom-built programs aligns with our core mission to spark transformation.

Futures is carving out a blue-ocean genre emphasizing exploration, discovery, and transformation for consumers and companies. We are offering tailored transformational experiences for individuals and organizations.

For more information, visit: chartwellfutures.com or email info@chartwellfutures.com.

CHARTWELL 
FUTURES



Travel to Hawai'i island to set intentions and focus on wellness.



Visit historical battlefields to unearth lessons from the past and apply them to your future.



Reconnect with nature on a dive trip to the Maldives where you'll discuss the relationship of coral reef societies with those of humanity.

Secretary of State: Did You Know?

By Karen Elliot

The Chartwell Compliance Licensing Team assists a variety of clients, ranging from B2B payment providers to virtual currency clients to gaming clients. A big part of the role Chartwell fills is to assist with NMLS requirements. As part of this process, Chartwell Compliance helps with the various Secretary of State requirements. These requirements vary from Certificate of Authority filings to Trade Name filings to Good Standing retrievals. Our team of experts has over 32 years' Secretary of State experience.

Certificates of Authority are legal documents that are filed in states where the entity is doing business. This document grants an entity authorization to do business within that state. Doing business in a state can vary state to state; from having a physical presence within the state, having employees within the state, shipping products in or out of the state, along with others. While Chartwell can assist with preparing and filing the Certificates of Authority, Chartwell cannot provide legal advice. Determining if your business needs to qualify is best decided by a Corporate Attorney or Accountant. Once that determination is made, Chartwell requires specific filing information in order to complete the required forms, either by paper or online. The process then becomes very simple, leave the rest to US!

The first step to file is determining if the name in the domestic state is available for use in the states where the entity will be doing business and filing Certificates of Authority. In order to file in a state, the name of the business must be available for use. If the name is not available for use, the entity is required to include a forced fictitious business name on the Certificate of Authority. This name becomes the name the entity will do business as within that state. Additionally, once the entity is registered to do business within the

state, it might be determined that the entity needs to do business under an alternate, elected name. This name becomes an additional name that the entity can use in a state where they are doing business. Chartwell can assist with both types of filings.

Trade Name or DBA filings are either filed at the state or county level within a state where they entity is doing business. Not all states protect DBA names; some states will allow more than one entity to have the same name, while other states do not. Chartwell can assist on both the state and county levels and can check for name availability to assure the name is available for use. Once the DBA is registered, the entity then has the authority to use that alternate name in the state.

Another requirement to file is finding and appointing a registered agent. A registered agent is a person or entity with a physical address within the state who will accept and forward legal documentation and will also forward any state/government mail. Chartwell

Secretary of State requirements vary from Certificate of Authority filings to Trade Name filings to Good Standing retrievals.

partners with two of the top registered agent companies who not only assist with the registered agent requirement, but also offer other resources, both to Chartwell and Chartwell clients.

After an entity is formed, a Good Standing certificate may be required. For instance, NMLS may require this to be uploaded in the profile on a yearly basis to assure the business is in good standing in the various states where registered. Chartwell can obtain these required documents. A Good Standing might also be needed to close on a transaction or to send to a potential client. Chartwell is here to assist.



KAREN ELLIOTT, SENIOR COMPLIANCE PROFESSIONAL AT CHARTWELL COMPLIANCE has over 17 years of experience in the Public Filings Industry working with the various Secretary of State offices. In addition, for several years Karen also sat on the Board of Directors for the National Public Records Research Association. For more information, contact Karen at [✉ kelliott@chartwellcompliance.com](mailto:kelliott@chartwellcompliance.com).



Buy Now Pay Later Licensing

By Dustin Stephans

Buy now pay later ("BNPL") is a financing tool that is unlocking the buying power of millions of consumers worldwide. The way BNPL works is just how it sounds. A consumer proceeds to submit payment for a particular product, and once at checkout, the consumer will have the ability to buy now and pay later. The BNPL company foots the bill and pays the merchant, while the consumer receives the product. After this, the consumer usually repays the BNPL company in four interest-free payments every two weeks. And so, they received their product now, but pay for it over the course of two months- no fees, no interest.

One of the benefits of this tool is that it doubles the buying power that a consumer otherwise has available. Because the consumer makes their payment to the BNPL company over the course of two months, they are able to leverage two months' worth of income, or alternatively, two months' worth of available credit provided by their credit card. Consumers worldwide are able to purchase items that they otherwise couldn't afford. This unlocked buying power is stimulating spending and therefore increasing revenue across the globe at millions of online merchants. How has the market responded- do consumers actually like this payment option? The answer is yes. Online spending exploded during the pandemic and so did 'Buy Now Pay Later'. 'Payment volume grew 230% from January 2020 through July 2021', and BNPL's global market share is expected to double by January 2024, according to Forbes.

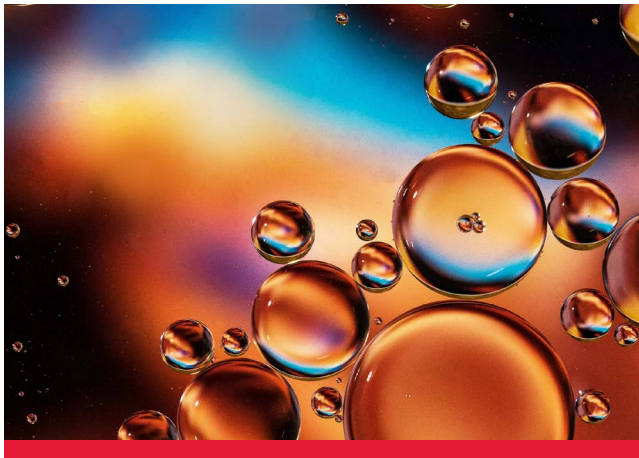
While this business model is layered with highly regulated activity, including consumer brokering and lending, money transmission, debt collection, and loan servicing,

"Buy Now Pay Later" doubles the buying power that a consumer otherwise has available. ... This unlocked buying power is stimulating spending and therefore increasing revenue across the globe at millions of online merchants.

It has proved to be highly profitable and promising for the future. Chartwell Compliance is well-equipped to provide expert-level consulting services to acquire and maintain the licensure necessary to support Buy Now Pay Later business models.



DUSTIN STEPHANS, COMPLIANCE PROFESSIONAL AT CHARTWELL, serves in Chartwell Compliance's License Acquisition team. In the 8 years prior to joining Chartwell, Dustin held numerous positions in both the U.S. Army and in the private sector at a licensed lending company. In the U.S. Army, Dustin served as a Financial Operations Officer and Senior Officer Candidate, and in both roles was responsible for the logistical planning and execution of financial based operations. For more information, contact Dustin at [✉dstephans@chartwellcompliance.com](mailto:dstephans@chartwellcompliance.com).



Permissible Investments Plain Talk

By John Laramie

In the money transmission industry, permissible investments (PI) regulations provide essential liquidity requirements to protect customers. Unfortunately, the variety and disparity in states' PI regulations create confusion for licensees, and money transmitters' compliance programs often overlook PI requirements. State money transmitter examiners observe frequent non-compliance in PI reporting and adequate maintenance of PI. Examiners often cite PI related findings with licensees in new industries, such as fintechs and virtual currency service providers. However, long-licensed money transmitters also exhibit difficulty in PI compliance. Despite the obstacles, state regulators prioritize PI as an essential component of oversight, with which money transmitters must prioritize compliance.

Firms often fail to understand the purpose or applicability of PI, resulting in deficient reporting and, in some cases, insufficient maintenance. So what is PI, and why do state regulators place so much emphasis on it? Basically, PI regulations enforce liquidity requirements for licensed money transmitters to safeguard customers' funds. Clients must maintain low-risk and highly-liquid assets to fulfill obligations to customers. As a simplistic example, if a customer provides \$100 dollars with transmission instructions to a money transmitter, the company must safely maintain \$100 dollars until the fulfillment of the customer's instructions. States allow certain low-risk and liquid assets as "permissible" methods to hold customer funds until fulfillment. Money transmitters demonstrate adequate PI by preparing reports showing the amount obligated to customers, or transmission liability, and the corresponding PI to meet or exceed those obligations.

States enforce PI requirements with good intentions, but often enact complicated rules for a wide variety of transmitter business models operating across our complex financial system. To further complicate the issue, different states possess varying, and sometimes conflicting, PI regulations for reporting and maintenance. States may require PI greater than customer obligations at any point in time, at months'

end, or calculated on an average of daily customer obligations over a designated period of time. States may require quarterly or monthly preparation of PI reports, but not submission, while others require preparation and submission. States might require specific PI reporting forms, and others provide suggested templates for guidance. States also vary on allowable, or permissible, investments such as surety bonds penal sums, authorized delegate receivables, or ACH and card receivables. And in all that variety, licensees must also complete the generic PI portion of the NMLS quarterly call reports. This regulatory complexity can make demonstrating PI compliance difficult for transmitters, especially for those licensed in numerous jurisdictions.

Firms may also allow PI compliance to slip through the cracks by failing to recognize the requirements and assign responsibility within the organization. Money transmitters designate compliance officers and departments to oversee responsibility for Bank Secrecy Act (BSA) and Anti-money Laundering (AML) requirements; however, states' PI doesn't fall under federal BSA/AML laws. As a result, firms may fail to assign PI responsibilities to BSA/AML compliance teams. A company's financial and accounting departments may maintain the information required to monitor PI levels and produce reports, but companies may not assign responsibility for regulatory compliance to accounting staff. This regulatory limbo often results in negligence of PI requirements until states conduct licensing examinations, then licensees often scramble to scrape together PI reports at the last minute, and inevitably incur violations.

States prioritize financial protection for the customers of money transmitters. PI regulations provide essential protections for customers' money, and states will continue oversight of PI maintenance

Permissible Investment regulations **provide essential liquidity requirements** to protect customers.

through company reports and the examination process. Licensed money transmitters must take steps to ensure compliance.

- ▶ Become familiar with the PI rules in all jurisdictions of licensure, and how they apply to the company's products and services.
- ▶ Designate a responsible staff member or department to monitor PI maintenance and prepare reports.
- ▶ Document PI reporting and maintenance in written policies and procedures to ensure consistent, and explainable, reporting for submitting required states' reports, NMLS call reports, and license examinations.
- ▶ Communicate with state regulators when questions arise (and they will).

Chartwell Compliance empowers financial institutions, such as money transmitters, with guidance to navigate the complex and evolving regulatory landscape. Our team of compliance professionals provide trusted advice for licensing and registration, development and implementation of policies and procedures, and ongoing maintenance of regulatory requirements



JOHN LARAMIE, COMPLIANCE DIRECTOR AT CHARTWELL and the functional lead for Chartwell's License Maintenance team, brings over 15 years' experience in organizational development and leadership, including program management, governance, policy writing, and training administration, and has extensive knowledge and expertise in Money Service Business (MSB) regulatory compliance. For more information, contact John at [✉ jlaramie@chartwellcompliance.com](mailto:jlaramie@chartwellcompliance.com).



Virtual Currency— What has FinCEN Been Doing?

By Russell Morin, CAMS

FinCEN has been active in its proposals to regulate convertible virtual currencies or ("CVC"), sometimes referred to more generically as cryptocurrencies and digital assets. While the high growth in this space has paused, the rulemaking has not which leaves many wondering where FinCEN is on its pursuit of the appropriate regulatory framework. Within the last decade, FinCEN has published advisories and guidance and rule proposals concerning how the Bank Secrecy Act ("BSA") regulatory structure applies to CVC. Other federal agencies are also interested in adding regulatory requirements. The IRS, for example, now requires taxpayers to answer "Yes" or "No" on Form 1040 whether the person has acquired an interest in cryptocurrencies and taxes any capital gains.

WHAT HAS FINCEN BEEN FOCUSING ON?

Let's take a look at some noteworthy FinCEN releases involving CVC:

March 18, 2013: FinCEN Guidance¹

FinCEN, in its first significant issuance relating to CVC, clarified the applicability of the BSA to VC. This release clarified that administrators and exchanger of CVC are MSBs under FinCEN's

regulations, and are money transmitters unless an exemption is available. As such, they are subject to the applicable registration, reporting, and recordkeeping regulations of the BSA.

May 9, 2019: FinCEN Guidance²

In this comprehensive guidance, FinCEN clarified that a transmittal order involving CVC is an instruction to pay "a determinable amount of money," and qualifies as a "transmittal of funds" and thus falls under BSA recordkeeping and reporting rules.

Of great significance to the cryptocurrency industry, the release clarified that the "Travel Rule" applies to CVC transmittals in the dollar equivalent amounts of \$3,000 or more. This requirement presents challenges to some industry participants, such as exchanges, because their systems are not designed to capture or transmit such Travel Rule information.

The high growth in
cryptocurrencies and digital
assets has paused, but the
rulemaking by FinCEN
has not.

Other Key Takeaways:

- ▶ Reaffirmed that administrators and exchangers are subject to the MSB regulations. It also discussed various CVC business models and clarified some of those subject to BSA regulations based on applicable facts and circumstances. For example, how the use of wallets may fall under FinCEN/BSA jurisdiction.

¹ www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf

² www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

- ▶ Defined CVC as a medium of exchange that either has an equivalent value as currency, or acts as a substitute for currency, but lacks legal tender status (e.g., Bitcoin). FinCEN has clarified application of the release to Legal Tender Digital Assets ("LTDA") in addition to CVC.
- ▶ FinCEN discussed anonymity-enhanced CVC transactions, for example those involving privacy coins, mixers, and tumblers, are generally subject to the BSA requirements and clarified that companies involved in such transactions do not fall under a regulatory exception.

October 27, 2020: Notice of Proposed Rulemaking (NPR) ³

FinCEN issued this NPR to essentially codifies the previous guidance above and clarifies the meaning of "money" to ensure the rules apply to domestic and cross-border transactions involving CVC. This release addresses key areas of interest to money transmitters including reducing the recordkeeping and "Travel Rule" thresholds for CVC transfers that begin or end outside the United States from \$3,000 to \$250.

December 18, 2020: NPR ⁴

In an effort to close perceived gaps in the regulations when applied to CVC, FinCEN proposed new rules requiring banks and MSBs to submit reports, keep records, and verify the identity of customers for transactions above certain transaction thresholds involving CVC/LTDA wallets not hosted by a financial institution (referred to as "unhosted wallets") or CVC/LTDA wallets hosted by a financial institution in certain jurisdictions identified by FinCEN.

Other Key Takeaways:

- ▶ Classifies CVCs and LTDAs as monetary instruments under the BSA.

³ <https://www.federalregister.gov/documents/2020/10/27/2020-23756/threshold-for-the-requirement-to-collect-retain-and-transmit-information-on-funds-transfers-and>

⁴ <https://home.treasury.gov/news/press-releases/sm1216>



- ▶ Mirroring CTR requirements, banks and MSBs would be subject to reporting requirements for CVC and LTDA transactions exceeding \$10,000 in value with such reports due to be filed with FinCEN within 15 days of reportable transactions.

- ▶ Banks and MSBs would be required to keep records of CVC/LTDA customers and transactions, including verifying customer identity, when a counterparty uses an unhosted or otherwise covered wallet and the transaction is greater than \$3,000. Some of the information required to be collected includes:

- › Name and address of customer
- › Type of CVC/LTDA used in the transaction
- › Amount of CVC or LTDA in the transaction
- › Time of the transaction
- › Assessed value of the transaction, in U.S. Dollars, based on the prevailing exchange rate.
- › Name and physical address of each counterparty to the transaction

December 2020 FBAR Notice ⁵

FinCEN announced its intention to amend FBAR regulations to include virtual currency as a type of reportable account.

SO WHAT ELSE SHOULD YOU EXPECT?

Even following the effective date of the above rulemaking (expected Fall/Winter 2022), Banks and MSBs can expect FinCEN to continue actively evaluating how the BSA framework needs to be updated to address the growing adoption of cryptocurrencies. It is important for financial institutions to embrace this new regulatory environment and understand the impacts.

Do not hesitate to reach out to a Chartwell representative with any questions you may have regarding this.

⁵ <https://www.fincen.gov/sites/default/files/shared/Notice-Virtual%20Currency%20Reporting%20on%20the%20FBAR%20123020.pdf>



RUSS MORIN, COMPLIANCE DIRECTOR AT CHARTWELL on the fintech compliance team is a subject matter expert on anti-money laundering, sanctions, broker/dealer and payments compliance. Russ has six years of experience regulating fintech and other types of payment companies with the Colorado Division of Banking. In addition, Russ worked in the securities compliance field for over 20 years as both a regulator with FINRA and as a compliance officer for a number of broker/dealer firms. For more information, contact Russ at ✉ rmorin@chartwellcompliance.com.

Truth in Crypto Lending

By Lauren Ceniviva

There is significant ambiguity surrounding the status of cryptocurrency. Is it actually a currency? Or is it a security or a commodity? Despite this uncertainty, entities continue to explore lending activity with cryptocurrencies; in particular, there has been a rise in consumer lending products involving digital currencies. This raises questions about the applicability of consumer protection laws and regulations to these products, especially whether the Truth in Lending Act ("TILA") applies. At present, this remains unclear. As the industry waits for more guidance from the federal agencies, any entity that wants to offer loans involving cryptocurrencies to consumers should proceed with caution and consider the following regarding TILA.

A LOAN'S PURPOSE AND THE "CREDIT" CONUNDRUM

TILA covers extensions of credit when the following four conditions are met: 1) the credit is offered or extended to consumers, 2) the offering or extension of credit is done regularly, 3) the credit is subject to a finance charge or is payable by a written agreement in more than four installments, and 4) the credit is primarily for personal, family, or household purposes.¹ Lenders should have processes in place to identify when a loan involving crypto meets these criteria. In particular, entities should assess the loan's purpose and determine if the loan will be used *primarily* for personally, family, or household purposes. TILA does not set requirements for making this determination, leaving it up to institutions to develop their own processes for identifying a loan's purpose. Whatever methods an institution employs, they should be applied consistently and documented within the company's system of record.

TILA defines credit as "the right to defer payment of debt or to incur debt and defer its payment" but does not further define what "debt" is.² Some entities are lending stablecoin and other digital currencies to consumers, rather than making loans in fiat money. Lenders generally can rely on this definition of credit to determine if TILA applies to the debt that is being repaid. However, without clear regulatory guidance, lenders remain uncertain on whether debts of cryptocurrency should be considered extensions of credit under TILA.

TO BE OR NOT TO BE ... REGISTERED WITH THE SEC

Further complicating matters, is the absence of a regulatory position on whether cryptocurrencies are considered securities or commodities, or what circumstances would require a crypto lender to register with the U.S. Securities and Exchange Commission ("SEC") or Commodity Futures Trading Commission ("CFTC"). There is an exception to TILA coverage for "transactions in securities or commodities accounts in which credit is extended by a broker-dealer registered with the SEC or the CFTC."³ It

should be noted that this exception does not apply to a transaction with a broker registered solely with the state, or to a separate credit extension in which the proceeds are used to purchase securities. Additionally, certain states have separate expectations regarding the treatment of digital currencies as securities or commodities. Lenders should consider whether they are required to register with the SEC or CFTC as a broker-dealer or with any state in which they currently lend or intend to lend to consumers.

Entities should be especially mindful that other crypto lenders have been subject to fines and enforcement action for not registering with the SEC. Cryptocurrency lender BlockFi agreed to pay a \$100 million penalty to settle a case involving its lending product that was determined to be securities lending. Further, because the company issued securities, the SEC also found BlockFi to have been operating illegally as an investment company.⁴

One method institutions have used to determine their SEC impact is the "Howey Test."⁵ The Howey Test refers to the Supreme Court's ruling in the 1946 case SEC v. W.J. Howey Co., which established the four criteria an asset or commodity must meet to be considered an investment contract subject to SEC regulation. While the Howey Test has been used to shield most crypto companies from the "securities" asset boogeyman, this may no longer be a solid legal strategy since the SEC can make an "economic reality" determination on a coin and thus put the operator in legal jeopardy. This would then obligate the crypto lender to register with the SEC anyway.

BEWARE OF VOLUNTARY COMPLIANCE

It is not unreasonable for entities who are unsure of their SEC registration responsibilities to assume that voluntary compliance with TILA is better than non-compliance. However, complying with TILA means extending to and informing consumers of certain rights and protections. Companies that choose to voluntarily comply should not take a "cafeteria style" approach, only picking and choosing the aspects of TILA they want to comply with and disregarding others. Lenders who voluntarily but only partially comply may be found to violate TILA or fair lending laws. Moreover, if consumers are incorrectly informed of rights and protections that are in fact not truly extended to them, it can expose lenders to risks related to unfair, deceptive, or abusive acts or practices ("UDAAPs").

KEY TAKEAWAYS

The applicability of consumer protection laws such as the Truth in Lending Act to loans backed by or disbursed with digital currencies is uncertain. Entities that wish to offer consumers lending products involving crypto should have processes in place to determine whether the loan meets the four conditions for TILA coverage, especially regarding the loan's purpose. Loans in which funds are disbursed in cryptocurrency may not be considered extensions of credit for purposes of TILA compliance, while crypto lenders registered as commodities or securities broker-dealers may be exempted from TILA coverage. Institutions that voluntarily comply with TILA should ensure full compliance to avoid regulatory scrutiny and UDAAP risks.

It is strongly recommended that institutions that want to engage in crypto lending consult with their legal counsel, fully assess their lending product, and take a risk-based approach when making a determination about TILA compliance.

1 <https://www.ecfr.gov/current/title-12/chapter-X/part-1026/subpart-A#>

2 [https://www.ecfr.gov/current/title-12/chapter-X/part-1026/subpart-A#p-1026.2\(a\)\(14\)](https://www.ecfr.gov/current/title-12/chapter-X/part-1026/subpart-A#p-1026.2(a)(14))

3 [https://www.ecfr.gov/current/title-12/chapter-X/part-1026/subpart-A#p-1026.3\(d\)](https://www.ecfr.gov/current/title-12/chapter-X/part-1026/subpart-A#p-1026.3(d))

4 <https://www.sec.gov/news/press-release/2022-26>

5 <https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets>



LAUREN CENIVIVA, CRCM, COMPLIANCE PROFESSIONAL AT CHARTWELL, brings over 10 years of banking and consumer compliance experience to the company. Prior to joining Chartwell, Lauren served as a Subject Matter Expert on the Compliance Advisory Team at Cenlar FSB, the nation's largest mortgage sub-servicer. Her primary responsibilities included developing and reviewing policies, procedures, and borrower communications; researching, validating, and approving client and internal audit findings and remediation plans; as well as conducting regulatory research, and providing regulatory guidance to clients, business lines, and other stakeholders. For more information, contact Lauren at lceniviva@chartwellcomplaine.com.



How to Catch a (Domestic) Terrorist: The Latest Trends in Following the Money Trail

By Monica Morales, CAMS, CFE

While Domestic Violent Extremism ("DVE") activities have trended upwards since 2014, the year 2021 saw a significant increase amid the escalating political polarization in the U.S. which continues to fuel the rise in domestic violent extremism.¹ DVE groups and individuals ("DVEs") pose a significant threat to national security. As such, there is a renewed focus to understand how DVEs are funded.²

There are groups linked to cross-border and transactional activities. However, for the purpose of this article, the focus will be on the money movement of individuals or small groups engaging in the promotion, recruitment, and funding of domestic terrorist attacks.

Terrorist financing patterns have shifted in recent years³ based on how the latest attacks have been executed. Domestic attacks carried out by a lone threat actor are increasingly more common due to the ease and cost of executing attacks while still inflicting significant damage. The use of virtual currencies such as cryptocurrency and digital in-game convertible currencies have allowed DVEs to move funds in ways that make detection increasingly more difficult.

Risk factors that add to the level of complexity when following the money trail for domestic terrorist financing are further complicated by the wide range of online and mobile money transfer services easily accessible to consumers:

- ▶ Financing can be derived from legitimate sources of income such as employment, merchandise sales, or donations for a cause.⁴
- ▶ Domestic terrorism is often self-funded or funded through peer-to-peer transactions.

The use of **virtual currencies** ... have allowed [domestic violent extremists] to move funds in ways that make **detection increasingly more difficult**.

¹ The Center for Strategic & International Studies (CSIS), May 2022, **Pushed to Extremes: Domestic Terrorism amid Polarization and Protest**, <https://www.csis.org/analysis/pushed-extremes-domestic-terrorism-amid-polarization-and-protest>, Accessed Aug. 2022.

² The Washington Post, April 2021, **The Rise Of Domestic Extremism In America**, <https://www.washingtonpost.com/investigations/interactive/2021/domestic-terrorism-data/>, Accessed Aug. 2022.

³ US Department of Treasury, Feb. 2022, 2022 **National Terrorist Financing Risk Assessment**, <https://home.treasury.gov/system/files/136/2022-National-Terrorist-Financing-Risk-Assessment.pdf>, Accessed Aug. 2022.

⁴ House Hearing, 115 Congress, From the U.S. Government Publishing Office, Sept. 2018, **Survey of Terrorist Groups and their Means of Financing**, <https://www.govinfo.gov/content/pkg/CHRG-115hhrg31576/html/CHRG-115hhrg31576.htm>, Accessed Aug. 2022.

- The amount of funds is often moved in small dollar amounts.

Lone threat actors that associate with hate groups are often loosely affiliated and not formal members and typically meet with like-minded individuals online through fringe social media platforms and encrypted messaging services such as Gab, 8chan, Telegram, and Signal,⁵ allowing for collaboration to easily take place in moving funds through peer-to-peer platforms, including crowdfunding websites.

Of particular note, cryptocurrency is on the rise as the currency of choice for several hate groups.⁶ Hatewatch, a part of the Southern Poverty Law Center, identified over 600 cryptocurrency addresses associated with far-right wing extremist groups. Notably, while it is estimated that approximately a fourth of Americans own cryptocurrency, research shows that there is close to "universal adoption" of cryptocurrency with known actors within far-right movements.⁷ As such, following the money associated with domestic terrorist financing may likely have some form of overlap with cryptocurrency, something to keep in mind during the course of an investigation.

In addition to AML red flags that investigators are trained to look for, there are additional red flags associated with domestic terrorist financing to look for when examining transaction activity:

- The frequency and pattern of peer-to-peer activity, such as the

rapid movement of funds in small amounts funneled through accounts likely inconsistent with patterns that would be normal and expected for a typical consumer account.

- Funds derived from donations through or even fees associated to, crowdfunding websites like GoFundMe, Kickstarter, or Crowdfunder.
- Identifiers, amounts, or numerical references in cryptocurrency or fiat associated with certain numbers including 14 and 88, 1488, 8814. Or 13 used in conjunction with either 52 or 90, or 109 and 110, with 110 sometimes combined with 1488.^{8 9 10}
- Use of funds showing the absence of expected personal activity such as paying bills (utilities, rent, insurance, etc.).
- Counterparties involved not just in selling weapons, ammunition, and gear but also merchandise, paraphernalia, and subscriptions.
- Membership fees to groups associated with militias and extremism rhetoric.
- Travel expenses to and/or cash withdrawals in locations within close proximity to rallies, protests, and other events attended by extremist groups.

Know Your Customer ("KYC") is a power tool that financial institutions have at

their disposal when evaluating the financial trail for domestic terrorist financing and should include the use of open-source data to evaluate what so-

"A better understanding of the red flags associated with the funding of terrorism ... gives financial institutions a powerful weapon to use in interrupting the flow of funds."

cial media platforms the user and any related consumer counterparties may be associated with. There may be hidden clues in usernames, email addresses, and transaction amounts that may indicate red flags related to domestic terrorist financing. Understanding what to look for can make the task of following the money for domestic terrorist financing less daunting.

Funding is the lifeline of terrorism. A better understanding of the red flags associated with the funding of terrorism coupled with timely reporting actions in domestic terrorist financing investigations, gives financial institutions a powerful weapon to use in interrupting the flow of funds, which is the best defense financial institutions have in the fight against DVEs.

5 Axios, Jan. 2021, *The Online Far Right Is Moving Underground*, <https://www.axios.com/2021/01/12/the-online-far-right-is-moving-underground>, Accessed Aug. 2022.

6 AP News, Sept. 2021, *Far-Right Cryptocurrency Follows Ideology Across Borders*, <https://apnews.com/article/cryptocurrency-coronavirus-pandemic-technology-business-europe-f7f754fc2c68b0eb0d712239323f26c3>, Accessed Aug. 2022.

7 SPLC Southern Poverty Law Center, Dec. 2021, *How Cryptocurrency Revolutionized The White Supremacist Movement*, <https://www.splcenter.org/hatewatch/2021/12/09/how-cryptocurrency-revolutionized-white-supremacist-movement>, Accessed Aug. 2022.

8 CoinDesk, Dec. 2021, *Bitcoin Adoption Among Far-Right Extremists Leaves Its Mark on the Blockchain*, <https://www.coindesk.com/tech/2021/12/08/bitcoin-adoption-among-far-right-extremists-leaves-its-mark-on-the-blockchain/>, Accessed Aug. 2022.

9 Anti-Defamation League (ADL), *Hate on Display / 1488*, Anti-Defamation League (ADL) Database Symbol Search, <https://www.adl.org/resources/hate-symbol/1488>, <https://www.adl.org/resources/search/84>, Accessed on Aug. 2022.

10 SPLC Southern Poverty Law Center, *Racist Skinhead Glossary*, <https://www.splcenter.org/fighting-hate/intelligence-report/2015/racist-skinhead-glossary>, Accessed on Aug. 2022.



MONICA MORALES, SENIOR COMPLIANCE PROFESSIONAL AT CHARTWELL serves in the Global Outsourcing team. She brings 19 years of private and public sector experience to the company, having worked in financial institutions of all sizes, a state government agency, and at a multi-national energy company. In 2003, Monica began her work life journey in banking and has spent the last 11 years in roles involving financial crime investigations, compliance, and risk management related to the Bank Secrecy Act, Anti-Money Laundering (AML), Anti-Bribery and Corruption, fraud, KYC and CDD due diligence, sanctions, as well as banking operations. For more information, contact Monica at mmorales@chartwellcompliance.com.



Does Fraud have an Age Limit

By Juan Saa

PICTURE THIS

You are a customer service representative, you have been trained on how to make it easy for customers to transact, to have a pleasant experience, to assist them as much as possible as fast as possible, and perhaps in doing so focused too much on the ease of doing business that maybe you miss the little things that turn out to be not so little. The first elder exploitation case I ever investigated is a perfect example of this.

The first case I ever investigated was a result of what appeared to be friendly help from the customer's boyfriend while the customer called to place trades. What started as friendly help over the course of several calls, because he was more educated on the subject, months later became a scenario typical of elder financial exploitation. Soon, with the permission of the elderly customer, the only person handling all transactions and account maintenance on their behalf, was their supposed boyfriend. Fast forward to the time this account was escalated due to concerns of who was giving the instructions and where funds were going, and only after more than half a million dollars had gone to the customer's boyfriend (under problematic circumstances) as permission allowed on these transactions was questionable at best. The only time I was able to speak directly with the customer was to address

her account and question where her funds had gone, only to find out that the boyfriend that was acting on her behalf and that she was helping with some small financial issues, was someone she had never met in person.

"[C]ompanies tend to build a program as a **reaction to fraud** rather than starting with a **proactive approach to prevent fraud** and protect its customers."

While in some situations a customer obtaining basic help is part of normal interaction, perhaps in this case, if more training on the many scams and targeting of elderly individuals along with a list of red flags to look for had been provided to me and other staff, the representatives dealing with this account would have realized sooner that the customer was being coached and taken advantage of over a long period of time. If that had been the case and representatives had identified this fraud sooner, the theft of more than half of her retirement funds would not have been taken by a never seen boyfriend overseas.

In today's age of social media, and in a post Covid era which has made face to face communication almost a thing of the past and isolation much more common, people tend to miss basic red flags in hopes of some continued human interaction, and sadly in many cases, elderly individuals are not only targeted for fraud, but also used as money mules without realizing it.

While the above scenarios may sound farfetched like something out of a movie, or a show like "The Tinder Swindler", it is an unfortunate reality to many individuals, especially elderly people every day, and startup or even well-established financial institutions may not always have the adequate controls and training to tackle fraud as it continues to evolve. As a result, companies tend to build a program as a reaction to fraud rather than starting with a proactive approach to prevent fraud and protect its customers.

WHAT IS ELDER FINANCIAL EXPLOITATION?

The Financial Crimes Enforcement Network ("FinCEN") and the Consumer Financial Protection Bureau ("CFPB") with some language taken from the Adult Protective Services ("APS") define elder financial exploitation as the illegal or improper use of an older person's funds, property, or other resources for monetary or personal benefit, profit, or gain. This includes, but is not limited to, theft, misappropriation, concealment, misuse, or fraudulent deprivation of money or property belonging to the elderly.

HAVE YOU LOOKED AT THE FOLLOWING?

According to the U.S. Department of Justice, elder abuse, which includes elder financial exploitation among other forms of abuse, affects at least 10 percent of elderly individuals in the United States

each year and based on the 2021 Federal Bureau of Investigation ("FBI") Elder Fraud Report, \$1.7 billion of losses reported were for adults aged 60 and over.

VICTIMS		
Age Range	Total Count	Total Loss
Under 20	14,919	\$101,435,178
20-29	69,390	\$431,191,702
30-39	88,448	\$937,386,500
40-49	89,184	\$1,192,890,255
50-59	74,460	\$1,261,591,978
Over 60	92,371	\$1,685,017,829

These are the figures that were reported to the FBI for which age information was provided. The sad part is that these figures are a decrease from previously reported numbers in 2020. In 2020, an estimated \$3.4 billion in elder financial exploitation was reported according to the CFPB, which is an alarming number taking into account that most of elder financial exploitation fraud goes unidentified and unreported as many victims chose not to come forward out of lack of resources, fear, or even embarrassment.

ARE YOU DOING ENOUGH?

Fraud and Compliance training may not be top of mind when establishing a company that provides financial services to consumers, but these companies can position themselves to play a vital role in detecting, responding to, and preventing elder financial exploitation with the right training and tools to detect and prevent elderly account owners from being targeted and/or victimized.

Creating a robust anti-fraud department with adequate policies, procedures, controls and the proper training, not just for your compliance department but all customer facing roles, is essential as it is your first line of defense equipping your staff with the knowledge and tools to detect all types of fraud such as: romance scams; grandparent scams; elder theft (i.e., power of attorney or legal guardianship exploitation); asset transfer; or gifting to fraudsters. These are only some examples among many others and establishing the proper fraud program can help you mitigate losses and keep our customers' accounts protected.

As a company that offers financial services, you not only have the ability, but in many instances, a requirement, to report suspected

elder financial exploitation to relevant federal, state, and local authorities such as FinCEN and the APS.

As technology evolves, fraudsters continue to take advantage of new methods of digital communication that further keep us apart from face-to-face contact. As we delve deeper into a digital world, we are responsible for establishing and implementing new techniques for detecting evolving fraud schemes. Companies must adapt, as the fraudsters do, by providing up to date training to its employees, creating new ways of truly knowing its customers, keeping up with the fraud trends to be able to identify account takeovers through the use of as malware, ransomware, sim swapping, and other tools used for fraud.

What used to be a concern of opening a phishing email for example, even if the reader realized it was potential phishing, is taken a step further nowadays by sophisticated looking emails that appear genuine and are hard to distinguish from a Company's legitimate communication. These emails guide users to almost identical domains to websites created almost as a mirror image of the legitimate company's to enter all of their credentials and identifying information, where by the time the customer realizes the image or hyperlink accessed is fake, its already too late, and their device has already been compromised with types of malware that can compromise their information and monitor activity, ultimately giving access to almost unlimited amounts of information that can later be used to impersonate the customer digitally.

By properly identifying the customer by means other than just obtaining an ID or verifying the same two pieces of information every time, a company will be able to reduce fraud and elderly financial exploitation. Thus, learning to verify and properly analyze things such as determining whether the ID presented is fake; the customer's geolocation in relation to their established address; devices used to log in to their accounts; detecting anomalies such as version discrepancies and downgrades of a mobile application, browser, or even on chain investigations; and examining Exif data from documentation requested or deep-fakes on selfie pictures and videos, either manually or relying on a vendor with the adequate technology. In addition, truly understanding how fraud takes place, the extensive red flags to look out for, and the fraud monitoring that should be conducted, will give companies a better chance of protecting itself and its customers, all the while maintaining the ease of doing business for its customers.

At Chartwell, we care about the underlying customer and have the knowledge and expertise to help Companies with the requirements and best practices necessary to establish robust fraud programs to abide by all regulations and do more in educating and protecting clients and their accounts. We focus not only on preventing elder financial exploitation, but also money laundering and fraud in general by providing proactive fraud detection techniques, establishing robust onboarding procedures to minimize the number of fraudulent accounts opened through stolen or synthetic identity, establishing adequate transaction monitoring controls and processes, and establishing working relationships with reliable vendors to further enhance all aspects of your program. These are just a few of the ways that Chartwell can help you accomplish your fraud prevention objectives.



JUAN SAA, COMPLIANCE PROFESSIONAL AT CHARTWELL, brings over eight years of BSA/AML, fraud, and sanctions experience. Prior to joining Chartwell, Juan worked at Robinhood as a Fraud Investigator with a special focus on regulatory inquiries and escalated cases as a result of internal and external referrals involving account takeovers, elder financial exploitation, and potential self-harm claims. For more information, contact Juan at jsaa@chartwellcompliance.com.

Compliance with a Founder's Mentality

By Martin Patterson, CAMS

A colleague of mine was recently asked to answer a question along the lines of trying to identify the single most important factor for consideration for fledgling fintechs as they begin to build out their compliance program and capabilities.

Professionals in this space may say a variety of things such as scale, budget, customer risk, product risk, policies, training, culture of compliance; all are relevant and important. However, none of these on their own is equal to the importance of choosing the right person to lead the compliance program in its earliest development. The right Compliance Officer is the key.

What do we mean by the "the right Compliance Officer"?

Of course, this really comes down to the business and how it operates – the culture and values it establishes – so finding the right fit is key. When we think about fintechs, we're generally thinking about startups and sometimes about legacy businesses looking to pivot into a new space with startup energy. This implies the need for a few basic skills besides the requisite experience and understanding of complying with regulations: the willingness and ability to wear multiple hats, adaptability, tolerance of the unknown, a genuine interest in the product or service, and a 'founder's mentality'.

The ability for a Compliance Officer to think and execute with a founder's mentality becomes truly critical for fintech startups with legal and regulatory requirements and/or other third-party obligations to be met. The term, itself, has been overly used in the past to mean, "do your best with what you've got." While I agree with that interpretation up to a point; there is a time and place for cost considerations especially when they impact compliance. However, there's an injustice done when it's used only in the context of resources as this is only a portion of the picture. The much more significant and impactful way to understand this trait is through the development of *relationships*. Often running with a skeleton crew, new fintechs live and thrive on positive, honest relationships cultivated internally amongst co-workers, colleagues in the industry, external vendors, bank partners, investors, and customers.

I've had the opportunity to speak with so many people over the years who work in some avenue of financial services compliance, and any time I meet someone new I love to hear about how they found this line of work. It's incredible, the number of people who feel as though they stumbled into the field and then find they're good at what they do. But so often, they view their role as sitting in the back seat; receiving information, analyzing, or catching things that have already happened, often responding reactively, and writing retroactive reports. There is no getting around the fact that these are often part of the

roles that we play. However, as leaders in the Compliance field we have to push beyond these boundaries to take a proactive stance. Bank partners and regulators expect and, today, really demand that the compliance function sit in a front seat position when it comes to the businesses with which they partner and oversee.

A Compliance Officer in these emerging spaces should find themselves, reaching out, sharing information, asking questions proactively about their part of the business and about all the other parts of the business, welcoming challenges to the way that they think, and seeking opportunities to get more involved. And for what it's worth, the rest of the leadership team should welcome that involvement with open arms; relationships are, at the very least, a two-way street. The business has to trust that despite the traditional narrative that Compliance is an obstacle to be overcome, their participation, opinion and experiences will bring tremendous value. The leadership teams that get this right and understand it, will use their pro Compliance stance as a differentiator with investors, bank partners, vendors, and customers. I've seen it time and again with clients. When the function is viewed as more than just a necessary evil (or necessity), but actually vital to the success of the company - there's nothing better than watching them succeed. This is the position in which Chartwell seeks to place all of its client.

NEEDED: The ability to wear multiple hats, adaptability, tolerance of the unknown, a genuine interest in the product or service, and a 'founder's mentality.'

I've been with the firm for over a year, and I'm gifted with the privilege to bring this message to startups every day who are looking for guidance – in many cases we're now serving as the day-to-day compliance administrators for those businesses who just need someone ready to jump in and help. Chartwell drew me in based on its commitment to quality and integrity, its diverse staff with deep compliance and licensing experience, its familial atmosphere, and above all else is Chartwell's commitment to relationships; and no coincidence that you'll also still find our own founder working in and on the business to the benefit of our clients. It's what he does- it's what we do. And we look forward to speaking with you and your teams to talk about how we can bring these strengths to bear for your business.



MARTIN PATTERSON, COMPLIANCE DIRECTOR AT CHARTWELL serves in Chartwell Compliance's Global Outsourced team with a focus on assisting clients with the day-to-day implementation and execution of the various aspects of their compliance program and related framework. Martin brings almost two decades of experience in US financial services compliance and operations oversight, corporate client due diligence, risk assessments as well as transaction monitoring, with a strong focus on implementing new processes and platforms. For more information, contact Martin at [✉ mpatterson@chartwellcompliance.com](mailto:mpatterson@chartwellcompliance.com).



Locational Data and Fraud Monitoring

By Erik Kemme

The advent of the internet age has steadily, and often explosively, altered the way that financial institutions and their related support industries have evolved in the ways they do business, from onboarding new clients both commercial and personal, to payment processing and compliance monitoring. As the public becomes increasingly expectant of their banking services to be seamless, frictionless, and interconnected, criminals and fraudsters have used this focus on high velocity banking and fund movement to load their quivers with a wide array of schemes and tactics to exploit customer and financial institutions alike. Further, with the meteoric rise of the popularity of Banking as a Service (BaaS), Fintech companies and traditional Financial Institutions have been simplifying the processes involved in onboarding and account creation. While this has vastly improved the convenience of banking and has provided consumers with an ever-increasing choice of how they wish to manage their assets, the resulting inevitable blow to effective collection of accurate CIP information and validation of personal identification has left BSA Banking Compliance and Fraud Monitoring Departments with more fraudulent activity than ever before. Additionally, the ease of use of technology has made the image of fraudsters being sophisticated hackers lurking in the shadows a thing of the past, with easy-to-acquire and easy-to-use programs and schemes being available to anyone with a computer, a few hundred dollars, and malicious intent. According to a recent study performed by AARP, Identity Theft losses in 2021 alone, aided by increase of P2P transfer platforms and frictionless onboarding practices, topped \$52 Billion, with nearly 42 million customers affected.¹ Additionally, it is estimated that Synthetic Identity Fraud (combining real information with fabricated personal data to create a viable "person") contributes around \$20 Billion in losses annually, an increase of 333% from 2016.² While it will always be difficult (read: impossible) to stop the bleeding entirely, BSA and Fraud departments in all banking sectors can help combat these trends, and more importantly be able to distinguish between suspect and victim more efficiently, by further integrating IP Address and Locational Data into their automatic monitoring systems and by demanding that vendors of these programs make collection and examination of this data part of their products' default functionality.

While IP addresses are typically seen as nebulous computer data which is held out in the ether, they have been a component of the internet since its military beginnings in the 1980s. IP (Internet Protocol) Addresses work in two primary fashions. Primarily, these addresses are used to route data (sent in "packets") from one router to the next, until these packets arrive and are placed in the correct order at the end destination, whether it be our homes, our banks, our libraries, etc. The second function of these addresses is to identify individual devices by a separate and unique address from the address your home is provided by your ISP (Internet Service Provider, such as Cox or Spectrum). In summary, this data denotes who is accessing the account, from where it is being accessed, and what device is being used to gain the access. This information can, and should, be leveraged in order to provide additional context to BSA and Fraud Monitoring departments.

An example can be easily constructed to illustrate the importance of easy access by Fraud and BSA Departments to this information. A Fraud Analyst is reviewing an account with a large number of returned transactions, with the customer indicating that they should not be held responsible for the activity because they had no hand in performing them, explaining that they believe their account has been "hacked". Without access to important IP locational data, the analyst would either have to take the customer at their word, refunding the money back to the customer at a significant loss to the institution, or spend precious time reaching out to external sources such as the destination bank or individual vendors who have no obligation to respond. However, if the customer had been directed to register devices to the account, and the information was readily available to be reviewed, a few clicks of the mouse could discover that the transactions being disputed were performed in the customer's neighborhood from a device that the customer had previously registered. Instead of a potentially large financial loss, the institution can save themselves that loss and decouple themselves from future risk by ending the customer's relationship without fear of reprisal or sanction. Inversely, should the information show that the account was accessed from an iPhone in Turkey when the customer is a 65-year old Accountant from Queens, hours of research which would have been traditionally required to identify the customer as a suspect or victim can be reduced to seconds, saving your employees from burnout, and increasing productivity by leaving them open to handle larger volumes of transactions.

While some institutions and software vendors have begun the process of implementing the necessary changes to provide this information as a default, the process is slow and lags far behind the fast pace and speedy evolution of the Fraudster. It is incumbent on both the Banking Community, and the FinTechs which rely on these institutions for accounts, to demand a push for integration of IP tracking into their monitoring and reporting suites, and it is without doubt that those software vendors which are the quickest to provide such functionality will be the ones to thrive moving forward as the financial services industry becomes further entrenched in the digital realm.

1 Identity Fraud Hit 42 Million People in 2021, April 7th, 2022, AARP.com

2 How Criminals Are Using Synthetic Identities for Fraud, December 3rd, 2021, Darkreading.com



ERIK KEMME, COMPLIANCE MANAGER AT CHARTWELL brings over 4 years of experience in BSA/AML Compliance focusing on KYC, Enhanced Due Diligence, Transactional Monitoring, Fraud Detection, and Quality Control. For more information, contact Erik at ekemme@chartwellcompliance.com.

National Multistate Licensing System & Registry



CSBS Releases Nonbank Cybersecurity Exam Procedures

CSBS released two new tools for nonbank financial services companies to improve their cybersecurity posture.

The [Baseline Nonbank Cybersecurity Exam Program](#) and the [Enhanced Nonbank Cybersecurity Exam Program](#) are tools used by state examiners nationwide to assess the cyber preparedness of nonbank entities. [Click here to read the full press release.](#)

NMLS Policy Guidebook Updates Available

An updated version of the [NMLS Policy Guidebook](#) has been posted to the NMLS Resource Center and the Regulator Resource Center. [Click here](#) to view a summary of the updates.

MSB Call Report Form Version Update

The [NMLS Money Services Businesses \(MSB\) Call Report](#) will be upgraded to Form Version 2 on April 1, 2023. The new form version will be effective starting with the first quarter 2023 MSB Call Report filing. For more information, see the Form Version 2 section

of the [Money Services Businesses Call Report](#) page of the NMLS Resource Center.

State News from NMLS:

Illinois Department of Financial and Professional Regulation Advises Licensees About Phishing Scam

The Illinois Department of Financial and Professional Regulation is aware of a phishing email that looks like an email from IDFPR. The email asks you to click a link to "complete your most recent up to date membership license certificate" and states that licensees must do so within 24 hours to avoid a license suspension.

The email comes from an email account not affiliated with IDFPR. If you receive an email like this, do NOT click any links and delete the email. If you have questions about the authenticity of an email from the Division of Banking or Division of Financial Institutions, please email IL.Banks@illinois.gov or FPR.DFI.Director@illinois.gov.

Utah Department of Financial Institutions adds new registration type to NMLS on September 1

NMLS will begin receiving new applications for the Utah Department of Financial Institutions. New applicants and will be able to submit these records through NMLS for the following registration type:

- ▶ Commercial Financing Registration

Applicants will be able to view the license requirements on the State Agency Licensing page on September 1. [Click here for more information.](#)

Alabama State Banking Department to Add ESB on August 31

Starting August 31, 2022, the Alabama State Banking Department will begin receiving new and converted Electronic Surety Bonds (ESB) through NMLS for the following license type:

- ▶ Consumer Credit License
- ▶ Mortgage Brokers License

See the [ESB Adoption Map and Table](#) for a list of state agencies who have also adopted ESB and required ESB conversion dates

Illinois Department of Financial & Professional Regulation to Add Electronic Surety Bond on August 1

Starting August 1, 2022, the Illinois Department of Financial & Professional Regulation will begin receiving new and converted Electronic Surety Bonds (ESB) through NMLS for the following license types:

- ▶ Debt Management License
- ▶ Debt Settlement Consumer Protection License

See the ESB Adoption Map and Table for a list of state agencies who have also adopted ESB and required ESB conversion dates

Nevada Financial Institution Division adds new registration types to NMLS on 8/1/2022

- ▶ Collection Agency – Exempt Registration
- ▶ Installment Loan Company – Exempt Registration

New applicants are now able to submit these records through NMLS. [Click here for more information.](#)

Starting August 1, the Nevada Financial Institution Division will begin receiving new Electronic Surety Bonds (ESB) through NMLS for the following license type:

- ▶ Collection Agency – Exempt Registration

See the [ESB Adoption Map and Table](#) for a list of state agencies who have also adopted ESB and required ESB conversion dates.

Kentucky Department of Financial Institutions adds new license types to NMLS on 8/1/2022

NMLS will begin receiving new applications for the Oregon Division of Financial Regulation. New applicants and will be able to submit these records through NMLS for the following license types:

- ▶ Federal Student Loan License

Applicants will be able to view the license requirements on the State Agency Licensing page on August 1.

Indiana Secretary of State Updates Checklists Due to July 1, 2022, Legislative Changes and Adds Compliance Alert to Securities Portal

Amendments to the Indiana Loan Broker Act are effective as of July 1st, 2022. The Securities Division is encouraging Loan Broker Affiliate Licensees and Loan Processing Companies to review the Securities Commissioner's related [Compliance Alert](#). Please thoroughly review all changes.

Nevada Financial Institutions Division Adds New License Types to NMLS on July 1, 2022

NMLS will begin receiving new applications for the Nevada Financial Institutions Division. New applicants and will be able to submit these records through NMLS for the following license types:

- ▶ Installment Loan Company License
- ▶ Installment Loan Company License – Alternate Location

Applicants will be able to view the license requirements on the State Agency Licensing page on July 1.

[Click here for more information.](#)

Illinois Department of Financial & Professional Regulation Adds New License Type to NMLS on July 1, 2022

NMLS will begin receiving new application filings for the below Illinois Department of Financial & Professional Regulation license on July 1, 2022. New applicants will be able to submit these records through NMLS. The agency will also begin receiving Electronic Surety Bonds (ESB) through NMLS for this license type.

See the [ESB Adoption Map and Table](#) for a list of state agencies who have also adopted ESB and required ESB conversion dates.

- ▶ Consumer Legal Funding Company

Applicants are now able to view the license requirements on the State Agency Licensing page. [Click here for more information.](#)

Illinois to Adopt Electronic Surety Bonds

Starting June 1, 2022, the Illinois Department of Financial & Professional Regulation will begin receiving new and converted Electronic Surety Bonds (ESB) through NMLS for the following license types:

- ▶ Consumer Loan Installment License
- ▶ Consumer Loan Installment Registration

See the [ESB Adoption Map and Table](#) for a list of state agencies who have also adopted ESB and required ESB conversion dates

Oregon Division of Financial Regulation Adds New License Types to NMLS on June 1, 2022

NMLS will begin receiving new applications for the Oregon Division of Financial Regulation. New applicants and will be able to submit these records through NMLS for the following license types:

- ▶ Student Loan Servicer License
- ▶ Student Loan Servicer License – Federal Contract
- ▶ Student Loan Servicer Branch License

Applicants will be able to view the license requirements on the State Agency Licensing page on June 1.

[Click here for more information.](#)

Starting June 1, the Oregon Division of Financial Regulation will begin receiving new Electronic Surety Bonds (ESB) through NMLS for the following license type:

- ▶ Student Loan Servicer License

See the [ESB Adoption Map and Table](#) for a list of state agencies who have also adopted ESB and required ESB conversion dates.

Wyoming Department of Banking Shares Notice from Wyoming Collection Agency Board

The WY Collection Agency Board has terminated the Certificate of Exemption Process. This determination does not have any effect on the requirements for licensure. [Click here for more information.](#)



Chartwell Shows You the Way

Founded in 2011, Chartwell Compliance delivers powerful solutions to complex regulatory, licensing, and compliance challenges experienced by fintech and financial services companies. Chartwell has served over 500 firms ranging from Fortune 50 to fintech's biggest unicorns throughout the world.

VALUE PROPOSITION

ONE-STOP SOLUTION

Complete outsourcing of worldwide license acquisition and maintenance and many day-to-day compliance and AML staff functions. Flex talent and variable fee structure that are superior to direct hiring or other service provider options.

SATISFIED CLIENTS

Over 500 satisfied clients, including some of the most prominent multinationals in their respective industries and many firms within the Fortune 1000.

"WALKS THE TALK" ON COMPLIANCE

Chartwell is proud to be an entity of MVB Bank, a regulated, publicly traded financial institution which Chartwell supports on compliance.

STABLE, HIGHLY QUALIFIED WORKFORCE

Nearly all employees possess over 20 years of experience as practitioners or regulators, and are employees, not contractors. Chartwell is proud of its low employee turnover rate and the many awards it has received for a unique and revolutionary corporate culture and approach to staff development.

EXCEPTIONAL PROJECT MANAGEMENT

Chartwell staff members practice a Kaizen methodology and use proprietary project management techniques that sustain a high level of quality.



"The Chartwell Team has been a breath of fresh air for the Mana team and me personally; you are making us better everyday with your guidance and we truly appreciate your partnership."

Bryn Smith, Director of Product Operations & Integration Mana Interactive, Inc.

Careers

Chartwell Compliance understands that great work means continuously making improvements not just within the company, but also within ourselves. Our staff members:

- ▶ Work every day with experts in regulatory compliance and financial crimes prevention.
- ▶ Assist some of the most innovative companies in the financial services industry.
- ▶ Thrive in a fast-paced, entrepreneurial environment with upward mobility.

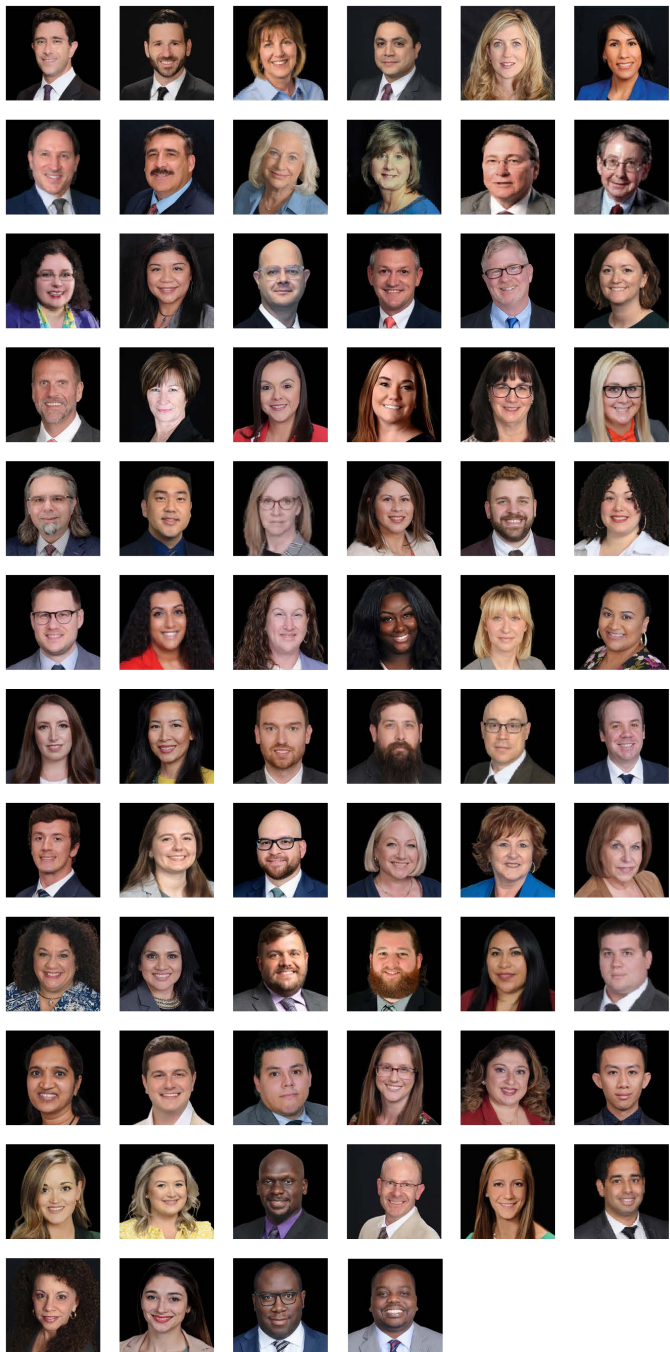
- ▶ Improve their skillsets and knowledgebases through relevant certificates, courses, or workshops that advance their careers and leadership.
- ▶ Receive Kaizen training, the Japanese principle that aims to create a work environment that is as efficient as it is productive and successful.

Chartwell is always looking for full-time skilled professionals in compliance and risk management, operations, corporate development, and consulting management. Please email careers@chartwellcompliance.com to apply for a position with Chartwell Compliance.

[VIEW CURRENT OPEN POSITIONS](#)



Chartwell Consultants



Chartwell's team members are 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 seasoned examiners, operators, and regulatory policy makers in the banking, non-banking, and emerging payments compliance segments of the financial services industry.

CONSULTANTS AVERAGE 20 YEARS OF EXPERIENCE

We use this vast experience to design and implement effective compliance and risk management programs properly calibrated to address both the current and prospective regulatory environment.

EXTENSIVE EXPERIENCE AT THE INDUSTRY'S BEST ORGANIZATIONS

Chartwell's staff members have served in:

- Internationally prominent U.S. payments licensing and compliance advisory outsourcing practice
- Regulatory and examiner experience with the California Department of Business Oversight, Colorado Department of Banking, Federal Reserve Bank of Kansas City, Michigan Department of Insurance & Financial Services, Texas Department of Banking (DOB), Washing Department of Financial Institutions, Washing US Department of Treasury and FINRA
- MSBs such as Western Union, First Data, and Sigue
- State and nationally chartered banks
- The Federal Bureau of Investigation's Financial Crimes and Terrorist Financial Crimes and Terrorist Financing
- Assistant director at the Office of the Comptroller of the Currency (OCC) Assistant Director of Enforcement



Chartwell Services

Fintech Licensing

With its large team of long-time licensing officers and former regulators, Chartwell has centuries of collective experience obtaining and maintaining thousands of regulatory licenses for fintech companies in areas like money transmission, cryptocurrency, prepaid access, currency exchange, lending, and gaming. The firm provides a fully outsourced solution in all key component parts of getting and staying licensed. Chartwell's emphasis on excellent project management and Kaizen methodology help ensure timely results. Chartwell and its staff have serviced, worked at, or supervised a statistically significant portion of all licensed U.S. money transmitters.

Fintech Compliance

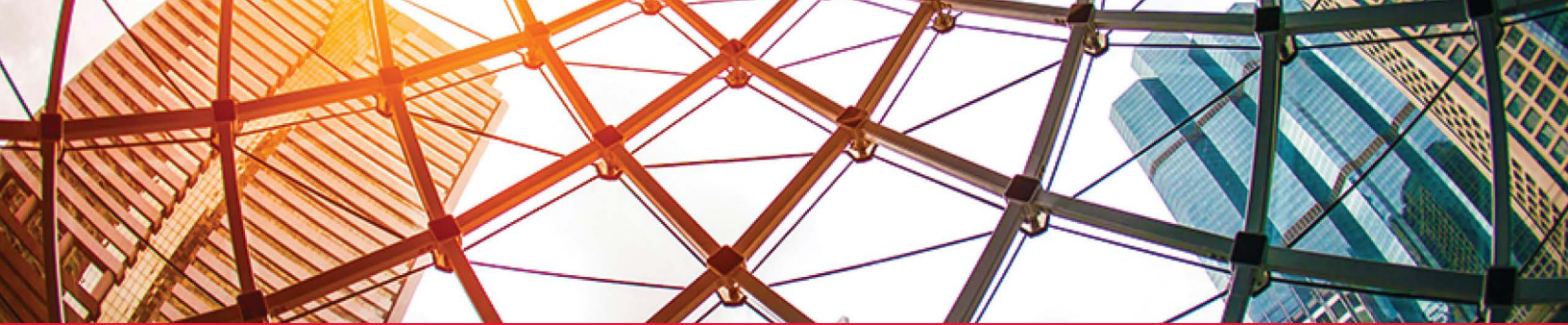
Chartwell is one of the world's preeminent providers of AML/CFT, fraud prevention, and regulatory compliance services to the fintech industry. Comprised of an incredibly deep bench of long-time practitioners from all corners of the fintech industry, the firm builds, localizes, enhances, and audits compliance programs. It has served many of the industry's leading fintechs, hundreds of companies overall throughout the world.

Banking Compliance

Chartwell has well-credentialed former bank compliance officers and regulators who serve all types of banks as well as challenger/neo/digital banks in most areas of bank regulatory compliance. Numerous clients come from the fintech industry and several of the fintech banking market leaders have worked with Chartwell. Chartwell brings a unique, first-hand experience to its work, with its own parent company being a publicly traded fintech bank and a client of Chartwell.

Global Outsourced Compliance

Chartwell's team of veteran compliance officers, regulators and analysts are positioned as an outsourced resource for compliance program execution with many financial services businesses. The firm handles many of the day-to-day functions required to maintain an effective compliance program, including transaction monitoring and reporting; sanctions screening; KYC and customer due diligence; onboarding and enhanced due diligence; fraud prevention; consumer compliance; and taking overall leadership of the program. Providing flex talent at variable cost, with excellent bench depth and quality assurance, Chartwell is a strong alternative to hiring directly in many cases.



Chartwell's Strategic Alliances



Fiserv, a global leader in payments and financial technology, helps clients achieve best-in-class results in account processing and digital banking solutions; card-issuer processing and network services; payments; e-commerce; merchant acquiring and processing; and the Clover® cloud-based point-of-sale solution.



Thomson Reuters is a leading provider of business information services. Our products include highly specialized information-enabled software and tools for legal, tax, accounting and compliance professionals combined with the world's most global news service – Reuters.



NICE Actimize uses innovative technology to protect institutions and safeguard consumers and investors by identifying financial crimes, preventing fraud and providing regulatory compliance.



Middesk's Identity product provides accurate, complete information that financial services companies need to make efficient onboarding decisions. Our Agent product makes it easy for employers to file with the state and federal agencies needed to establish their business across the country. Our customers include Affirm, Brex, Plaid, Mercury, Divvy, Rippling, Gusto, and others.



Acuant Compliance's Trusted Identity Platform provides identity verification, regulatory compliance (AML/KYC) and digital identity solutions leveraging AI and human-assisted machine learning to deliver unparalleled accuracy and efficiency.



Through its subsidiary, MVB Bank, Inc., and the Bank's subsidiaries, MVB Community Development Corporation, Chartwell Compliance and Paladin, MVB provides financial services to individuals and corporate clients in the Mid-Atlantic region and beyond.



Accuity offers a suite of innovative solutions for payments and compliance professionals, from comprehensive data and software that manage risk and compliance, to flexible tools that optimize payments pathways.



Coinfirm is a global leader in AML & RegTech for blockchain & cryptocurrencies. Offering the industry's largest blockchain coverage - over 98% of cryptocurrencies supported - Coinfirm's solutions are used by market leaders, ranging from VASPs such as Binance, and protocols like WAVES, to major financial institutions and governments.



Chartwell New Hires

Chartwell is pleased to welcome the following individuals to its team of professionals.



Daniel Lee
Joined Chartwell on June 1st, 2022

Assistant Compliance Director - Fintech Compliance

Daniel Lee is an Assistant Director in Chartwell's Fintech Compliance team with over 15 years of regulatory compliance and consulting experience in the Banking and Money Service Business industry. As a former examiner and Fintech subject matter expert at the Colorado Division of Banking, Daniel led examinations of Fintechs and virtual currency companies for compliance with state and federal regulations. [Read more about Daniel](#)



John Laramie
Joined Chartwell on August 1st, 2022

Compliance Director – License Maintenance

John Laramie is a Director with Chartwell and is the functional lead for Chartwell's License Maintenance team. With deep knowledge and expertise in Money Service Business (MSB) regulatory compliance, John has over 15 years' experience in organizational development and leadership including program management, governance, policy writing, and training administration. [Read more about John](#)



Juan Saa
Joined Chartwell on June 21st, 2022

Compliance Professional – Outsourced Compliance

Juan Saa is a Compliance Professional with more than eight years of BSA/AML, fraud, and sanctions experience. Prior to joining Chartwell, Juan worked at Robinhood as a Fraud Investigator with a special focus on regulatory inquiries and escalated cases as a result of internal and external referrals involving account takeovers, elder financial exploitation, and potential self-harm claims. [Read more about Juan](#)



Jaanae Wilkes
Joined Chartwell on September 8th, 2022

Senior Compliance Professional – License Maintenance

Over 9 years of experience in compliance industry working in PCI Compliance and License Maintenance at CEXIO and Fiserv, Inc, responsible for maintaining regulatory reporting requirements in NMLS and state portals, Secretary of State maintenance and reporting as well as creating procedure documents and various other compliance related functions. [Read more about Jaanae](#)



Karen Elliott
Joined Chartwell on July 11th, 2022

Senior Compliance Professional – License Maintenance

Karen Elliott is a Senior Compliance Professional at Chartwell Compliance and has over 17 years of experience in the Public Filings Industry working with the various Secretary of State offices. In addition, for several years Karen also sat on the Board of Directors for the National Public Records Research Association. [Read more about Karen](#)



Lisa Mueller
Joined Chartwell on September 8th, 2022

Senior Compliance Analyst – Banking Compliance

Over 4 years of experience in BSA/AML Compliance focusing on KYC, Enhanced Due Diligence, Transactional Monitoring, AML/ Fraud Detection, Training and Quality Control at AML RightSource. [Read more about Lisa](#)



Shannon Rice
Joined Chartwell on August 1st, 2022

Compliance Professional – License Acquisition

Shannon is a Compliance Professional in Chartwell's Licensing team and has heavy duty Money Transmitter regulatory experience and over 16 years in varying regulatory roles with the state of Washington. Prior to Joining Chartwell, Shannon served as a Program Specialist for the Washington Department of Financial Institutions Consumer Services division, licensing Money Transmitters and Mortgage Loan Originators, as well as overseeing the Refund Anticipation Loan program. [Read more about Shannon](#)



Christopher Wilson
Joined Chartwell on September 15th, 2022

Compliance Analyst – Banking Compliance

More than 15 years of experience in the banking industry, in customer service and financial advisory and branch manager roles. In addition, deep knowledge in AML focusing on Enhanced Due Diligence with Wells Fargo and Capital One. [Read more about Christopher](#)

Culture and Honors

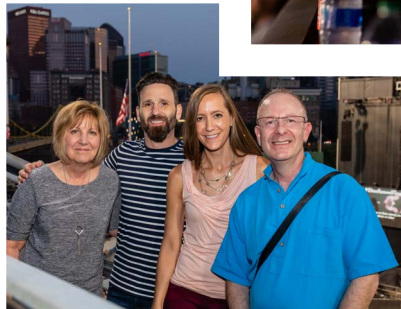


Chartwell Foresight is the parent organization for Chartwell Compliance and Chartwell Futures, offering a holistic approach to health, growth, and innovation for individuals and corporations.



Fall Retreat 2022

The entire Chartwell Foresight family joined together for a time of team building, togetherness, and Elton John concert!



FORWARD UNTO FUTURES

*Come, ye pilgrims, from near and from far
Drink from the oasis that inspires who you are
Through journeys long and short, just waiting to begin
The transformation out starts from within*

*Break down these walls, the constructs of old
Reveal hidden foundations, former muses to the bold
Unlock what is hidden, locked away deep inside
Waiting to be released, to RISE*

*Forge ahead by looking back through our heirs
Relive the lives of our forebears
Empowered and revived to challenge the new dawn
Through reflection and acceptance, feel ancestors
nudging you on*

*Shatter what was known to relearn what you knew
Each corner of globe contains lessons so true
If the mind is set free, the soul can then soar
To height once though unreachable before*

*A metamorphosis of mind, body, and heart
A life-changing experience is what can impart
No mountains too high, no ocean too deep
Endless adventures abound, if only you seek*

*Experience events that know not time
Forever woven into the tapestry of the world, so fine
Young or old, new or seasoned alike
Can be reached, moved, and inspired for life*

*Go beyond the norms challenge the status quo
Take heed from "The Seuss": "Oh, the places you'll go!"
Forge a new path, blaze a trail all your own
For with each new milestone you can strengthen your home*

*So open your mind, let go of what you know
Embrace the unknown and be inspired to grow
If you lean into the change the possibilities take flight
Your future, or rather "Futures" will guide you to new heights*

—JEB CLIBER

A poem inspired by
Chartwell's 2022 Fall Retreat,
in Pittsburgh, PA., authored by
our colleague, Jeb Cliber.



Subscribe today

Get your complimentary subscription today and learn the latest on financial regulatory compliance, crime prevention, and risk management. Send an email to:

compass@chartwellcompliance.com

Chartwell is honored to be recognized by the following organizations:



CHARTWELL

REGULATORY COMPLIANCE & RISK MANAGEMENT

301 Virginia Avenue, Fairmont, WV 26554 | chartwellcompliance.com

Chartwell Compliance is a wholly-owned subsidiary of MVB Bank, Inc. 



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.

PHOTOS: UNSPLASH, GETTY IMAGES, CHARTWELL COMPLIANCE

 Printed on recycled paper.