REGULATORY INTELLIGENCE BRIEFING — ISSUE 7, 2018

ARE CRYPTOCURRENCIES AND BLOCKCHAIN THE FUTURE OF FINANCE?

Capco Center of Regulatory Intelligence

CAPCO

IN THIS ISSUE

EDITORIAL NOTE FROM THE MANAGING PRINCIPAL, CENTER OF REGULATORY INTELLIGENCE

PETER D. DUGAS
MANAGING PRINCIPAL, CENTER OF REGULATORY INTELLIGENCE

Peter has more than 16 years of government and consulting experience in advising clients on supervisory matters before the U.S. government and in the implementation of enterprise risk management programs. He is a thought leader in government affairs and regulatory strategies in support of banks' and financial institutions' compliance with the Dodd-Frank Act and Basel Accords. Prior to joining Capco, he served as a director of government relations at Clark Hill and in senior government positions, including serving as a deputy assistant secretary at the United States Department of the Treasury.

The idea of cryptocurrencies is not a new one. Starting in as early as the 1980s, there were attempts to build digital currencies to replace or coexist with fiat currencies. But in the last decade, the technology has boomed, bringing us to an age of cryptocurrency that has the critical advantage of a history of failed attempts. Ten years ago, Satoshi Nakamoto wrote the code for one of today's top cryptocurrencies, and a paper on an electronic peer-to-peer currency system that catapulted virtual money into a tangible innovation.

As virtual currencies have taken on a worldwide fascination, the headlines now involve predictions on economic impact and the myriad of government responses range from welcoming adoption to strict bans. Consumers and traditional financial services institutions alike are wondering what the implications of these technologies will be — can they really be used as money? How can we ensure the systems are safe to use? How else can we utilize blockchain technology?

Capco Center of Regulatory Intelligence (CRI) has heard from many clients expressing interest in answers to these questions. In this month's RIB, we take a global look at virtual currencies to better understand some options the U.S. government could adopt for treatment of these innovations. We bring you up-to-date with where international jurisdictions stand to show how these external decisions could impact or forecast what might be in store for the U.S., as policies continue to shift and our administration continues to strive for economic growth.

This month, we have weaved the Congressional Activity Summary into the focus article, to better provide a current-state snapshot of the conversation around virtual currencies at the congressional level. We review a recent congressional hearing, focusing on the discussion surrounding a potential government-backed, central bank-issued virtual currency. Then, we provide updates on some of the actions individual regulating agencies have taken in the past few months with regard to these technologies.

Our secondary article this month provides more concrete and direct best practices for financial institutions, delving into the ongoing role institutions play in the credit reporting process. With recent enforcement actions highlighting the importance of getting it right, this article provides a necessary review of where the requirements stand, as well as best practices to ensure compliance and protect your institution and your customers. ❖

REGULATORY ROUNDUP

Regulatory and Compliance Alerts

GAO Issues Report on Federal Tax Withholding

On July 31, 2018, the Government Accountability Office (GAO) issued a report on federal tax withholding. The report includes an evaluation of how the Department of the Treasury (Treasury) and IRS develop federal tax withholding tables and subsequently conduct outreach on the tables.

FHFA Announces Decision to Stop Credit Score Initiative

On July 23, 2018, the Federal Housing Finance Agency (FHFA) announced that the agency will not make a decision in 2018 about updating the credit score model that Fannie Mae and Freddie Mac (the Enterprises) use, as previously announced. Instead, FHFA is shifting its focus to implementing Section 310 of the Economic Growth, Regulatory Relief, and Consumer Protection Act (EGRRCPA). The Act requires FHFA to define, through rulemaking, the standards and criteria the Enterprises will use to validate credit score models.

Congress Passes Law to Extend NFIP

On July 31, 2018, President Donald Trump signed Senate Bill 1182 into law, reauthorizing the National Flood Insurance Program (NFIP) through November 30, 2018.

FRB Launches New Supervisory Bulletin

On July 26, 2018, the Federal Reserve Board (FRB) launched a new publication titled "Consumer Compliance Supervision Bulletin." The first edition of the bulletin covered redlining, discriminatory loan pricing and underwriting and various unfair or deceptive acts or practices.

OFAC and Others Issue Advisory on North Korea

On July 23, 2018, the Office of Foreign Assets Control (OFAC), along with the Departments of State and Homeland Security, issued an advisory to highlight North Korea's sanctions evasion tactics that could expose businesses — including manufacturers, buyers and service providers — to sanctions compliance risks under U.S. or United Nations sanctions authorities.

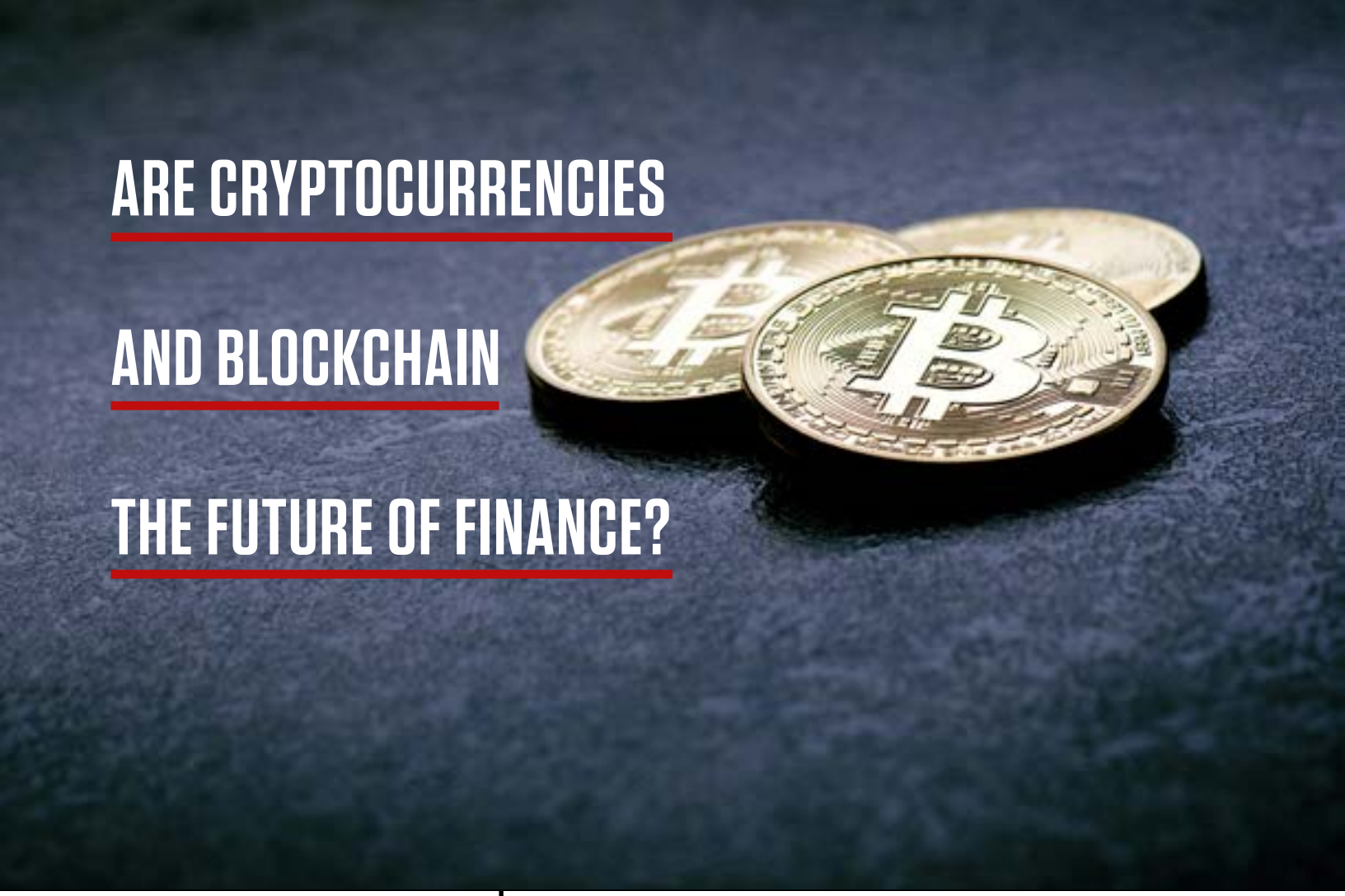
OCC Begins Accepting National Bank Charter Applications from Fintech Companies

On July 31, 2018, the Office of the Comptroller of the Currency (OCC) announced it will begin accepting applications for national bank charters from nondepository fintech companies engaged in the business of banking. As part of this announcement, the OCC issued a related policy statement and a supplement to the *Comptroller's Licensing Manual*.

Agencies Issue Statements regarding HMDA Compliance in Response to EGRRCPA

On July 5, 2018, the Bureau of Consumer Financial Protection (BCFP or CFPB) issued a statement in response to provisions in EGRRCPA related to the Home Mortgage Disclosure Act (HMDA), as implemented by Regulation C. EGRRCPA provided partial exemptions for some insured depository institutions and insured credit unions from certain HMDA requirements, and the CFPB plans to release additional guidance in the near future on this topic.

ARE CRYPTOCURRENCIES AND BLOCKCHAIN THE FUTURE OF FINANCE?



This year marks the ten-year anniversary of the publication of Satoshi Nakamoto's paper describing how a new digital financial instrument could be created and operated securely with a blockchain. The growing usage and range of capabilities indicate that cryptocurrencies are taking on an ever more important role in the lives of a growing number of people (and machines) around the world.

However, amongst all the excitement and enthusiasm in the press, there has also been some hyperbole. In this article, we provide a realistic snapshot of the virtual currencies industry, and include actionable intelligence for how your institution should ensure best practices.

A BACKGROUND ON CRYPTOCURRENCY AND ITS UNDERLYING TECHNOLOGY

The financial industry is transforming before our eyes. Digitized assets and innovative financial channels, instruments and systems are creating new paradigms for financial transactions and forging alternative conduits of capital.

Blockchain has received a significant amount of analyst and press attention over the last few years as this emerging technology holds significant potential. Use cases are many and varied: ranging from programmable cryptocurrencies and property deeds management to provenance tracking and voting records.

Cryptocurrencies were the first application of this technology, and this innovation introduced an entirely new set of businesses, jobs and vocabulary to the world of payments.

What Are 'Cryptocurrencies'?

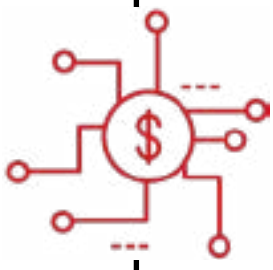
"Cryptocurrencies" are digital money with artificial limitations, without coins and notes. With the help of cryptography and a collective booking system called "blockchain," cryptocurrencies build a distributed, safe and decentralized payment system, which does not need banks, intermediates, an organization or a central technical infrastructure to work.

The main difference from the current types of money we know is that an intermediate responsible for production (e.g., central bank) or exchange (e.g., banks) is not needed. Instead, two individuals make direct exchanges of digital values and goods.

In a sense, these cryptocurrencies are scarce commodities, as the amount of available currency units is, in most cases, limited by mathematical algorithms. After every digital currency unit is issued, there is no way to generate additional currency units from it (e.g., one of the most popular cryptocurrencies is limited to 21 million units). Furthermore, every cryptocurrency has its own currency-generating process.

The market cap of cryptocurrencies increased to over $200 billion in 2017 and received the attention of the global central banks. In our opinion, main factors likely to affect the future development of cryptocurrencies are:

- Interventions by the government and central banks
- Questions on how the sector will be regulated
- Growing competition between cryptocurrencies



Blockchain: The Underlying Technology

A "blockchain" is a decentralized database, which includes a steadily rising list of transactions. It enables the worldwide exchange of data — without a central party — through a peer-to-peer network. Due to decentralization, transaction costs are lower, and business can be done faster.

Around the clock and worldwide, individuals are using digital money for transactions. The "blockchain network" puts any unconfirmed transaction into a list — the so-called "block." A confirmed block is then added to the "blockchain." This process is called "mining."

THE IMPLICATIONS OF INNOVATION

What Potential Do Cryptocurrencies Have?

Analyzing money development shows that every historically successful currency has needed the support of a central authority to guarantee the money's value and deliver securities to investors. To strengthen trust in the value of cryptocurrencies, changes such as increased regulation and tangible securities are likely necessary.

Cryptocurrencies do not currently fulfill the criterion of general acceptance; central banks (as well as the relevant literature) do not vouch for their quality.

However, because most cryptocurrencies are limited, the inflation risk is low. And while reproductions and splitting could have an impact on the inflation rate (as this could increase the number of available currency units), cryptocurrencies could, in fact, represent a form of protection against inflation in crisis countries.

Proof of Potential: The Crisis in Venezuela and the Cryptocurrency Solution

On July 23, 2018, Director of the International Money Fund Alejandro Werner wrote in the agency's blog that they are "projecting a surge in inflation to 1,000,000 percent by end-2018 to signal that the situation in Venezuela is similar to that in Germany in 1923 or Zimbabwe in the late 2000's." This rapid devaluation and volatility is obviously hugely detrimental to those who hold assets in the Venezuelan currency, the bolivar fuerte.

For some Venezuelans, this means cryptocurrency is a reasonable and more stable option. Indeed, the country has seen a significant spike in virtual currency usage, and surpasses its neighboring and more affluent countries in value of top cryptocurrency transactions.

For some countries in crisis, such as Venezuela, cryptocurrency provides:

1. **Stability**

   Even though virtual currencies seem volatile for those who hold assets in stable fiat currencies such as the U.S. dollar, an intriguing quality of cryptocurrencies for those in crisis countries is that the value with not depreciate with inflation, as a national currency would.

2. **No additional fees**

   Conversion fees on remittances can be extremely costly — cryptocurrency transfers are fee-free.

3. **Security**

   Stealing cryptocurrency is extremely difficult, and in many crisis countries, robbery is a major concern.

4. **Access**

   In crisis countries, access to traditional banking services is not a given. But, many people have smartphones and access to digital assets are only a few swipes away.

What Risks Do Cryptocurrencies Face?

Theft

As the transactions are based on cryptography, stealing or losing information is possible through bugs, trojans or viruses. To avoid this, wallet apps provide different opportunities for security.

Technical Progress

Expected to be available for purchase in 10 years at the earliest, quantum computers will have enormous computing power and be able to decrypt the algorithms that encrypt cryptocurrencies. However, as the technology required for these types of machines develops, so do other innovations; for example, new encryption methods that will protect against quantum computers.

Political risks and regulation

Another risk is that large economic powers prohibit trading and payment with cryptocurrencies. For example, in September 2017, China's Central Bank banned all Initial Coin Offerings (ICOs), which companies use to create their own crypto-money and sell to the public. Central banks could also introduce their own cryptocurrencies to drive private cryptocurrencies out of the market.

Reproduction

Various cryptocurrency replicas or splits — "forks" — are likely to occur in the future as most cryptocurrencies are based on an "open-source" blockchain, a protocol freely available to everyone. These forks are forcing investors to assimilate to a cryptocurrency because transaction costs, value and competition can change dramatically. It is possible that after a fork, only one currency of the spinoffs prevails.

Sustainability

Power consumption for one of the most popular cryptocurrencies' mining platform worldwide now amounts to 24.52 terawatt hours annually. This roughly corresponds to the annual energy needs of Nigeria. Based on the data of this one currency's mining operation, the resulting environmental impact for a transaction corresponds to a 125-mile journey in an SUV

HOW REGULATORS ARE APPROACHING THE UNKNOWN: A GLOBAL PERSPECTIVE

Diverging Approaches to Regulating Virtual Currency Trading: A Spectrum

There is a wide range of regulatory involvement and interaction for cryptocurrency oversight.

No Action:	Self-regulation:	Adjusted Direct Oversight and Rules:	Trading Ban:
GERMANY: Ad-hoc intervention where needed; Germany Federal Financial Supervisory Authority (BaFin) provides authorization under existing framework depending on services offered	**JAPAN:** Creation of industry-led, self-regulatory body **US:** Federal agencies calling for self-regulatory organization to oversee exchanges **UK:** Setup of CryptoUK	**EU:** Adjustments to Fifth Anti-Money Laundering Directive (AMLD) to cover crypto-exchanges **US:** Treasury and states regulate exchanges only as money service businesses	**CHINA:** Banned local investments in ICOs, considering blocking access to overseas websites that offer trading

Europe: From Consumer Warnings to Balanced Regulation

European Commission

Key Concerns:

- Believes there is a need to differentiate between cryptocurrencies and underlying technology
- ICOs putting investors at risk

Regulatory Response:

- "FinTech Action Plan" released on March 8, 2018, asking for a framework on ICOs
- AMLD expanded
- Ongoing monitoring of developments of crypto-assets and ICOs

European Central Bank (ECB)

Key Concerns:

- Due to limited distribution, currently considers impact on financial stability to be low; depending on use, this might change
- Does not consider virtual currencies to be "money" as they miss the characteristics of money

Regulatory Response:

- Ongoing monitoring of market developments (distribution, type of use, participants)
- Supports adoption of instant payments to make cryptocurrency redundant

Germany Federal Financial Supervisory Authority (BaFin)

Key Concerns:

- Believes cryptocurrency is prone to cybersecurity risks; impaired access to digital wallet (e.g., due to hacking attacks) might result in total loss for investors
- Believes ICOs might result in total loss for investors
- Does not consider virtual currency to be "currency" or "e-money," thus there is no legal tender to cash investment
- Precludes a one-size-fits-all approach through various specifications

Regulatory Response:

- Provided clarification via information sheet: derivatives on cryptocurrency fall under the German Securities Act (WpHG); will take a case-by-case approach to determine the status of a particular product and the appropriate legal framework
- Willing to act to protect consumers even in advance of dedicated cryptocurrency regulation

Bank of England (BoE), Financial Conduct Authority (FCA), Her Majesty's Treasury (HM)

Key Concerns:

- Shows "significant risk" for investors to lose their investment; investor protection is key regulatory focus
- Believes virtual currencies are a major risk for money laundering and tax evasion

Regulatory Response:

- Official warning on ICOs and the payment with cryptocurrency for them
- Expected to expand financial system standards to crypto-asset ecosystem
- Expected to adjust AML rules and tax regulations

Asia-Pacific (APAC): Focus Shifting from Opportunities to Risks

Monetary Authority of Singapore (MAS)

Key Concerns:

- Sees risk of fraud due to difficult verification of issuer's authenticity
- Believes there are risks relating to insufficient secondary market liquidity
- Sees a lack of exit options
- Views unregulated exchanges or trading platforms as risky
- Sees risks relating to highly speculative investments
- Believes there is risk of money laundering and terrorist financing

Regulatory Response:

- Published advice for consumers on potential risk of digital tokens and virtual currency-related investment schemes
- Issued warnings for digital token exchanges and ICO issuer
- Research on Central Bank Digital Currencies (Project Ubin)
- While not regulating virtual currencies directly, further regulation for activities around virtual currencies is expected (e.g., provisions for anti-money laundering/combatting the financing of terrorism)

The Securities and Futures Commission (SFC) / Hong Kong Monetary Authority (HKMA)

Key Concerns:

- Sees high risk of money laundering

Regulatory Response:

- Warning on virtual currencies
- HKMA revision of "Guidelines on Authorization of Virtual Banks"
- Carried out proof-of-concept for a potential digital currency project, but announced they have "no plans to issue [Central Bank Digital Currency] at this stage but will continue to monitor international development"
- Will regulate ICOs

People's Bank of China (PBoC)

Key Concerns:

- Believes there is risk of fraudulent behavior and illegal public financing behavior

Regulatory Response:

- Prohibited initial coin offerings and trading with virtual currencies
- Further actions expected

International

Financial Stability Board (FSB)

Key Concerns:

- Due to virtual currencies' small size, does not currently consider them to be a systemic risk; however, financial stability issues could emerge if a virtual currency is adopted widely
- Sees risk of use for illegal activities, including cyberattacks

Regulatory Response:

- Request for relevant authorities to analyze the potential implications of virtual currencies for monetary policy, financial stability and the global monetary system
- Provided a report to the G20 on crypto-assets

Bank for International Settlements (BIS)

Key Concerns:

- Thinks it is unlikely that virtual currencies will displace sovereign currencies
- Believes central bank-issued digital currencies could impact deposits with implications for financial stability in times of market stress
- Believes there is no evidence that digital currencies would allow for improved monetary policy

Regulatory Response:

- Request for national central banks to decide upon Central Bank cryptocurrencies
- Research report on central bank digital currencies, calling for thorough consideration of potential side-effects

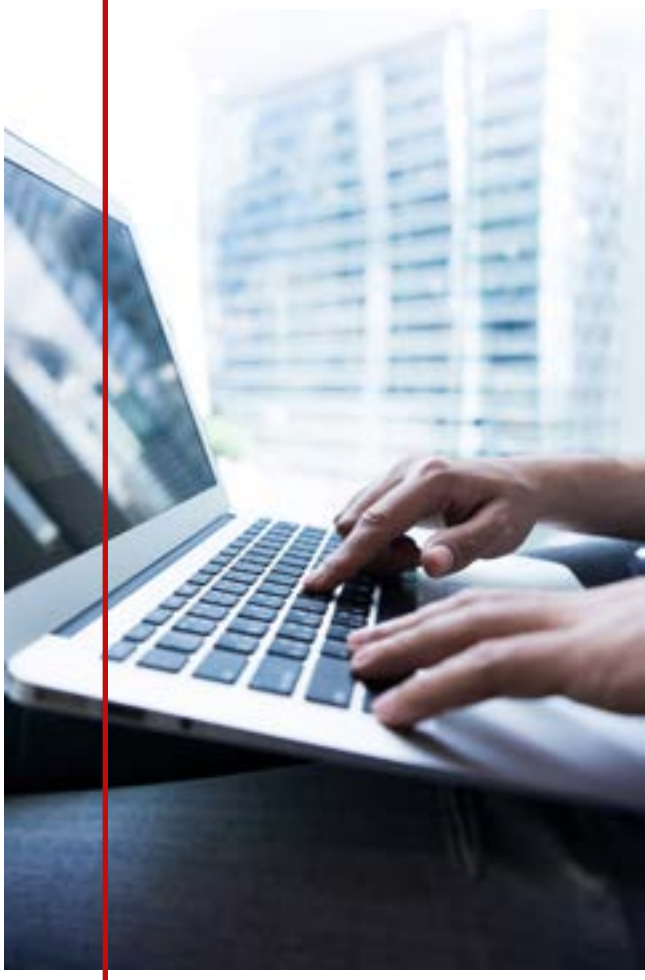
Group of Twenty (G20)

Key Concerns:

- Has not yet published a specific positioning on cryptocurrencies

Regulatory Response:

- Global approach towards virtual currencies discussed during G20 meeting in March
- No short-term actions expected



US: Consolidating Diverging Perspectives

Federal Reserve Board (FRB)

Key Concerns:

- Believes wide-scale usage could open the U.S. to serious financial stability issues due to lack of predictable and stable exchange rate and subsequently unpredictable demand for liquidity

Regulatory Response:

- FRB Governor Lael Brainard said "a more holistic approach to the security of the broader cryptocurrency ecosystem, along with added layers of security on top of cryptography" would be necessary for wider cryptocurrency acceptance
- Ongoing support of industry efforts to improve harmonization across the sector
- Ongoing monitoring of further developments

Commodity Futures Trading Commission (CFTC)

Key Concerns:

- Treats cryptocurrency as a commodity so that exchanges are subject to the agency's requirements for listing a new virtual currency derivative product/contract
- Pays attention to price volatility and trading practices in the underlying cash and futures markets
- Believes key risks of virtual currencies to be: operational, speculative, cybersecurity and fraud and manipulation
- Holds both oversight and enforcement authority over derivative markets, but is limited to just enforcement authority for spot markets where commodities themselves are traded

Regulatory Response:

- Consumer warning on virtual currencies
- Future monitoring of the virtual currency derivatives market, developments in positions, open interest, margin requirements and stress testing positions
- Potential future measures to increase margin requirements for derivative clearing and additional reviews of exchanges, clearing organizations and individual traders involved in trading and clearing of cryptocurrency futures
- Ongoing internal discussions on self-certification framework that is "consistent with public policy that encourages market driven innovation," yet may not be an appropriate tool for all new products
- Self-regulatory approach encouraging oversight by a privately-owned, independent organization

Securities and Exchange Commission (SEC)

Key Concerns:

- Believes unregistered securities investments falsely labeled as ICOs pose threat to investor protection
- Claims cryptocurrency exchanges may fall under SEC mandate and these exchanges could be shut down if they fail to abide by existing SEC rules

Regulatory Response:

- Consumer warnings on ICOs
- Support of policy efforts to review existing frameworks
- On high alert for certain offerings, which have key features of securities but are then labelled as ICOs
- Highlighted concerns in Staff Letter on engaging on fund innovation and cryptocurrency-related holdings

RECENT DEVELOPMENTS IN THE US

Congressional Activity

On July 18, 2018, the House Subcommittee on Monetary Policy and Trade held a hearing titled "The Future of Money: Digital Currency." The hearing examined:

- The extent to which the U.S. government should consider cryptocurrencies as "money"
- The potential domestic and global uses for cryptocurrencies
- The merits of any uses by central banks of cryptocurrencies
- The future of both cryptocurrencies and physical cash

The witnesses' testimonies mostly focused on whether the U.S. government should consider creating its own central bank-backed digital currency. While all witnesses agreed cash is still widely used in the US, and will remain so for at least the near future, they did question how this might be changing and what role digital currencies will play. Some witnesses pointed out that cash usage in some other countries is declining, as more and more digital currencies transition to becoming fiat currencies (i.e., those that can be used for payments, as the value is backed).

University of California Santa Barbara's Rodney Garratt supported the idea of a government-backed retail-oriented digital currency. To assuage fears that this may too broadly and negatively change the current banking system, he said, "A common objection to expanding access to central bank money [by creating a central bank cryptocurrency] is that it could disintermediate banks. However, it is also plausible that it could produce healthy competition. The risk of excessive disintermediation would be mitigated by making any new form of central bank currency more like cash, and less like deposits."

However, Norbert Michel, director of The Heritage Foundation's Center for Data Analysis, brought up several points against any type of central bank-backed cryptocurrency, saying "the federal government should not step in and tilt the playing field. It should treat cryptocurrency, and all other forms of money, neutrally." He called for a levelling of the playing field to promote competition, and made suggestions such as:

- Not bestowing legal advantage on any particular type of alternative payment systems
- Removing barriers to certain types of payments, such as the capital gains tax from cryptocurrency and foreign currency purchases
- Considering allowing U.S. government agencies to accept these alternative payments

But, using other countries as an example, Eswar Prasad, Senior Fellow at The Brookings Institution, claimed the objective of a digital fiat currency is not to "reduce innovation but to basically provide a backstop to the payment system to make sure it's not all in the private sector and subject to a crisis of confidence."

Questions remained what the specific details of a central bank digital currency would be, including:

- Would the government pay interest on digital currency accounts?
- Would backing a currency mitigate concerns regarding volatility and therefore usability?
- What would cause consumers to turn to a government-backed digital currency?
- Would a government-backed digital currency be less susceptible to Bank Secrecy Act/Anti-money Laundering (BSA/AML) risk than other forms of currency (both private digital currencies and pre-existing fiat currencies)?

Federal Agency Activity

Also on July 18, 2018, Bureau of Consumer Financial Protection (BCFP or CFPB) Acting Director Mick Mulvaney announced Paul Watkins as director for the newly created Office of Innovation. The Office of Innovation will replace Project Catalyst, but shares the stated objective of promoting "consumer-friendly innovation" in consumer financial services.

Mulvaney has stated that he expects the Office of Innovation to examine regulation options for cryptocurrencies, blockchain technology and microlending (i.e., peer-to-peer loans which individuals, rather than banks, issue).

Watkins previously led fintech initiatives in the Arizona Attorney General's Office, helping to create and manage the first state-supported fintech regulatory sandbox program. The extent to which the Office of Innovation will fully adopt Arizona's sandbox approach — in which companies can test products while subject to reduced regulatory requirements, but under close supervision — remains to be seen, but Watkins's appointment could signal that this is the intended direction for the unit.

In the last month, other developments in the cryptocurrency feild amongst U.S. regulators included:

- On July 6, 2018, Financial Industry Regulatory Authority (FINRA) issued a regulatory notice regarding developments in the digital asset marketplace and encouraged any firm to promptly notify FINRA if the firm, or its associated persons or affiliates, currently engages, or intends to engage, in any activities related to digital assets, such as cryptocurrencies and other virtual coins and tokens.
- On July 16, 2018, the FSB published a report that sets out the metrics the agency will use to monitor crypto-asset markets as part of its ongoing assessment of vulnerabilities in the financial system.
- On July 18, 2018, CFTC Director of LabCFTC and Chief Innovation Officer Daniel Gorfine testified on cryptocurrency before the House Committee on Agriculture.
- On July 24, 2018, FATF published a report to G20 Finance Ministers and Central Bank Governors regarding money laundering and terrorist financing risks from crypto-assets, and the urgency of action to address these risks.
- On July 27, 2018, FINRA issued an investor alert titled "The Ins and Outs of Initial Coin Offerings."

OVERVIEW: IMPORTANT QUESTIONS

Is inflation a threat for cryptocurrencies?

Inflation in each cryptocurrency depends on production rate, demand and limitation. If new units of a cryptocurrency are generated, there is some degree of automatic inflation as the supply rises. One of the top cryptocurrencies, for example, has a yearly expansion rate (in terms of supply) of 4 percent. But the demand for this currency is rising faster than the amount of new currency generated. Also, the amount of rewarded currency per block decreases over time. There is a possibility of reproduction and splitting because most cryptocurrencies are based on a publicly open protocol. This has inflationary potential.

Does technological development threaten the security of cryptocurrencies?

Malware, viruses or trojans represent threats, as they are designed to hack the private key and access the digital account. It remains to be seen how fast quantum computers are developed and become market ready, as their computing capacity is capable of encrypting the coding of transactions. This is ultimately a race against time: the cryptographers of cryptocurrencies must make their systems safer to be protected against all kind of external attacks.

Is it possible to hack the blockchain technology?

The security of blockchains is guaranteed by a decentralized system without a central data base. The blockchain is also protected by cryptography which modern computing capacity cannot hack. Each block that is added to the blockchain has its own encrypted identity and is visible for each user after it has been confirmed. As each block has its own visible encryption, this makes it impossible for hackers to gain access and alter the hash code in one block, as each alteration is easily visible.

Are cryptocurrencies scalable and sustainable?

For a few cryptocurrencies, scalability is questionable. Rising demand and block size impact both time to confirm transactions and transaction costs. There are some cryptocurrencies that have strived to solve this problem with a new blockchain structure. Sustainability depends on the mining process for each cryptocurrency. While some currencies' mining demands high amounts of energy, others consume almost no energy as mining is not a feature of the currency.

Are there alternatives to the blockchain?

Blockchain technology is currently in its development process. One weakness is the scalability of each block. However, there are new blockchain developments which appear to have solved this problem.

Why are smart contracts important?

Smart contracts, which use blockchain technology to create, supervise and execute the conditions of a contract, create automation and mitigate human error. The advantage of computers only knowing "yes" and "no" comes in handy: every condition in a contract leads to a decision. Equipped with the right content and algorithms, encrypted data blocks guarantee correct contract observance, and prevent human mistakes during composition and execution.

FUTURE OUTLOOK

Global Cryptocurrency Outlook

- **Cryptocurrencies currently represent a highly speculative and unregulated risk investment.** Because they lack traditional money functions and have scalability problems, we would not assume that cryptocurrencies replace fiat currencies. However, regulated cryptocurrencies could be introduced as an addition to real currencies (as seen in Dubai).
- **Cryptocurrencies could develop into a new asset class in the future.** But for this purpose, more regulation and some degree of security needs to be implemented, to provide more trust, transparency and security to investors.
- **Main factors affecting the future development of cryptocurrencies are likely to be government intervention and competition between cryptocurrencies.** In addition, central banks could develop their own cryptocurrencies and replace the private ones in the market.
- **Cryptocurrencies will raise further attention.** Especially in crisis countries, they could represent an alternative to inflation-threatened currencies. It will be very interesting how the blockchain technology evolves beyond cryptocurrencies in the public and financial sector.

Global Blockchain Outlook

- **The opportunities associated with blockchain technologies are huge.** Bigger banks are likely starting to implement the technology in their systems.
- **The dsiruptive nature of blockchain has the potential to change the financial sector in a sustained way.** We see major opportunities for stock markets and trading.
- **Blockchain could protect elections from hacking.** Agreements with employers, government or companies directly, and the registration of rights on ideas, inventions or digital goods are also possible with the technology.

Alternate Blockchain Utilization

Electric Vehicles
There is a German energy supplier that developed the usage of blockchains as charging stations for electric cars.

Trading
One trading floor giant introduced a blockchain-backed service mainly used for authentications.

Bond Markets
First successful tests based on smart contracts include a German auto company that issued the first blockchain debt certificate, and a Japanese financial information supplier issued the first bond with one of the top virtual currencies.

Virtual/Digital Currencies
Central banks' digital currencies could change the business model of banks fundamentally: some banks are designing a cryptocurrency to help bankers, making stock broking faster and cheaper.

Public Administration
General administration and elections could become tamper-proof by utilizing blockchain technology.

Music Industry/Copyright Infringement:
Music can be published and purchased securely in a digital format.

Conclusion

Blockchain technology and cryptocurrency have separate implications. Blockchain, in some senses, can be more easily applied to our understanding of a future landscape.

Distinguished by high transparency and a decentralized system, we see in the blockchain one of the most innovative developments in recent years. We expect that the blockchain will change the business model of companies in a sustained way. The blockchain technology enables a faster and cheaper exchange of assets and financial products between individuals without an intermediate, which reduces the asymmetry of information between the individuals.

Furthermore, while cryptocurrency uses blockchain technology as its core technology, it is important to remember that digital currency currently has no general acceptance. No one needs to take this type of currency as a payment method, and the effectiveness of these digital currencies varies from moment to moment and country to country.

Both cryptocurrency and blockchain will remain in the spotlight, especially as regulators continue debating appropriate safety measures, governments continue researching fiscal security implications and market participants continue striving for rewarding innovation. ❖

ENSURING FAIR CREDIT REPORTING ACT COMPLIANCE

Financial Institutions' Role and How to Get it Right

Credit reporting remains in the legislative and regulatory spotlight following a 2017 breach at one of the nation's biggest credit reporting agencies. This has not just occured at the federal level; state legislators have concentrated on the credit agency reporting process as well, although more focused on the consumers' role. This article will reinforce how financial institutions play into the credit reporting process; address some best practices in the space; and cover recent developments.

FINANCIAL INSTITUTIONS' ROLE

The Fair Credit Reporting Act (FCRA) and its implementing regulation, Regulation V, contain provisions to help ensure that the information circulating about consumers' finances (e.g., information contained in consumers' credit reports) is accurate and handled properly. Financial institutions are generally both users and furnishers of consumer report information.

- They are "users" subject to the permissible purpose requirements because they obtain consumer reports for a variety of tasks such as underwriting credit.
- They are "furnishers" subject to the many requirements of providing information to the consumer reporting agencies (CRAs), which becomes part of the consumer report.

The FCRA imposes an affirmative obligation on furnishers to ensure the "accuracy and integrity" of the data they supply to CRAs. However, as financial institutions play this dual role, they have struggled to ensure this "accuracy and integrity."

THE DIFFICULTY OF ENSURING 'ACCURACY AND INTEGRITY'

Information is largely technology and system driven, making it susceptible to the common pitfall of placing excess reliance on the system to take care of correcting discrepancies. In addition, different types of credit information (e.g., credit versus deposit account information) furnished to different types of CRAs require distinctive approaches to gathering and providing information.

This can result in significant variances in the type, frequency and nature of information furnished, and may even require different reporting formats and codes. Many of these processes are complicated and challenging.

COMMON CAUSES OF REPORTING INACCURATE OR INCOMPLETE DATA

- System incompatibilities causing data to be lost in transmission between platforms
- Furnisher policies and procedures not tailored to each different type of reporting
- Validation and periodic check-ins not completed to verify that systems were set up properly and that they continue to operate as desired
- Failure to update technology as needed
- Human error when handling/transferring data
- Human error based on inadequate training and a lack of understanding of requirements
- A lack of monitoring and testing, preventing the institution from identifying gaps or errors and correcting the root cause to prevent recurrence
- Inadequate vendor oversight

Inaccurate information can lead to inaccurate reports and cause harm to consumers, including inability to receive credit, housing or employment. These are some of the reasons consumers may dispute information on their credit reports to either CRAs or furnishers. Either way, this provides a direct investigation requirement for furnishers.

RECENT DEVELOPMENTS

On July 12, the Senate Banking, Housing and Urban Affairs Committee held a hearing where representatives from the Bureau of Consumer Financial Protection (BCFP or CFPB) and the Federal Trade Commission (FTC) provided testimony on the FCRA and credit reporting.

- Associate Director for the Division of Privacy and Identity Protection at the FTC Maneesha Mithal stated, "vigorous enforcement of the FCRA continues to be a top priority."
- Assistant Director for the Office of Supervision Policy, Supervision, Enforcement and Fair Lending at the CFPB Peggy Twohig highlighted the agency's *Supervisory Highlights Consumer Reporting Special Edition* from March 2017. The agency issuance splits its focus between CRAs and furnishers. For furnishers, the *Supervisory Highlights* address items such as data governance, policies and procedures, data accuracy requirements and dispute handling requirements. The report also states: "[CFPB] will continue to prioritize new and existing FCRA areas based on insights from a robust number of data sources that help us to identify areas where the risk of consumer harm is greatest."

A recent CFPB enforcement action highlights some of the problems related to furnishers.

On June 13, 2018, the CFPB entered into a consent order with a South Carolina corporation and its subsidiaries in their capacity acting as information furnishers to CRAs. The consent order related primarily to violations under the FCRA and Regulation V. In its investigation, the CFPB found that the furnisher failed to establish and implement reasonable credit reporting policies and procedures; failed to update and correct inaccurate credit reporting; and failed to furnish the date of first delinquency.

Specifically, the CFPB found that the furnisher did not have strong enough policies and procedures, including: coding customer account information or responses using the industry data specification; addressing standard data reporting formats or standards about transmission to consumer reporting agencies; maintaining records for a reasonable amount of time; deleting, updating or correcting information in their own records; and confirming the accuracy and integrity of the consumer information.

In the past, when the furnisher determined updates or corrections were needed, it was slow to make changes, with systemic changes taking more than a year to update and correct in some instances. This contributed to the furnisher overwriting corrected information with incorrect information on its internal system in some instances or, in other instances, refurnishing the same information already determined to be inaccurate.

Among other things, the consent order stipulated the furnisher must implement and maintain reasonable written policies and procedures regarding the accuracy and integrity of the information they furnish to CRAs, taking into consideration the guidelines laid out in Appendix E of the Furnisher Rule. The furnisher is also required to review its policies and procedures at least annually; make periodic updates; notify those consumers affected; and provide redress options, free of charge.

BEST PRACTICES: POLICIES AND PROCEDURES

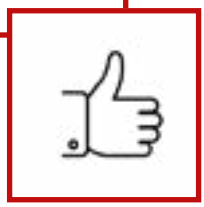
- Reflect the nature, size, complexity and scope of an institution's activities
- Review periodically and update when necessary
- Ensure information is for the correct person, and reflects the terms of the account and the consumer's performance on the account
- Establish internal controls for the accuracy and integrity of information, such as through random sampling
- Prevent re-aging and duplicative reporting, particularly following sales, mergers or other transactions
- Ensure dispute-handling agents perform a reasonable reinvestigation and that it is completed timely instead of responding "verified" upon receipt

BEST PRACTICES: DISPUTE HANDLING

- Establish a process to modify, delete or permanently block inaccurate, incomplete or unverifiable information
- Ensure every CRA which received inaccurate or incomplete information receives the correct information
- Determine if there is additional information provided in a direct dispute notice that a consumer had not included in the previous dispute to help understand whether a furnisher should reinvestigate
- Report the results of direct dispute investigations to consumers, even in unorthodox situations, like bankruptcy
- Test systems to ensure unique situations do not cause glitches in reporting direct dispute investigations

BEST PRACTICES: DATA ACCURACY

- Delete, update and correct information in a prompt manner, including payment information
- Conduct reasonable investigations when disputes are received
- Utilize communication with CRAs that prevents duplicative reporting of accounts, erroneous information with wrong consumers and other occurrences that may compromise the accuracy or integrity of information provided to CRAs
- Implement effective oversight of third parties whose activities may affect the accuracy or integrity of consumer information
- Pay special attention to the furnishing of specific items, such as: Credit Limits, Disputed Information, Closed Accounts, Delinquent Accounts and Negative Information



CONCLUSION

Financial institutions should proactively perform an FCRA compliance self-assessment to self-detect and correct weaknesses or non-compliance. The big question institutions must ask themselves is: "Are we in full compliance with FCRA as both a furnisher and a user, and is our compliance management system ready to demonstrate how our institution mitigates FCRA risks and prevents problems?"

Capco will continue to closely monitor regulatory activity on this topic, not only at the federal level, but also as states become more active in the space. ❖

ABOUT CAPCO

Capco is a global business and technology consultancy dedicated to the financial services industry, plus a dedicated energy division. Capco delivers innovative solutions in Banking & Payments, Capital Markets and Wealth & Asset Management, designed to withstand market forces, continual regulatory change and increasing consumer demand.

WORLDWIDE OFFICES

Bangalore	Hong Kong	Singapore
Bratislava	Houston	Stockholm
Brussels	Kuala Lumpur	Toronto
Chicago	London	Vienna
Dallas	New York	Warsaw
Dusseldorf	Orlando	Washington, DC
Edinburgh	Paris	Zurich
Frankfurt	Pune	
Geneva	São Paulo	

CONTACT US

Capco Center of Regulatory Intelligence
1101 Pennsylvania Ave., NW Suite 300
Washington, DC 20004
E: capco.cri@capco.com
P: 202.756.2263

@CAPCO

WWW.CAPCO.COM

© 2018 The Capital Markets Company NV. All rights reserved.

CAPCO