Cryptocurrency and Cybersecurity

September 12, 2019

Continuing Legal Education

CLE Notice: This presentation is an accredited program under the regulations of the Iowa Supreme Court Commission on Continuing Legal Education. This program will provide a maximum of 1 hour of regular credit toward the mandatory continuing legal education requirements established by Rules 41.3 and 42.2. [Activity #328453]
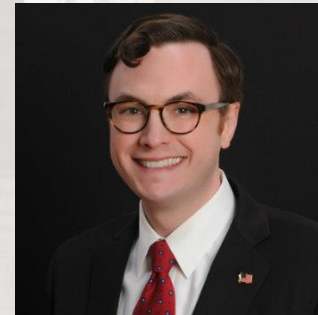
Today's Presenters:

Michael J. Neuerburg
(319) 896-4116
mneuerburg@spmblaw.com

Eric J. Langston
(319) 896-4074
elangston@spmblaw.com

Cryptocurrency

Though seemingly obvious: What is Currency?

- A widely accepted token that can be exchanged for goods and services

- Currency functions as a medium of exchange based on trust
  - If I accept what you give me, then I need to *trust* that I can subsequently use it for future exchanges

- "Money isn't a material reality - it is a psychological construct"

- "Money is accordingly a system of mutual trust, and not just any system of mutual trust: money is the most universal and most efficient system of mutual trust ever devised"
  - "Sapiens A Brief History of Humankind" by Yuval Noah Harari

Types of Currency

- Commodity money – Value derives from the item's material or people's *perception* of the item's value
    - Coins made of precious metals
    - Cowry shell (historic international non-fiat currency)
- Representative money – Value derives from the thing it represents
    - Gold or silver-backed certificates
    - Certificate for goods held at a warehouse
- Fiat currency – Value derives from it being back by government
    - US Dollar, Euro
- Virtual currency ??

What is a Virtual Currency?

- Digital medium of exchange that does not have legal tender status in any jurisdiction

- Examples
    - Cryptocurrencies (Bitcoin, Ethereum, Ripple, and many others)
    - Frequent flyer miles
    - Microsoft or Nintendo points
    - Gold in World of Warcraft

- Similar to commodity money in that the value partially derives from people's perception of the currency, but virtual currencies have no intrinsic value
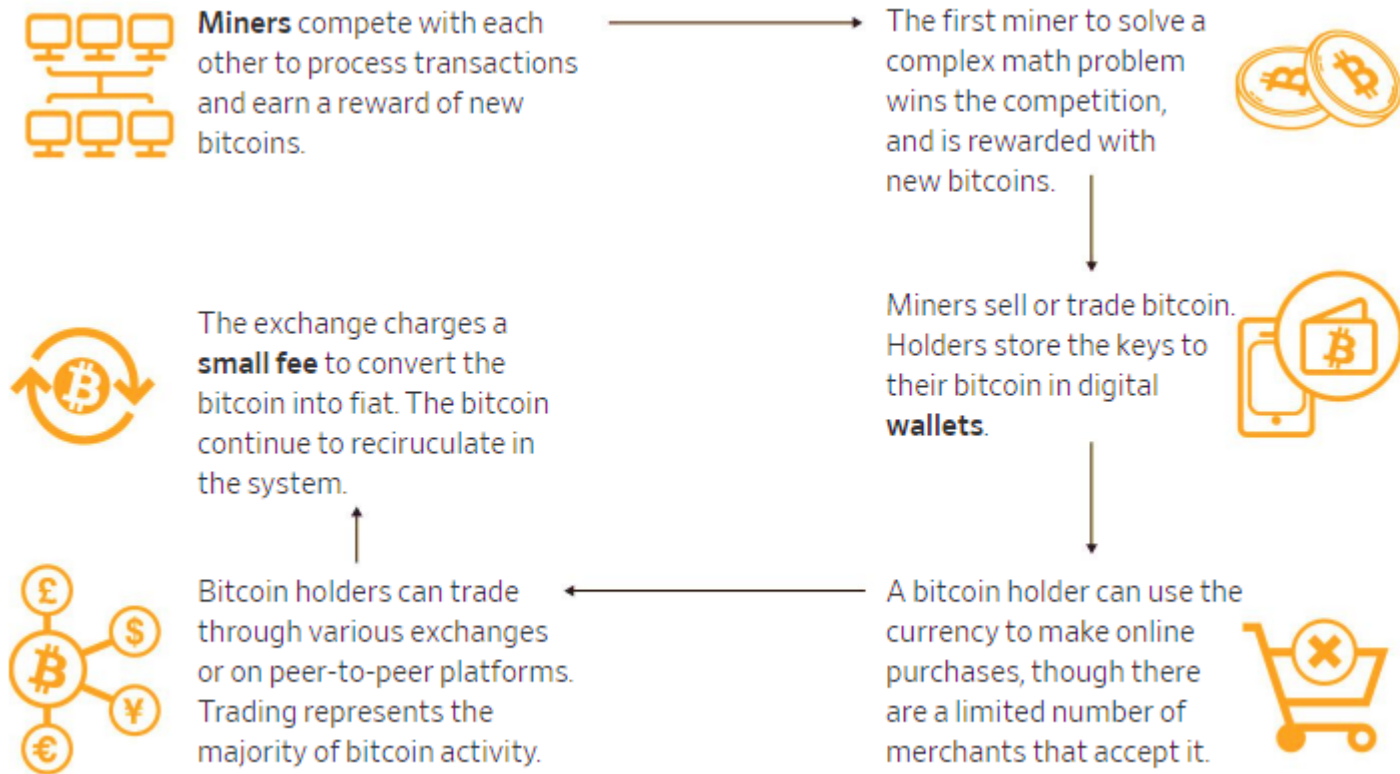
How are Cryptocurrencies Different?

- Cryptocurrencies are decentralized
    - No central repository
    - No single administrator
    - Distributed system of trust

- Cryptography is used
    - To secure accounts
    - To secure transactions
    - To control the creation of new currency units

How Does Bitcoin Work?

Miners compete with each other to process transactions and earn a reward of new bitcoins.

The first miner to solve a complex math problem wins the competition, and is rewarded with new bitcoins.

Miners sell or trade bitcoin. Holders store the keys to their bitcoin in digital **wallets**.

A bitcoin holder can use the currency to make online purchases, though there are a limited number of merchants that accept it.

Bitcoin holders can trade through various exchanges or on peer-to-peer platforms. Trading represents the majority of bitcoin activity.

The exchange charges a **small fee** to convert the bitcoin into fiat. The bitcoin continue to reciruculate in the system.

Credit: https://www.wsj.com/articles/facebooks-libra-cryptocurrency-how-it-stacks-up-to-bitcoin-and-paypal-11561714204

Practical Differences Between Bitcoin and Dollars

- **Bitcoin is very volatile**

- **Time to resolve bitcoin transactions can be hours**
  - Resolving a transaction requires that it be included in a "block" and the transactions selected for inclusion depend on how much of a "miner fee" is offered. Transactions with lower fees take longer to clear.

- **Bitcoin mining requires significant resources**
  - Estimated energy consumption for bitcoin mining is equivalent to the total energy consumption of the Czech Republic (pop. 10.6 million), and while some of this is green energy, much is not
  - Profitable mining requires specialized computing hardware that can quickly become obsolete

Technical Challenges of Decentralized Currency

- No central arbiter to validate ownership
- Banks validate ownership through
  - Possession
  - Documentation
  - Customer contact
  - Passwords/PINs/Biometrics
- Bitcoin validates ownership through public key cryptography
  - One-way mathematical operation also used for secure messaging
  - Anyone can transfer bitcoin to an account (public key)
  - Only the owner can transfer bitcoin out of the account (private key)
    - If anyone else has the key, they own your account
    - If you lose your key, your bitcoin are gone forever

Technical Challenges of Decentralized Currency

- No central arbiter to validate transactions

- Banks validate transactions for their customers
    - Centralized private ledger

- Bitcoin validates transactions through the blockchain
    - Distributed public ledger (processes ~7 transactions/second)
    - But, Elixxir was designed to increase speed and decrease energy

- Spikes in unrelated activity may slow processing
    - Dec 2017 – the Ethereum network was overrun by a surge in the trading of virtual kittens
    - https://blogs.wsj.com/cio/2017/12/08/the-morning-download-ethereum-blockchain-faces-test-as-cryptokitties-go-viral/
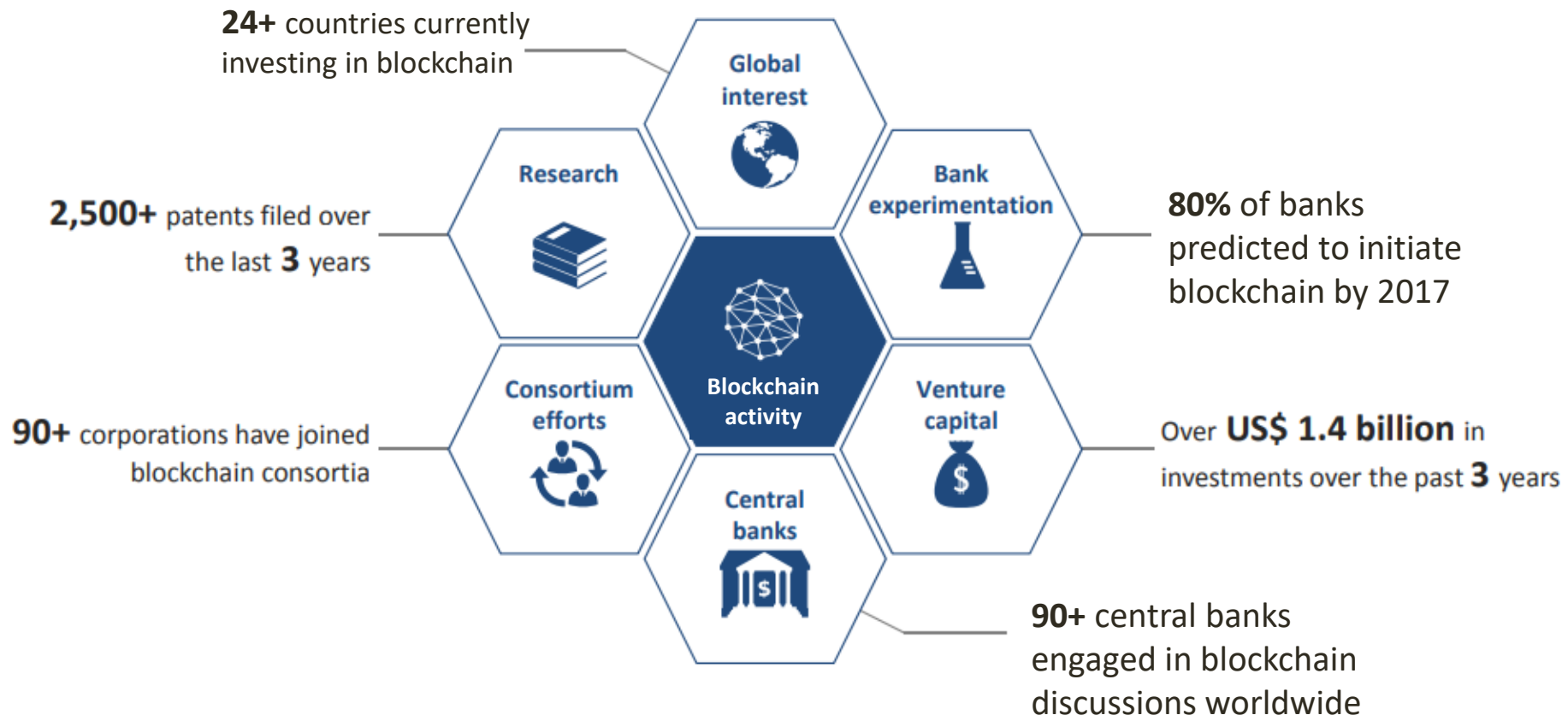
Blockchain

Blockchain Basics

- Transactions records are encoded in a "block"

- Blocks are distributed and validated by a peer-to-peer network using cryptographic means

- Blocks are "confirmed" upon inclusion in the blockchain

- Each block depends on every block that has come before it

  - Retroactive changes to transactions are impossible without majority agreement, but networks may be susceptible to "51%" attacks

  - July 2016: Etherium implemented a "hard fork" to undo a $60m theft

- "Mining" – Doing the cryptographic calculations necessary to include a block in the blockchain in exchange for a reward

Blockchain has captured the imaginations, and wallets, of the financial services ecosystem.

24+ countries currently investing in blockchain

Global interest

2,500+ patents filed over the last **3** years

Research

Bank experimentation

80% of banks predicted to initiate blockchain by 2017

Blockchain activity

90+ corporations have joined blockchain consortia

Consortium efforts

Venture capital

Over **US$ 1.4 billion** in investments over the past **3** years

Central banks

90+ central banks engaged in blockchain discussions worldwide

Source: http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf

Applications of blockchain will differ by use case, each leveraging the technology in different ways for a diverse range of benefits

Examples of blockchain value drivers and benefits

Use case	Value driver	Benefits
Trade finance	Operational simplification	Enables real-time multi-party tracking and management of letters of credit, and enables faster automated settlement
Automated compliance	Regulatory efficiency improvement	Provides faster and more accurate reporting by automating compliance processes that draw on immutable data sources
Global payments	Settlement time reduction	Enables the near real-time point-to-point transfer of funds between financial institutions (FIs), removing friction and accelerating settlement
Asset rehypothecation	Liquidity and capital improvement	Provides market participants with an improved line of sight into assets, enabling improved risk evaluation and decision-making

Syndicated Loans

Summary

Utilizing DLT to automate syndicate formation, underwriting and the disbursement of funds (e.g. principal and interest payments) can reduce loan issuance time and operational risk

Regulator — *Lead Arranger* — *Requesting Entity* — *Syndicate*

Implications for FIs

- Forming syndicates through smart contracts can increase speed and provide regulators with a real-time view to facilitate AML/KYC

- Performing risk underwriting through DLT can substantially reduce the number of resources required to perform these activities

- Smart contracts can facilitate real-time loan funding and automated servicing activities without the need for intermediaries

Critical conditions for implementation

- Building risk rating framework for syndicate selection
- Standardizing diligence and underwriting templates
- Providing access to financial details on the distributed ledger

Trade Finance

Summary

Utilizing DLT to store financial details can facilitate the real-time approval of financial documents, create new financing structures, reduce counterparty risk and enable faster settlement

Correspondent Banks — *Importer* — *Import Bank* — *Customs* — *Exporter* — *Freight* — *Export Bank* — *Inspection Company*

Implications for FIs

- Storing financial details on the ledger can automate the creation and management of credit facilities through smart contracts

- DLT can improve real-time visibility to the transaction to better institute regulatory and customs oversight

- Utilizing DLT will enable direct interaction between import and export banks, and eliminate the role of correspondent banks

Critical conditions for implementation

- Providing transparency into trade finance agreements
- Enabling interoperability with legacy platforms
- Rewriting regulatory guidance and legal frameworks

SPMB

SIMMONS PERRINE MOYER BERGMAN PLC

Other Potential Uses for Blockchain Technology

- Banking
  - Clearing and settlement
  - Equity and debt issuance
  - Reference data
- Online voting
- Tracking use of and payments for digital files
- Blockchain technology "is not a panacea; instead it should be viewed as one of many technologies that will form the foundation of next-generation financial services infrastructure"
  - "The Future of Financial Infrastructure: An ambitious look at how blockchain can reshape financial services" by the World Economic Forum, August 2016
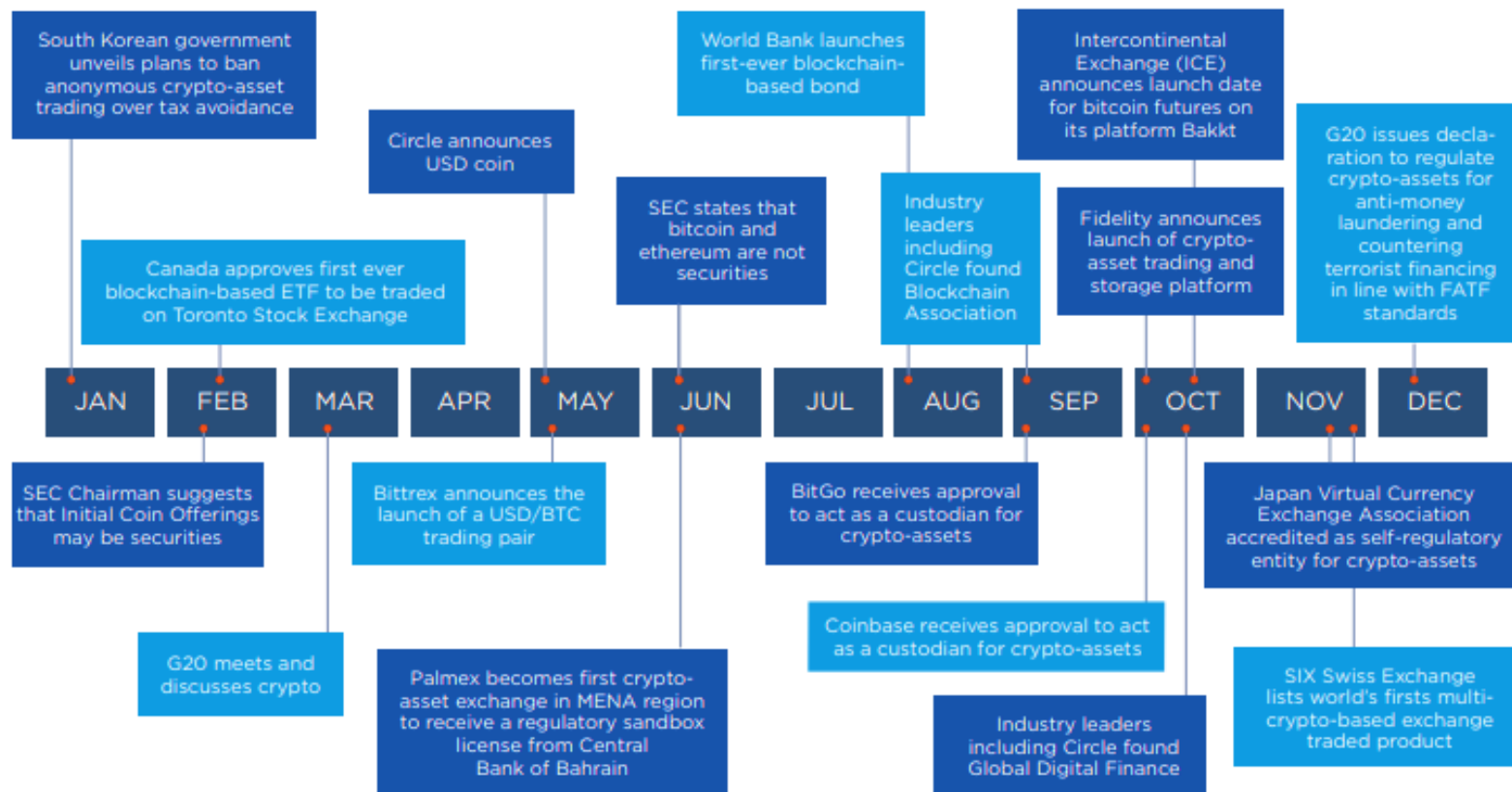
Regulatory Considerations

SPMB

SIMMONS PERRINE MOYER BERGMAN PLC

www.spmblaw.com

2018: Notable Developments

Timeline (JAN–DEC)

Above timeline:
- South Korean government unveils plans to ban anonymous crypto-asset trading over tax avoidance
- Circle announces USD coin
- Canada approves first ever blockchain-based ETF to be traded on Toronto Stock Exchange
- SEC states that bitcoin and ethereum are not securities
- World Bank launches first-ever blockchain-based bond
- Industry leaders including Circle found Blockchain Association
- Intercontinental Exchange (ICE) announces launch date for bitcoin futures on its platform Bakkt
- Fidelity announces launch of crypto-asset trading and storage platform
- G20 issues declaration to regulate crypto-assets for anti-money laundering and countering terrorist financing in line with FATF standards

Below timeline:
- SEC Chairman suggests that Initial Coin Offerings may be securities
- Bittrex announces the launch of a USD/BTC trading pair
- BitGo receives approval to act as a custodian for crypto-assets
- Japan Virtual Currency Exchange Association accredited as self-regulatory entity for crypto-assets
- G20 meets and discusses crypto
- Palmex becomes first crypto-asset exchange in MENA region to receive a regulatory sandbox license from Central Bank of Bahrain
- Coinbase receives approval to act as a custodian for crypto-assets
- Industry leaders including Circle found Global Digital Finance
- SIX Swiss Exchange lists world's firsts multi-crypto-based exchange traded product

Credit: https://www.fireeye.com/content/dam/fireeye-www/partners/pdfs/rpt-marsh-fireeye-crypto-paper.pdf

Regulatory Treatment of Virtual Currencies

- U.S. Treasury Financial Crimes Enforcement Network ("FinCen") defines virtual currency as a medium of exchange that operates like currency in some environments, but does not have all the attributes of real currency

- IRS treats virtual currency as "property" for federal tax purposes
  - Notice 2014-21, but in April 2019, 20 lawmakers requested updated guidance

- U.S. Securities and Exchange Commission treats the offering of virtual currency (an "ICO")as the sale of "securities" under certain circumstances

- U.S. Commodity Futures Trading Commission treats derivative contracts based on virtual currency as "commodities" under certain circumstances

How do Regulators Define or Treat Virtual Currency?

- U.S. Bank Secrecy Act ("BSA"): primary federal statute governing anti-money laundering ("AML")requirements for financial institutions

  - Applies to "money service businesses" ("MSBs") operating as money transmitters

  - An "administrator" or "exchanger" of virtual currency is a money transmitter subject to BSA and FinCen regulations and guidance thereunder

  - BSA requires MSBs to adopt an AML compliance program and file suspicious activity reports ("SARs")

  - FinCen is taking an aggressive approach to BSA examinations. Speech of FinCen Director Kenneth Blanco on August 9, 2018 outlined concerns

How do Regulators Define or Treat Virtual Currency?

- State Money Transmitter Laws: these laws generally apply to receiving money or monetary value for transmission and require licensing and adherence to certain capital and other requirements. Applies to "money service businesses" ("MSBs") operating as money transmitters

  - Virtual currency platforms must determine whether their activities constitute "money transmission" in each state they offer their services

  - Only a small number of states have amended their money transmitter statutes or otherwise issued guidance addressing whether virtual currency activities constitute money transmission

  - New York Department of Financial Services issued rules on June 3, 2015 creating a "BitLicense" comprehensive framework for the licensing and regulation of virtual currency activities

  - Some virtual currency platforms (e.g., itBit) have opted to obtain a trust company charter to market "custodial" activities and avoid money transmitter laws

What Issues Exist for Banks Dealing with Those in the Virtual Currency Business and Bank Customers Seeking to Invest in Virtual Currency?

- Banks are subject to BSA "Know Your Customer" and AML requirements and fear potential liability for failing to police unlawful bank account activities involving virtual currency

- Concern that bank customers buying virtual currency on credit card or by other bank means may have "buyer's remorse" because of price volatility and put the bank in the middle and seek chargeback

Consumer Risks in Virtual Currency Transactions

- The significant consumer protection laws applicable to traditional payment systems do not apply to virtual currency transactions

- Concern that consumers do not appreciate how virtual currency works and the risks involved

Consumer Protection for Investors in Virtual Currencies

- Major losses involving virtual currencies:
  - Mt. Gox
    - Bitcoin exchange, handled ~70% of global bitcoin trades in 2013 and early 2014
    - Suspended trading in February 2014, admitted that it had lost ~$450MM in customers' bitcoin
    - Loss appears to be a combination of fraud and theft
  - Bitfinex
    - Large bitcoin exchange, lost $72MM in customers' bitcoin in 2016 in an apparent security breach
    - Has had difficulty maintaining a relationship with traditional banks, does not disclose to customers where fiat money is kept

Consumer Protection for Investors in Virtual Currencies

- Major losses involving virtual currencies:

  - QuadrigaCX

    - Canadian virtual currency exchange

    - Founder and CEO was responsible for keeping majority of customers' cryptocurrency in cold storage (offline)

    - Founder passed away in 2018 and company has been unable to access the $190MM in cryptocurrency stored offline

- Countless smaller frauds and scams involving bitcoin and other cryptocurrencies

Consumer Protection for Investors in Virtual Currencies

- Trend toward "know your customer" regulations for virtual currency exchanges and trading platforms reduces anonymity and makes fraud more difficult

- Computer Fraud and Abuse Act (CFAA)
    - Provides a private cause of action for "hacking-type" attacks on virtual currencies
    - Can file "John Doe" complaints and use civil discovery to subpoena virtual currency exchanges, ISPs, etc.

- Commodities Futures Trading Commission
    - Broad anti-fraud and anti-market-manipulation powers
    - CFTC treats bitcoin as a "commodity" under the Commodity Exchange Act
    - CFTC has filed charges against persons involved in Ponzi schemes and other fraud using bitcoin

Cybersecurity

Global Cybersecurity in Banking

- No financial institution is safe
    - Institutions large and small are under attack
    - Hacking
    - Phishing/social engineering
    - Destructive malware/ransomware
    - Attacks on third-party partners/vendors
- Engaging in new areas of business brings new risks
    - Cryptocurrency exchanges are already targeted

The Cost of a Data Breach:
2018 Ponemon Institute Study

Global study at a glance

> Average total cost of
a data breach:

$3.86 million

> Average cost per lost or
stolen record:

$148

> Likelihood of a recurring material
breach over the next two years:

27.9%

> Average total one-year
cost increase:

6.4%

> One-year increase in
per capita cost:

4.8%

> Average cost savings with an
Incident Response team:

$14 per record

Financial Institutions: $206 per breached record vs. $148 average

Source: Cost of a Data Breach Study, sponsored by IBM, conducted by Ponemon Institute LLC (July 2018), available at
https://www.ibm.com/security/data-breach.

Direct vs. Indirect Costs

- Direct Costs (35% of breach costs)
  - Engaging forensic experts, hiring a law firm, hiring PR firms, creating breach hotline, or offering victims identity protection serves

- Indirect Costs (65% of breach costs)
  - Employees' time, effort, and other organizational resources, internal investigations, costs to notify victims, loss of goodwill and customer churn

Cybersecurity Misconceptions

- Cybersecurity is not just IT's job
  - Substantial fraction of data breaches are due to employee acts, either accidental or maliciously induced
  - Security requires ongoing training and vigilance
  - Company culture of security should come from the top
- Preventing intrusions can't be the only focus
  - No security is perfect
  - Without strong programs for breach detection and monitoring you may not even know you've been compromised
  - Today's detection is tomorrow's prevention
  - *Have (and practice) an incident response and recovery plan*
- Regulator tools and exams (e.g. FFIEC Cybersecurity Assessment) are helpful but are not sufficient. Regulators are not at the cutting edge of cybersecurity

Key Ingredients for Cybersecurity

- Culture of security (physical, behavioral and electronic)

- Capable and empowered IT department

- Regular training and security audits

- Incident response and recovery plan

- Insurance

  - Coverage for data breaches may exist under umbrella policies, but specific policies help eliminate costly coverage disputes

  - Insurers are litigating coverage for cyber-attacks

    - Whether cyber-insurance covers incidents of "social engineering," i.e. when a fraudster tricks an employee into wiring funds improperly

    - Whether "war exclusions" exclude coverage for state-sponsored cyberattacks

Incident Response Plan: Plan Goals

- Identify

- Assess

- Contain

- Remediate

- Recover

- Notify

Incident Response Plan: The Response Team

- Who makes up the IR team?

    - Information Security

    - Internal Stakeholders (e.g., IT, HR, Compliance, Finance, Marketing)

    - External stakeholders (outside counsel, forensics, PR, insurance)

    - Senior leadership (C-suite, board, etc.)

Legal Issues with Cybersecurity

- Patchwork of regulations and oversight results in compliance difficulties

  - Multiple agencies at the state and local level with varied approaches and overlapping mandates

    - Federal Financial Institutions Examination Council ("FFIEC") – provides a cybersecurity assessment tool for financial institutions

    - New York Department of Financial Services ("NYDFS") – leader in state-level cybersecurity regulation for financial institutions

    - National Association of Insurance Commissioners ("NAIC") – model law requires risk assessments

    - Financial Services Sector Coordinating Council ("FSSCC") – has attempted to synthesize standards into a single assessment tool

  - Lack of central guidance makes demonstrating compliance complex and costly

  - Regulations can be impractical or even outright harmful (e.g. rigid vs. risk-based scoring systems)

Legal Issues with Cybersecurity

- Response and recovery to data breaches
  - Regulatory compliance re: investigation and recovery
  - Notifications to and from business partners/vendors
  - Notifications to regulators and affected customers, e.g. Iowa Code § 715c
    - § 715c requires notice to affected customers
    - If more than 500 Iowa residents are affected, must also give written notice to the Iowa Attorney General's Consumer Protection Division

# Incident Response Plan: Legal Requirements

- Incident response plans should build-in all applicable legal requirements for your organization, including:
    - Required deadlines and content for customer notification
    - Required decision-making criteria for notifications (e.g., affected data client thresholds)
    - Required regulatory reporting and contact info
    - Required follow-up activities and remediation measures

Questions?

Michael J. Neuerburg
(319) 896-4116
mneuerburg@spmblaw.com
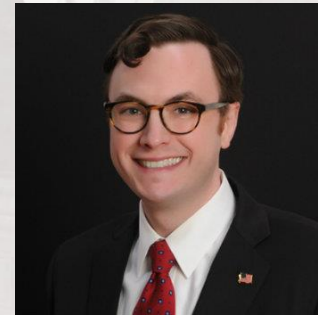
Eric J. Langston
(319) 896-4074
elangston@spmblaw.com

SPMB
SIMMONS PERRINE MOYER BERGMAN PLC

www.spmblaw.com

Disclaimer: This presentation is designed and intended for general information purposes only and is not intended, nor should it be construed or relied on, as legal advice. Please consult your attorney if specific legal information is desired.