LJN LAW JOURNAL NEWSLETTERS

Cybersecurity LAW & STRATEGY

An ALM Publication

January 2018

In This Issue:

Cybersecurity Law & Strategy

January 2018

Volume 2, Number 8

Cybersecurity Law & Strategy

D. Reed Freeman Jr.
Wilmer Cutler Pickering Hale and Dorr LLP
Washington, DC

Alan L. Friel
BakerHostetler
Los Angeles

Collin J. Hite
Hirschler Fleischer
Richmond,VA

David F. Katz
Nelson Mullins Riley & Scarborough LLP
Atlanta, GA

Ari Kaplan, Esq.
Ari Kaplan Advisors
New York

Justin Hectus
Keesal, Young & Logan
Long Beach, CA

Staci D. Kaliner
Redgrave LLP
Washington, DC

Dan Lear
Avvo
Seattle, WA

Kelly Lloyd
McCarter & English
Newark, NJ

Emile Loza
Technology & Cybersecurity Law Group, PLLC
Washington, DC

Ian D. McCauley
Morris James LLP
Wilmington, DE

Jeffrey D. Neuburger
Proskauer Rose LLP
New York

Nicholas A. Oldham
King & Spalding LLP
Washington, DC

Mark Sangster
eSentire
Cambridge ON, Canada

The Uber Breach and the Need for an Independent Privacy Function

By Paige Boshell

The 2016 data breach involving 57 million Uber riders and drivers and the ensuing efforts to conceal the breach appears to have tapped into the public's — and the government's — frustration with a series of increasingly large data breaches experienced by some of our most visible companies and institutions.

Uber has incurred significant legal and reputational exposure as a result of the way that the company handled the breach. In the coming months, there will be a great deal of information and regulatory and judicial action that will act as guidance, or more precisely, a checklist of what-not-to-do, for companies that suffer a data breach.

Regaining Trust: The Chief Privacy Officer

The CEO has announced Uber's intent to put integrity at the core of every business decision and to work to regain the trust of its consumer customers. That commitment, and the steps taken pursuant to that commitment, will be critical to mitigate its legal and reputational exposure and survive the impending inquiries and actions. One key to that commitment should be the development and maintenance of an independent privacy function at Uber.

Although we don't yet know all of the Uber players involved in the breach cover-up, it appears that the breach response was directed by three Uber officers: the CEO; the CSO (chief security officer); and the inside counsel responsible for regulatory compliance and law enforcement. According to news reports, the privacy function was subsumed in the CSO's duties, although presumably inside counsel was also involved in the consideration of the privacy issues posed by the breach. Uber does not, however, have a separate CPO (chief privacy officer).

How would a CPO's involvement have impacted the breach response? It is not possible to know for sure without knowing more about the facts and the decision-making process, but looking at the core functions and motivations of each officer demonstrates a likely need for a CPO.

The Role of the CPO

The CEO's primary duty is to plan and manage the overall business strategy for the company and to manage or oversee management of the related day-to-day activities of the company. The CEO reports to the Board of Directors and has responsibility to the company's owners but, as Uber is not publicly-traded, there is no direct duty to shareholders and no direct regulatory oversight. In a privately-held company where the CEO is the founder and determines the culture and business strategies, it may not be uncommon for the CEO to make independent business decisions involving data breach response. The incentives are to protect the company and its value. This is oversimplified and does not take into account whether or not the CEO had the responsibility to consult with the Board or the investors in this case. The CEO's focus would, however, have been on the company's business objectives.

The CSO protects company data and systems. Generally, the CSO is data-neutral. The business function of the company assigns value to the data and the CSO works to protect it in accordance with the company's objectives. In a data breach situation, the CSO's focus is on containing the breach, protecting company systems, and recovering the data, or ensuring that there is no further disclosure of the data.

Inside counsel is responsible for determining and advising executive management regarding the applicable legal requirements and company compliance. The inside counsel's incentives are to determine the legal requirements applicable to the company's business strategies and practices.

This too is a generalization that does not address all of the counsel's responsibilities in the data breach context, but it should be fair to state that, at a minimum, counsel's focus in that context is on ascertaining the company's legal obligations and advising the CEO and the CSO in that regard.

The CPO's primary duty is to consider the privacy obligations and goals of the company and to align those with the company's business goals. In a data breach situation, the CPO would advise the CEO, counsel and the CSO on developing and implementing the response strategy with respect to the privacy issues implicated by the breach. It is not clear whether or not Uber had a formal data breach response plan in place at the time of the breach, but a CPO would have ensured that there was one and that it addressed the roles and responsibilities of each member of the response team (including the CEO, counsel and the CSO) and provided a formal mechanism for decision-making during the response period.

In this breach response, the CPO's role would have been to consider the legal guidance and the privacy values and objectives of the company. If Uber's commitment had been to transparency and fairness in its privacy decision-making, this may have prompted the CPO to advise: notifying the consumers, even in those cases where notice may not have been technically required; reporting to regulators of U.S. states or municipalities with whom Uber had signed agreements regarding its privacy or security practices; notifying the regulatory authorities in other countries where such notice may have been required; and raising the breach and response with the Federal Trade Commission in the course of its enforcement action against Uber for a previous, and not entirely dissimilar, breach.

Further, an independent CPO works with and reports to the CEO but is ultimately responsible to the Board, much like an independent ethics or audit function. In this case, if the CPO had escalated these issues to the Board, there would have been additional oversight of the response strategy.

It appears that there was not one person directly involved in the breach response whose sole, or primary, function was privacy.

Implementing the CPO Role

In order to address regulatory and consumer concerns, Uber should consider putting privacy in the core of its decision-making as well.

A CPO and privacy team that reports separately to the CEO and the Board would ensure the independence of the privacy function and the commitment of the company to privacy. Stated privacy commitments to data minimization, fairness, transparency, access and redress with concomitant build-outs in process and infrastructure, would alleviate concerns about the reoccurrence of concealment efforts in response to a data breach and would also make proactive steps toward a privacy and consumer-focused service. Indeed, consumer riders want the following from Uber: ease and convenience of transport; reasonable pricing; physical safety; and data privacy. By affirmatively committing to enhanced privacy practices favoring consumers, Uber could improve the value of its service and brand.

An Action Plan

An incoming CPO would evaluate Uber privacy practices, including the following:

Geolocation Tracking

Uber has committed to tracking rider locations only while riders are using the Uber app. Is that limited to calling for a ride or requesting pricing on a ride, or is location tracked whenever the app is open?

Minimization of personal data collected and retained

Does Uber collect only the information that it needs to facilitate rides and payments for rides? This relates to the geolocation issue above. What does Uber need to know? The name of the person? Their contact number? Method of payment? Billing information? For example, currently, it appears that you can add payment methods to the app or change primary payment methods, but it is not readily apparent how such payment information may be deleted. This may result in Uber retaining more personal information than it needs to provide the service.

Consumer access and redress

Currently, Uber appears to offer only an automated app response contact for customer care. The options for this care are limited. For example, there appears to be no way to reach a live person or to raise a concern not specified by the app. How does the rider raise a privacy concern? If you have a question about an Uber charge to your payment method, the app asks you for specific transaction information that you would not have if you did not order the ride. And, there is no way to dispute more than one charge at a time. The information fields have to be entered individually for each separate charge. It is easier to file a complaint with the FTC about Uber online than it is to register a complaint directly with Uber.

Security of personal information

Uber has indicated that it masks the rider's telephone number, affording the driver a way to contact the rider without having access to their individual number. How does this work? The driver has the rider's name — is this limited to first name only? What other precautions are taken to protect disclosure of personal information to the driver? Is the transmission of personal information via the app adequately protected from third party interception? Is it encrypted? What other steps are taken during transmission? How is the information secured while maintained by Uber? Does Uber retain only the information necessary to continue providing rides? If a rider deletes the app, is their personal information deleted from Uber systems? If not, how can the rider ensure that this is done? Are there adequate administrative, physical, and technical controls to limit access to the personal information and to ensure its security and integrity?

Conclusion

The above is just a quick highlight of potential privacy issues; these may have already been considered or addressed by Uber. The intent is to illustrate that the CPO can conduct a thorough privacy assessment of current practices and develop a privacy framework and procedures for the company, which may not already be addressed by management or security or legal.

The recommendation is that Uber, and other companies, consider whether or not an independent privacy function would better protect the company from data breaches, botched responses, and other liability and reputational exposure and be used to bolster the company's reputation and value.

*****

Paige Boshell is a partner in the Birmingham office of Bradley Arant Boult Cummings LLP where she serves as team leader for the firm's Cybersecurity and Privacy Team and its related Digital Services and Electronic Contracting Team and Cybersecurity and Financial Privacy Team.

—❖—

How Blockchain Technology Can Drive the Legal Industry Forward

By Dmitry Dontsov

Trust has always been a key instrument of economics. Up until recently, central banks have acted as the metaphorical custodian of trust, employing complex processes that force populations to participate in bank accounts and credit cards to earn trust benefits, like credit scores. Yet, devastating moments such as the 2008 U.S. financial crisis that took an enormous taxpayer-funded bailout showed the same centralized and slow processes were weakening and could not adapt quickly enough in a digital economy. Further, banks have become the number one target for malicious hackers. As a result, banking systems, credit rating agencies and other traditional legal instruments no longer remain effective mechanisms for P2P reputation and trust measurement.

A new legal structure that bestows and monitors trust must be employed. Is decentralization of these traditional, gigantic repositories of data the answer? Is blockchain technology the new path that the legal industry should take to sustain in the digital age? Let us consider the most significant implications of decentralized technologies to the legal industry.

Blockchain is one of the most promising new technologies to emerge from the past decade. Financial institutions, healthcare, public sector and government agencies, manufacturing, and energy companies are all embracing digital business trends. Law firms have commonly lagged behind other industries in adopting new technology, but unlike other technologies, the blockchain is a safer tool for law firms.

Making Businesses Safer

Top billing clients of law firms (financial institutions, healthcare, public sector and government agencies, manufacturing, energy companies) found continued success in the deployment of tech innovations, including cloud-based services, cloud security, Machine Learning, Artificial Intelligence, and robotics — all of which present tremendous opportunities for saving time, boosting savings, and accelerating overhead cost reduction. To bear the changing tide of regulatory requirements, these high net clients have proactively adopted rapid updates with cybersecurity solutions to ensure confidential information remains ironclad against the latest cyber attacks.

Along with securing digital transactions, blockchain technology integration within existing security protocols reduces numerous cybersecurity risks. For instance, DDOS attacks are effective because they send a barrage of requests that eventually overwhelm and take down the targeted servers. However, with the blockchain's decentralized nature, these attacks would be less effective since the information would be stored among a large network in many locations. Blockchain is a sure win for these clients and the law firms that want to be in the role of a secure technology advisor. Blockchain technology can bring a lot of benefits for law firms looking to embrace success in the 21st century.

The legal industry should watch DLT innovations as they are quietly revolutionizing the way people connect and transact. In the next few years, we will see blockchain fundamentally alter the way people:

- Trade commodities, services, and assets without involving third parties (*e.g.*, an exchange) as blockchain provides infrastructure for cross-border transactions.
- Propel various crowdfunding models to break free from investment fund oversight burdens and gain more direct benefits from returns. The idea of the DAO and self-

inserting smart contracts is to democratize early-stage investing in the blockchain environment.
- Provide automatic control over transfer of assets.
- Keep track of land registry and improve deed management.
- Ensure clearing and contract disputes settlement in a digital manner to avoid court procedures.
- Store, exchange, and control access to valuable data and any other PII from the Internet and/or any digital infrastructure.

In addition to these changes, blockchain and DLTs will replace the traditional role of legal professionals by adopting more sophisticated functions, such as becoming an arbiter in dealmaking, advisory, matchmaking, due diligence, assets transfer, financial crime prevention (AML), improving regulatory processes, and other tasks typically associated with legal experts. Three significant pillars in this new "Trust Economy" era have since surfaced: recordation of assets, value exchange, and smart contracts, in which blockchain technology trims the trade lifecycle to a single trade stage. We will explore these pillars more in depth.

Ledger Technologies for Regulatory Reporting and Compliance

Blockchain is practically immutable due to four key characteristics of its architecture, which help eliminate the risk of fraudulent transactions:

1. Data is stored in decentralized locations.
2. Data is immutable. In order to affect the blockchain, bad actors need to delete or change data in all locations.
3. Multiple sources are required for new data to qualify for acceptance into the blockchain.
4. Reducing the number of steps in transactions and confirmation times eliminate chances for a transaction to be compromised.

Today, legal professionals are facing multiple challenges related to regulatory compliance management and globalization. The speed of modern business, enhanced service availability, and fast transactions require clients of law firms to ensure security while easily sharing huge amounts of documents between teams, clients and contractors. At the same time, these organizations need to make sure all compliance and regulatory requirements are duly met, including clarity over jurisdictions as data passes between multiple parties.

Blockchain-based solutions help maintain uniformity, consistency, and accuracy of data, minimize manual intervention into systems and human errors, and make sure compliance is achieved. User authentication with a Public Key Infrastructure (PKI) approach is vulnerable to human errors and numerous types of cyber attacks. Simple logins, password authentication, and centralized IT infrastructures are major vulnerabilities that law firm clients face, and this is why blockchain-based technology should be implemented to protect sensitive data.

Major Cybersecurity Challenges for Lawyers and Law Firms

The legal industry continues to be a major focus for cybercriminals, and the leading cybersecurity solutions providers continue to develop innovative products to solve two significant problems: data loss and data leaks in the cloud. Cyber criminals are targeting law firms because they have access to their clients' most valuable information. The less tech-savvy a law firm is, the more attractive a target it is for cyber criminals, because hackers are able to detect those firms that have weaker security. Data protection is a core element of corporate security, and this is especially true for law firms dealing with clients' sensitive data, which is becoming a bigger target for cyber attacks. Law firms need to implement exceptionally secure

mechanisms to protect content and file sharing to ensure that only authorized partners can access highly confidential documents, including data encryption capabilities or file-level usage rights. Law firms should never assume that they won't be targeted, but instead be cybersecurity-savvy and protect against security breaches as they emerge. Law firms should fight the growing cybersecurity threat since the risks are increasingly evolving. Now, let's take a quick look at the recent top data leaks of the world's largest law practices.

Notable Data Breaches, and Law Firms Victimized

- Hackers are aggressively targeting law firms' data. If you thought hackers were afraid of the guys who can prosecute them, think again.
- Leading offshore firm Appleby admitted it was the victim of a hack in 2016.
- In the Panama Papers scandal, the law firm Mossack Fonseca was basically wiped out of existence after 11.5 million documents were revealed as a result of data leaked to a German publication, *Sueddeutsche Zeitung.* Mossack acknowledged the firm's credibility had been entirely destroyed.
- Cravath, Swaine & Moore and Weil Gotshal & Manges, which represent Wall Street banks and Fortune 500 companies, were attacked in 2016. Hackers penetrated into a computer network and stole the confidential information worth over $4 million for the purpose of insider trading and planned mergers.
- Several law firms in British Columbia, Canada, were infected with ransomware. The companies that were targeted by cyber criminals preferred to remain anonymous to avoid potential reputational damages. Similarly, an Indianapolis-based law firm was infected by ransomware distributed through a spear-phishing email message, containing a malicious attachment impersonating the United States Postal Service.
- Thirty Nine Essex Street fell victim of a cyber attack. Reportedly, the Russian state-sponsored group Energetic Bear was behind it.
- And recently, Deloitte suffered a sophisticated cyber attack, where clients' emails were stolen along with other confidential information.

Ransomware infects organizations through phishing, and law firms need to implement comprehensive information security awareness programs for their employees. Cybersecurity experts recommend using fully automated and sophisticated protection against ransomware for your SaaS data with the help of machine-learning algorithms.

Blockchain-Powered Protection for SaaS Data

There are solution providers that are taking the lead to help law firms secure their data. For instance, a blockchain-based company undertook a crucial initiative to develop a unique Blockchain Single Sign On solution (BSSO), which is a technological answer to these compliance and regulatory challenges. BSSO will automate regulatory and compliance processes, and enable organizations to comply with the standards and federal laws for customers subject to ISO 27001, EU Model clauses, HIPAA BAA, FISMA, and others. Blockchain Single Sign On (BSSO) for G Suite, Office 365 and other leading cloud services is the most secure data leak protection, which provides password-free access to customers' critical SaaS data through an SSL certificate that can be easily installed on any device, with a high level of protection of the certificate itself at all stages. BSSO allows organizations to access and share highly confidential documents securely from anywhere.

Blockchain Single Sign On for Leading Cloud Services

Additional security is added by rethinking the username-and-password model of inputting credentials. Now, there will be password-free access to SaaS data stored in G Suite, Office 365,

and other cloud services based on Single Sign On (SSO) authentication and blockchain. SSO based on certificate authentication has long been deployed in corporate solutions. The X.509 protocol-based certificate is supported by all browsers, OS, and most software products. This method has not been widely adopted yet, since deep technical skills are required for users and administrators, along with the availability of a special PKI, or a Certificate Authorization (CA) service. However, the traditional CA model involves two serious vulnerabilities:

User Identification

Certificates contain user data (email, login, etc.). When issuing a certificate, CA identifies the user requesting the certificate by using the authentication data contained in it. To implement thorough identity checks, most Certificate Authorities require physical authentication documents, such as a SSN, a driver's license, utility bills, etc. This brings inconveniences and limitations of use, such as the service only being provided in some countries. If the Certificate Authority alleviates the identification requirements, it might play into the harmful hands of a cybercriminal who can impersonate the victim, issue fake certificates in their name, and get full access to the victim's cloud services.

Fraudulent Certificates

Legitimacy of a digital certificate is ensured by the secure Root Key issued by CA, which is the principal identifier for all users. If a hacker steals or forges a root certificate, this will enable him to forge certificates of any other user as well. Cybersecurity experts are reporting a growing number of compromised CA certificate attacks. Blockchain-based companies intend to solve the problem of traditional PKI by introducing a unique user identification procedure via leading cloud providers such as Google, Microsoft and certificate recordings in blockchain. SaaS providers verify the digital identity of a certificate holder and ensure that the certificates are requested by the cloud account holder, thus avoiding fraudulent attacks on accounts.

Blockchain companies will save the digital fingerprint of the certificate issued in the blockchain network. The certificate will be transferred to the user and will not be stored by the solution provider. All data required for user authentication will be kept solely by the user. In order to verify the certificate, the checksum needs to match the one stored in the certificate.

Because of the distributed nature of blockchains, this data cannot be falsified, as the checksum ensures the integrity of a digital certificate. That's why blockchain plays a crucial part and creates a unique interaction between cloud providers and the users of blockchain in order to implement a simple and secure way to access cloud data.

Basic Principles of BSSO Solution

- The confirming factor is the permission to access the profile through the API of leading cloud providers such as Google, Microsoft, Salesforce, etc.
- The blockchain-based solution provider doesn't store personal data of its customers. After the certificate is created, the client data is completely deleted from the solution provider's servers.
- The certificate is stored only on the client's device.
- Checksums of certificates are stored in the blockchain decentralized network, therefore, it is impossible to replace the existing certificate or create a fake one.
- The client must have an active account at G Suite or Office 365.

BSSO Is Capable of Re-Engineering Cybersecurity

The blockchain-based provider's solution eliminates the security problems of classic PKI: trust of the certificate is not based on the certificate chain, but on the strict verification of the checksum of the certificate that is stored in the blockchain and cannot be replaced. There is no dependence on the availability of the CRL when the certificate is validated. The data stored in the distributed network block is always available for verification. Compromising blockchain-based solution provider's key does not lead to a compromise of the issued certificates. To verify a user's certificate, the Web service is accessed in blockchain.

Conclusion

Groundbreaking blockchain technology is poised to transform traditional legal services, improve core business processes, facilitate regulatory and compliance procedures, and significantly simplify contract execution. It is clear from the many tangible blockchain use cases that law firms owe it to the profession and their clients to learn more about how disruptive technologies can help them provide cutting-edge services.

*****

Dmitry Dontsov is the CEO and founder of Spinbackup and the former CEO of Optimum-web, where he led the company for 10 years. He is an expert in SaaS data security and has built a successful software development company that was focused on cloud and mobile app development, and has contributed as a CTO in two startups. Dmitry supports early technology and commercialization of data management, protection, and recovery capabilities. He also holds a number of patents and continues to push for market adoption of industry standards-based security and blockchain.

—❖—

Regulators are Catching Up to Cryptocurrency and Blockchain Technology within the Financial Services Industry

By Craig Nazzaro, Brad Rustin and John Jennings

Part Two of a Two-Part Article

The proliferation of cryptocurrency and blockchain is being driven by the efficiencies and protections afforded to early adopters. The operational efficiencies and resulting cost savings are readily apparent in the financial services industry and are equally coveted by the entities trying to implement them and by the customers who will benefit from the implementation. However, neither party can fully enjoy these benefits without first understanding and overcoming the various regulatory hurdles.

By no means is this meant to be an exhaustive discussion of the financial regulatory burdens faced by this technology. To cover the entire regulatory landscape would be too great an endeavor, given what we can cover in this article. In Part II of this article, we will continue to focus on additional common regulatory issues faced by market participants in this space. (See Part One here.)

The U.S. Commodity Futures Trading Commission (CFTC)

The CFTC regulates the futures and option markets within the U.S. financial services industry. In July 2017, the CFTC issued an order granting LedgerX, LLC registration as a derivatives clearing organization (DCO) for BitCoin options (the first of its kind). While this registration further legitimized cryptocurrencies/virtual currencies (specifically BitCoin) by demonstrating acceptance by a federal regulator, the CFTC was sure to include the following language in the press release accompanying the order, "[t]his authorization to provide clearing services for fully-collateralized digital currency swaps does not constitute or imply a Commission endorsement of the use of digital currency generally, or bitcoin specifically." Also, while the legitimacy was welcomed, it did come at the cost of setting a precedence of adhering to federal regulators.

The CFTC's seemingly favorable view of virtual currencies and the underlying blockchain technology was exhibited earlier in the year during a speech at the New York FinTech Innovation Lab. Here, the CFTC's chair (J Christopher Giancarlo) stated the agency "might collaborate with other authorities on leading development of best practices to support the development of "regulator nodes" on distributed ledgers, or experiment with collecting or distributing existing CFTC reports through blockchain technology." This again legitimized the adoption of the technology.

Anti-Money Laundering (AML) / Know Your Customer (KYC) and Office of Foreign Assets Control (OFAC) Concerns

Without getting too bogged down into the operation of the various underlying regulations, Anti-Money Laundering (AML), Know Your Customer (KYC) and the Office of Foreign Assets Control (OFAC) all require banks and other financial services industry participants to have policies, procedures and controls in place to identify the source of funds (AML), have a reasonable understanding of who your customer is (KYC) and checks in place to identify individuals and companies owned or controlled by certain countries that the U.S. government has blocked from utilizing the U.S. banking system and for individuals, groups and entities, such as terrorists and narcotics traffickers designated under various programs that are not country-specific.

These regulations are at odds with one of the fundamental ideologies of cryptocurrency and blockchain technology. When blockchain was developed to create BitCoin, the developers were looking to create a secure way to store and move value while also protecting the owner's privacy from everyone, including any government. This creates problems for anyone subject to AML, KYC and OFAC regulations. As mentioned earlier, when an entity is deemed a MSB, it must have robust programs covering these regulations. Also, depositories may want to maintain a correspondent relationship with a virtual currency exchange. The challenge then arises as to how to develop programs to implement these requirements.

Currently, there are no bright-line tests or rules put forth by any of the financial services regulators when creating AML/KYC and OFAC procedures and controls to govern a product or process using blockchain technology. Nor are there any safe harbors for those who want to pioneer the applications. At the same time, most of the regulators have identified AML/KYC concerns as an area of focus for 2017 and 2018. This all adds to the regulatory uncertainty and apprehension within the industry while the severity of AML fines leaves no room for noncompliance. Finally, the fact that a majority of the teams of legal and compliance professionals who support the financial services industry do not understand the technology or the possible remedies to achieve compliance while implementing the technology add to the headwinds and the uncertainty.

On the flip side to viewing the use of blockchain as a roadblock for those working in KYC compliance, there are entities that are exploring how the Ethereum blockchain technology can ease the burden of KYC compliance through the use of a smart contract. This can be accomplished because the technology can operate as "self-proving" through verification of its own chain/dataset. This provides an opportunity to build customer identification into the technology itself where it can be set as a condition precedent prior to contract execution. If successful, this would drastically lower the cost of each institution's having to investigate and identify each customer as the chain would have the ability to authenticate said customer.

State Regulation

The regulatory burden is again amplified when you start to consider the pace at which states are introducing and adopting legislation that governs the use of blockchain. For example, in June 2017, Arizona signed House Bill 2417 into law that acknowledges the legitimate use of blockchain technology to secure an electronic signature and that states that "smart contracts" (which utilize blockchain) cannot be denied effect. In 2016, North Carolina signed House Bill 289 into law which updated North Carolina's Money Transmitter Act to include the transmission of virtual currency. In Connecticut, the governor just signed House Bill 07141 in June 2017. If and when this regulation is adopted, it will establish capital requirements for money transmitters dealing in virtual currency. Texas, Nevada, Delaware, Florida, New Hampshire and others have all recently adopted legislation that addresses blockchain technology in certain aspects. The speed at which states are adopting legislation around virtual currency and blockchain makes the need for a current 50-state survey of applicable state law a necessity to minimize your regulatory risk in the space.

Unsurprisingly, New York perhaps has the most robust regulations codified at 23 CRR-NY 200 entitled "Virtual Currencies." New York requires any person engaged in any "virtual currency business" activity to obtain a license. The regulation defines "virtual currency business" as activity involving any one of the following types of conduct that takes place in New York or involves a New York Resident:

(1) Receiving virtual currency for transmission or transmitting virtual currency, except where the transaction is undertaken for non-financial purposes and does not involve the transfer of more than a nominal amount of virtual currency;
(2) Storing, holding, or maintaining custody or control of virtual currency on behalf of others;
(3) Buying and selling virtual currency as a customer business;
(4) Performing exchange services as a customer business; or
(5) Controlling, administering, or issuing a virtual currency.

The regulation goes on to require that each licensee maintain and enforce written compliance policies, including policies with respect to anti-fraud, AML, cybersecurity, privacy and information security and a customer identification program. The AML and customer identification requirements are further discussed in a separate section (23 CRR-NY 200.15). For example, a complaint customer identification program under the regulation will require at a minimum: 1) verification of the customer's identity, to the extent reasonable and practicable; 2) maintenance of records of the information used to verify such identity, including name, physical address, and other identifying information; and 3) a check of customers against the Specially Designated Nationals (SDNs) list maintained by OFAC. The regulation also goes on to state that enhanced due diligence may be required based on additional factors, such as for high-risk

customers, high-volume accounts or accounts on which a suspicious activity report has been filed.

While the regulation is very dense, the fact that it covers activity involving any New York resident is almost a relief, given the fact that it insures that if you want New Yorkers as customers, you will now have a clear set of guidelines for best practices in multiple areas.

Although the regulation of blockchain technology and virtual currencies within the financial services industry presents certain challenges, and is evolving month to month, the explosion in the use of the technology is not slowing down. As of October 2017, there were slightly less than 1,200 different virtual currencies in circulation that can trade on a little more than 6,000 different exchanges. All while depositories, lenders, FinTech vendors and other players all continue to innovative by creating new ways to deploy blockchain technology every day. The speed of the development of the technology, as well as the regulation, demands that you consult an attorney well versed in both financial regulation and the underlying technology as a means to best limit your regulatory exposure.

*****

Craig Nazzaro is Of Counsel in the Atlanta office of Nelson Mullins Riley & Scarborough LLP. His practice areas include Alternative Lending & Other Non-Bank Financial Services, FinTech, and Payments & Digital Commerce. **Dowse Bradwell "Brad" Rustin, IV**, is a partner in the firm's Greenville, SC, office whose practice areas include Banking & Financial Services, FinTech and Payments & Digital Commerce. **John M. Jennings** is a partner in the firm's Greenville office whose practice areas include Banking & Financial Services, Blockchain & Digital Currency, Private Equity and Securities Offerings.

—❖—

Top Cybersecurity Takeaways from Relativity Fest 2017

By April Runft

Cybersecurity is a hydra of complexity. Keeping a grasp on it requires constant re-education. What no one tells you: managing your company's cyber vulnerability demands a willingness for *personal* vulnerability. Being honest about our cyber risks is painful. And scary.

"There is real fear there — and there *should* be fear," said John deCraen, director of global cyber risk services at Alvarez & Marsal. "Fear is healthy. We should learn to understand what we're facing and be honest with ourselves on how we're doing with those risks."

No surprise here: cybersecurity was a prominent topic at the 2017 Relativity Fest, where 2,000 legal professionals met in Chicago to swap ideas about the legal tech industry.

Managing e-Discovery's Inherent Risks

There's no getting around it: e-discovery can be risky for law firms and providers, as well as for the clients whose data gets ingested.

In his conference session, deCraen gave attendees a guided tour of provider vulnerabilities along each stage of the EDRM (e-Discovery Reference Model) and how to address them. For starters, when providers import clients' data, there's a chance that the data is infected and can poison the provider's own systems.

Smart organizations assume they're importing "dirty data" and plan accordingly.

"If you're already spending the energy using something like a FIPS (Federal Information Processing Standard)-compliant FTP, then you're way ahead of the competition," deCraen said.
And from client's perspective, entrusting your company's data to an outside custodian is risky in another way: sometimes the story begins with a big *oops*.
"A company came to us for help when a high-level financial manager lost an unencrypted laptop," said Brian Blush, a director in KPMG's forensic technology practice. "They were worried about what kind of data and personally identifiable information had possibly gotten out into the world."
We're human. *Oops* situations happen — so in addition to planning for bad actors, let's also build in strategies for handling them.

More Top Takeaways from Relativity Fest 2017

Ineffective Leadership

One of the biggest cybersecurity hurdles isn't technical — it's human.
"The number one driver in most cybersecurity breaches is ineffective leadership and board culture," deCraen said. "I find this in every organization I assess, without fail. They don't have the budget they need; they're woefully understaffed; they don't have the tools or activities in place they should have."
Even if you've named a diligent chief information security officer who's on top of what your company needs, she can't be effective without the appropriate budget, staff, and executive sponsorship when business verticals push back on cyber requirements.
The result is bare minimum compliance.
Another danger? Thinking you're immune to a breach because of your company's location, industry, or revenue level (or any other factor).
"Hubris is a killer," deCraen said. "It will absolutely lead to a breach, one way or another."

Reset Your Impression of Today's Hacker

No longer fear the lone actor in his mom's basement, hacking just to see how far he can get. Today it's a whole new game. There are real organizations offering real rewards for cyber attacks.
"Keep asking, 'what am I not aware of that I could or should be? Why am I not aware of it?'" said deCraen. "Think progressively. Your enemies are."
A healthy cyber program should pull in a diversity of expert perspectives and includes nearly 100 different activities, according to deCraen. To name a few:

- **Asset management and classification:** Catalogue your hardware, software, and data.
- **Data encryption:** Encode data at rest and in transit.
- **Data loss protection:** Prevent end users from sending sensitive information outside your network.
- **Indicator of compromise (IOC) hunting:** Patrol your network and operating systems for signs of an intruder.
- **Identity access management:** Perform regular entitlement reviews to ensure only the necessary people can access data; require two-factor authentication for all resource access (*more on this later*).

Compliance Is Not Security

"In every single incident I've responded to, the companies have been compliant with regulatory frameworks," deCraen said. "If you line up these frameworks left to right, you'd be surprised at the huge gaps in required activities. That's because when the regulations are written, they're aiming to deal with a single problem at a time."

Plus, in e-discovery, there aren't specific regulations for companies that handle third-party data. Without that guidance, it's up to you to decide you're going to create a program to protect your clients. Think security first and compliance will follow.

Two-Factor Authentication Is Non-Negotiable

With the intent, any hacker worth his salt can have your password in three seconds. A strong password is no longer enough. Whether we're talking on-premises or in the cloud, two-factor authentication is a must.

"Two-factor authentication requires something you *know* — like a username and password — paired with something you *have* — like a token sent via email," said Amanda MacAllister, infrastructure engineer at Relativity. "This is a great example of 'defense in depth,' the new industry standard for security. By implementing two layers of defense instead of one, an attacker must compromise both your credentials and your emails to access the system."

Double Down on Securing Systems That Touch the Internet — Yours and Others'

The connectivity the Internet offers can be a blessing and curse. Do real due diligence before you engage with third-party cloud vendors to dig into how they plan to safeguard your data.

"There are several key things you'll want to ask about," said Andrew Watts, vice president of information technology at Relativity. "Are they following NIST standards? Do they require background checks and security training for all employees? What measures are they taking to create a physically secure environment? Are they using multifactor authentication and rotating certificates, keys, and passwords? Do they staff a round-the-clock security team, perform regular penetration tests? Can they discuss their business continuity and disaster recovery plans?"

Another tip for your own systems:

"Create a demilitarized zone between the Internet and your internal environment," said Matt Spurr, senior lead security engineer at Relativity. "By having your external Web server separated from your internal environment, an attacker would have to breach two devices to enter your network instead of one."

In the event of a breach, leverage your existing e-discovery tools to assess damage and respond quickly.

Back to the earlier *oops* case study: KPMG's client needed help to figure out whose sensitive data they may have lost and notify them within days or risk massive fines. KPMG put a global e-discovery team on it and used their in-house e-discovery tools to move swiftly. "Once we pulled down a backup copy of the laptop's data from the cloud, we used a combination of Regular Expressions and keyword search to seek out potentially sensitive data in the set and prioritize it for review," said KPMG's Daniel Smith.

That alone was a lifesaver. KPMG took it a few steps further.

"We used a Q&A log to capture any questions reviewers had along the way, so we could relay them to the client," Smith said. "We also built an overlaid application we called a 'biography tracker'. It allowed reviewers to log information they found by individual to give a personalized view of the depth of what was compromised."

Conclusion

The reality is this: there have been more than nine billion data records lost or stolen since 2013.

"Modern enterprises are coming to accept that 100% cybersecurity is an impossibility," said Judy Selby, an insurance and strategic cyber risk consultant. "Rather, it's about understanding and managing your cyber risks."

While you're not personally expected to be a cybersecurity expert, you *are* obligated to find the resources and expertise you need to secure your own and your clients' data.

Shortchanging cybersecurity in your organization is like splurging on a meal at a high-end restaurant but not reserving enough budget to tip your waiter. If you can't set allocate the resources to do it right, do you have any business being there in the first place?

*****

April Runft is a writer and webinar producer for software firm Relativity. She leads Relativity's monthly webinar series on e-discovery, cybersecurity, and information governance topics and writes regularly for The Relativity Blog.

—❖—

The Impact of the Surge of Biometric Data Privacy Lawsuits Against Employers

By Hanley Chew and Eric Ball

Since July 2017, there have been a surge of lawsuits brought against employers under the Illinois Biometric Information Privacy Act (BIPA) in Illinois courts. More than 30 class action lawsuits have been brought against employers of such companies as United Airlines Inc., Intercontinental Hotels Group, Hyatt Corp., Bob Evans Restaurants, Speedway LLC, and others for their use of biometric data in the workplace.

Although the details of each individual case may vary, the plaintiffs often allege that the employer failed to comply with the requirements of BIPA when they used fingerprint-operated machines to record employees' work hours. The growing acceptance of biometric data as a form of identification for employees means that many employers will likely have to face either these or similar issues in the immediate future.

The Illinois Biometric Information Privacy Act (BIPA)

In 2008, Illinois passed the BIPA, which provided rules for the collection and use of biometric data. Organizations must provide written notice to their employees prior to the collection of any biometric identifier. The notice must include the purpose of the collection and the duration that the organization will use or retain the data. Only after obtaining written consent can organizations begin their collection activities. Once they have collected biometric data, the BIPA requires organizations to protect that data in the same manner it would protect other sensitive and confidential information using the reasonable standard of care in its industry. And, the BIPA requires organizations to have a publicly available, written policy stating how long the organization will retain the data and rules governing the destruction of that data.

The BIPA prohibits organizations from selling or profiting from the biometric data they collect. It also prohibits organizations from disclosing biometric data unless: 1) they obtain consent; 2) the disclosure completes a financial transaction requested by the individual; 3) the disclosure is required by federal, state or municipal law; or 4) the disclosure is required by a valid warrant or subpoena.

The BIPA provides a private right of action for violations of the statute and entitles a prevailing party to statutory damages for each violation equal to the greater of $1,000 or actual damages for negligent violations and the greater of $5,000 or actual damages for intentional or reckless violations.

The plaintiffs in the BIPA employer lawsuits allege that the employers violated the BIPA by failing to provide notice to their employees concerning the companies' use, retention and destruction of fingerprint data and/or obtain consent from their employees before collecting and

using the fingerprint data. In at least one case, the plaintiff alleged that the employer violated the BIPA by improperly disclosing and sharing the information with a third party.

The BIPA employer lawsuits may have a significant impact on future biometric data privacy statutes. Currently, the landscape for statutes governing biometric data is fairly sparse. There is no federal statute that regulates the collection, use, retention and destruction of biometric data, and only two states (other than Illinois) have enacted biometric data statutes.

Biometric Data Privacy Laws for Texas and Washington

Texas enacted a biometric data privacy law, similar to the BIPA, shortly after the passage of the BIPA. The Texas law required informed consent by individuals before organizations could begin collecting biometric identifiers. However, the consent did not need to be written. The Texas biometric data privacy law also imposed limitations on the sale of biometric information and included security and retention requirements. Unlike the BIPA, only the Texas Attorney General can enforce the Texas biometric data privacy law as the law does not provide a private right of action.

This year, Washington State enacted its own biometric data privacy statute. The Washington statute defines "biometric identifiers" as "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual." Perhaps in response to the BIPA lawsuits based on the collection and use of facial scans, Washington's definition of "biometric identifiers" expressly excludes "physical or digital photograph, video or audio recording or data generated therefrom."

Washington's biometric data privacy law applies only to biometric identifiers that are "enrolled" in a commercial database, which is defined as "captur[ing] a biometric identifier of an individual, convert[ing] it into a reference template that cannot be reconstructed into the original output image and stor[ing] it in a database that matches the biometric identifier to a specific individual." Organizations may not enroll a biometric identifier unless they provide notice and obtain consent.

Like the Texas biometric data privacy law, the Washington statute imposes limitations on the sale, leasing and disclosure of biometric data to third party and establishes security and retention requirements. The Washington statute also does not provide a private right of action. Only the Washington Attorney General can bring an action enforce to enforce the statute under the Washington Consumer Protection Law.

The Shape of Future Biometric Data Privacy Laws

Given the growing prevalence and importance of biometric data, several state legislatures are considering legislation that would regulate its collection, use and retention. The Alaska (HB 96), Connecticut (HB 5522), Montana (HB 518) and New Hampshire (HB 523) legislatures all have pending bills governing biometric data. The bills in Alaska, Montana and New Hampshire require that notice be given and consent obtained before biometric data is collected, used or retained. These three bills also have requirements for the retention, disposal and/or security of this data. The Connecticut bill simply prohibits the use of facial recognition for marketing purposes. The Alaska and New Hampshire bills provide for a private right of action; while, the Connecticut and Montana bills do not.

The BIPA employer litigation may give states that are considering or in the process of drafting their own biometric data privacy laws some pause. In light of the multitude of class action lawsuits that have been filed, states may either reconsider the scope of their proposed biometric data privacy laws or the wisdom of even enacting such laws. States wishing to attract businesses

might be concerned that the potential liability from biometric data privacy laws may act as a deterrent. States may also be concerned that potential liability may discourage businesses currently residing in their states from adopting cutting edge technology that employs biometric information.

If states do decide to adopt biometric data privacy laws, the scope of those laws may not be as broad as the BIPA. Like the Texas and Washington laws, future biometric data privacy laws may not provide for a private right of action. Only the State Attorney General Office or the Office/Bureau of Consumer Protection in a state may be able to bring an action to enforce the law.

Even if states do provide a private right of action, they may include exemptions or exceptions in the law that narrow it. For example, just as the Washington statute expressly excluded physical or digital photographs and video or audio recordings from its purview, future biometric data privacy laws enacted by states could exclude biometric data collected for noncommercial, administrative purposes from their reach.

Tips for Employers Responding to Biometric Data Privacy Laws

Even as other states grapple with the question of whether to adopt biometric data privacy laws, employers with operations in Illinois, Texas or Washington should consider taking the following steps where appropriate to protect against potential lawsuits.

First, employers should consider providing written notice to their employees and obtaining the written consent of their employees before they collect, use or store the biometric data of those employees. Such a notice should describe the type of biometric data that is being collected, the specific purpose of the collection, and the time period during which the biometric data will be collected, used and stored.

Second, employers should also think about developing and implementing a policy about the retention and disposal of biometric data.

Third, employers should contemplate protecting the biometric data that they collect in at least the same manner as other sensitive and confidential information. This includes using reasonable safeguards, such as encryption, in the storage or transmittal of this information.

Fourth, employers who use third parties in the collection or storage of biometric data should weigh conducting appropriate diligence on these third parties as necessary to ensure that they adhere to the same standards of security. Employers should also consider including these third parties in the notice and consent provided to employees.

Fifth, employers should look at adopting safeguards to prevent the sale, lease or sharing of the biometric data that they collect from their employees where required. Adopting a compliant policy can go a long way in avoiding or, at least, mitigating potential liability. However, it should also be noted that courts have rejected BIPA claims which were based on procedural violations of the statute and which failed to allege any actual injury.

*****

Hanley Chew is Of Counsel in the Litigation Group with Fenwick & West. He focuses his practice on privacy and data security litigation, counseling and investigations, as well as intellectual property and commercial disputes affecting high technology and data driven companies. **Eric Ball** is a partner in the Litigation Group with Fenwick & West. He focuses his practice on complex commercial litigation and trademark disputes for technology and gaming companies. This article also appeared in *Legaltech News*, an ALM sibling of *Cybersecurity Law & Strategy*.

—❖—

Legal Tech

Looking Ahead: 2018 Legal Technology Predictions

By Jeff Ton

At law firms and legal departments, preparing for the new year should mean looking back at the last year and prioritizing revenue-driving activities, identifying strategies to grow your firm or company while mitigating risk and budgeting for new projects to meet client demands.

While end-of-year planning is a typical tradition for any company, it's important to understand that 2018 will be anything but the status quo for daily law practice. In November, Bluelock released a whopping 50-page eBook of predictions for the legal industry in 2018, compiled with thoughts from 15 individuals at law firms and organizations that service the legal industry. To give you a taste of what to expect in the new year, I have detailed a few predictions below.

Ransomware Will Become a Bigger Deal

Ransomware attacks made headline news in 2017, entering the general public's knowledge. We're seeing new variants coming from the hands of more cybercriminals than ever before. The black market has made it for possible for anyone to execute an attack with the rise of Ransomware-as-a-Service. This is horrible news for the legal industry in 2018, since the cyber-criminal community views law firms as willing to pay, given the mass quantities of sensitive data lawyers are using for case proceedings every day.

We'll also see more ransomware attacks with the intent to disrupt rather than turn a quick profit, such as the one we saw happen to DLA Piper in 2017, where the firm was caught up in the unfortunate crosshairs of cybercriminals trying to upset an entire country's economy.

How does a law firm prepare and protect their information? The answer is multi-faceted, but I'll try to break it down in simple terms. You need a two-pronged approach: a balance of preventative and restorative measures, with detection solutions as a bridge between the two to identify when a breach has occurred. We'll be seeing more ransomware attacks that lay dormant before launching in 2018, so restorative and detection methods are especially key. One way firms will begin to strengthen their IT stance is with Disaster Recovery-as-a-Service (DRaaS), which can be used as a mitigation tool in the event of an attack to quickly retrieve clean datasets from prior to the encryption, enabling fast recovery without paying a ransom.

Law Firms Serving International Clients Will Need to Meet International Standards

As global demands increase and law firms take on more clients with international ties or dealings, the pressure to meet certain postures of data protection will also become more intense. This means that the upcoming enforcement of the EU General Data Protection Regulation (GDPR) in May 2018 will have a rippling impact on the legal industry, at home and abroad.

To retain counsel among international clients, law firms will be rushing to meet new standards of data privacy and management — so it's best to start looking into these changes now rather than face surprises in spring. This scramble for regulatory compliance won't stop with GDPR: rulings like this one are on the rise and won't be going away. Given the dependence modern business now has on technology and the sensitivity of sharing information via electronic means, it's only natural that there should be precautions in place. The business community has been slow to adopt necessary changes to account for privacy and data management needs, so it's no surprise government entities have had to step in. For law firms with IT budgets that haven't seen a bump in years, this will come as a particularly painful reality, since meeting GDPR and other regulatory demands is near impossible with outdated solutions.

Artificial Intelligence and Machine Learning Will Make Waves Across the Entire Legal Industry

We've heard a lot about Artificial Intelligence (AI) for a while now. But in 2018, it is finally traveling from the pages of sci-fi novels to become a reality in people's lives (take the increased attention on driverless cars, for example). For the legal industry, AI represents an opportunity to streamline firm practices and operations (such as in e-discovery), but also some areas of concern.

AI and machine learning could begin to take on more and more of the attorney's workload from researching case law to even writing some briefs. Taken to the extreme it could replace paralegals and even attorneys themselves someday. But, let's not get ahead of ourselves.

We have already seen some real-life examples of AI, machine learning and big data impacting the practice of law. What if you had a tool that could study hundreds and thousands of cases and give you a prediction of your likelihood of winning a case and which one you should settle? This innovation could enable you to spend your time on the cases that are most impactful for you and your clients.

The ability for a firm to ensure continuous operations will become as integral to a firm's livelihood as profitability, since it will become even more so linked to reputation in the marketplace. In 2018, we will see firms embrace machine learning to ensure continuous service to clients.

Blockchain Will Become a Force for the Legal Industry's Future

Blockchain will become more of a force for change within the industry in 2018. Dan Tapscott, author of the *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business and the World*, defines blockchain as "a vast, global distributed ledger or database running on millions of devices and open to anyone, where not just information but anything of value money, but also titles, deeds, identities, even votes can be moved, stored and managed securely and privately. Trust is established through mass collaboration and clever code rather than by powerful intermediaries like governments and banks."

Clients will start using this technology to create "smart contracts," which leverage the ability to share secure information between parties economically and with convenience. This will create a bridge between the lawyer, software designers and software developers. Imagine legal and IT working together to create contracts that automatically execute the terms of the agreement based on external events. Sound like science fiction? Many industries are beginning to see significant disruptions from blockchain technology and smart contracts.

While you may not see this phenomenon inside your practice next year, your clients in the financial services, insurance, music and real estate industries will. They will be coming to you to seek your counsel on how best to implement these technologies within their companies. You will need to be prepared and educated in the nuances to stay relevant.

Cultural Changes Are on the Horizon

Looking into the future, above all else, requires flexibility to change. That's why 2018 will be the year of a cultural shift within law firms. With more millennials entering the workforce, this doesn't just change the make-up of law firms, but a firm's client base as well. Generation X and millennial groups, for example, have different values, expectations, etc. — and these differences will be a lynchpin for upsetting the status quo.

The demand to protect sensitive information for clients and ongoing cases is already forcing the adoption of new approaches to data protection and risk mitigation — but is the legal industry ready? Here, multi-generational gaps could also mean exploitable gaps for the cybercriminal

community. The older generation may be comfortable in their traditional way of doing things, unwilling to adopt more efficient ways of practice having learned from mistakes in the past. On the other hand, the younger generation may recognize the efficiencies of new technologies but may never have been burned by technology before so don't recognize the risks. The two groups are blinded by their own biases.

Multi-generational lawyers and firm IT personnel must learn to come together to solve for problems the industry faces with new innovations and expectations. More importantly, these lawyers and technologists will learn from their mistakes and their counterpart generations to become a more cohesive unit.

*****

Jeff Ton is executive vice president of product and service development for Bluelock where he is responsible for driving the company's product strategy and service vision and strategy. Ton has over 30 years of experience in business and information technology and previously served as CIO for Goodwill Industries of Central Indiana and Lauth Property Group.

—❖—

Legal Tech

What an Attorney Can Learn from Legal Tech Marketing Professionals

By Jonathan Friedland

I didn't know what to expect when I decided to attend the Legal Marketing Association's Legal Marketing Technology Conference in Chicago. The LMA, I had assumed, is an organization by, of, and for people who work in a marketing capacity at law firms and, you see, I am a practicing attorney.

If one were to judge by the attendee mix alone, one might think I was correct. But within an hour of walking in the door, I realized that I would walk away learning a lot of useful information, beyond simple marketing advice and products. The following are some key takeaways and hot topics that should be on the radar of lawyers:

- There are a host of contact and customer relationship management solutions in the market place vying for market share. I've tried several services but none of them have fully met my needs, and I am now aware in talking with other attendees and vendors that my own difficulty in selecting the appropriate product is widespread. Some products are basic, offering little more functionality than Outlook programs. Others are more robust, capable of syncing with various billing, docketing, and document management programs. The options appear to be almost limitless and vary drastically in terms of cost and sophistication. Attorneys who want to add this type of product to their practice would likely be well-served to try out a few options first to find the one that feels the most comfortable in terms of usage, and which can integrate well into the existing systems.
- The struggle to "mine" the relationships of each lawyer in a firm appears to be a universal one, again making me feel better about our own trials and tribulations in this regard. LMA member Cindy Thurston Bare shared Orrick's experience in implementing a firm-wide process for developing and maintaining its experience database. This type of data accumulation and presentation, one might think, would be a relatively easy undertaking.

But there a lot of moving pieces involved. At the same time, the benefits of such an institutional depository of expertise are obvious both for current attorneys, and also to greatly streamline the onboarding process when bringing new lateral hires up to speed on their new colleagues' experience.

- More and more vendors are offering firms a way to monitor news stories about their clients and their prospective clients, at a cost. While these services are interesting, and may be of value for large firms employing thousands of attorneys and countless practice areas, I am not yet persuaded that any are significantly better than simply using Google Alerts, which is a free service. Attorneys should nonetheless keep an eye on these services to determine when the cost/benefit analysis mat start to swing in their favor for even small and mid-sized firms.
- The average attorney (certainly those who seek to demonstrate thought leadership) could stand to learn a little about search engine optimization (SEO). SEO is a marketing discipline focused on growing visibility in organic (non-paid) search engine results. SEO encompasses both the technical and creative elements required to improve rankings, drive traffic, and increase awareness in search engines. "Serving Up SEO Success: The Perfect Recipe for Data and Content Collaboration," presented by the engaging duo of Allison Spence and Stephanie Richter, both of Thompson Coburn, was chock full of good information.
- The topic of how artificial intelligence will impact the practice and business of law is on a lot of peoples' minds, and it is probably time for more of us to start paying some attention to the topic. Attorneys who are regularly involved in e-discovery have been on the forefront of the intersection of law and AI through increasingly common use of assisted-review technology. But AI is likely to a far-reaching impact on the practice and business of law, well outside of streamlining massive document productions. Think for example of a large company or governmental organization with thousands of employees, and all the electronic information that they create and maintain. What if a particular risk existed, but the data that would reveal the risk was vast and unstructured? AI could help in a preventative sense, in that the C-Suite could have routine audits for issues to be uncovered before they explode.
- On a personal level, I discovered that imperfect relationship I have had with some marketing folks at prior firms is not unusual. Having the opportunity at the LMA Conference to interface with marketing professionals and hearing the tensions that commonly exist between lawyers and marketing professionals, gave me a much better understanding of the challenges they face and how we attorneys can work a lot more productively with them.

This brings me back to a point I started with: I believe, based on what I experienced at the conference, that some lawyers (at least those involved in firm management or meaningful business development) would benefit greatly from attending some LMA events. And, likewise, I think LMA events would benefit from the perspective we can add.

The conference, all in all, was excellent and its co-chairs, Rich Marsolais, Jennifer Klyse and Maureen Farr deserve kudos. I look forward to attending again next year.

*****

Jonathan Friedland is a partner with the Chicago/NY law firm, Sugar Felsenthal Grais &

Hammer. He is also the founder of Financial Poise, a thought leadership platform for attorneys and other trusted advisors.

—❖—

Legal Tech

SEC's New Cyber Unit Moves to Tackle 'Scam' Coin Offering

In the First Enforcement Action Initiated By Its New "Cyber Unit," the SEC Announced It Has Secured a Court Order to Freeze the Assets of Individuals Behind a "Scam" Initial Coin Offering

By Ben Hancock

In the first enforcement action initiated by its new "Cyber Unit," the Securities and Exchange Commission (SEC) recently announced it has secured a court order to freeze the assets of individuals behind a "scam" initial coin offering, or ICO.

The case, filed in federal court in Brooklyn, NY, targets an allegedly repeat securities fraudster in Canada who promised purchasers of a digital token called "PlexCoin" quick returns on their money — potentially exceeding 1,000%.

The court issued an emergency order allowing the SEC to freeze the assets of defendants Dominic Lacroix and Sabrina Paradis-Royer, according a press release from the commission.

Lacroix has been the target of previous legal enforcement action over PlexCoin by financial authorities in Quebec, the SEC's complaint says.

"This first Cyber Unit case hits all of the characteristics of a full-fledged cyber scam and is exactly the kind of misconduct the unit will be pursuing," Robert Cohen, the chief of the new unit, said in the release. "We acted quickly to protect retail investors from this initial coin offering's false promises."

Former SEC lawyers said that the enforcement action was not surprising, given the commission's messaging in recent months, and that it is unlikely to shed more light on how the SEC determines whether an ICO is a security. Although the complaint alleges that the PlexCoin ICO was an unregistered security offering, it does not give a detailed analysis to back up that argument.

"It's clear out-and-out fraud that has the ICO component, so it fits in with what the SEC has been talking about in different speeches," says Michael Dicke of Fenwick & West, who was previously an associate regional director for enforcement in the SEC's San Francisco office.

"The question is what [will the SEC do] if there's not fraud, but there's a registration violation," Dicke adds. "That's unanswered."

Nicolas Morgan, a partner at Paul Hastings and former senior trial counsel in the SEC's enforcement division in Los Angeles, also says he expects the commission to pursue more cases involving serious fraud claims in the future — rather than expending its limited resources on cases that touch on more nuanced elements of securities law.

At the same time, Morgan says he anticipates the SEC is looking closely at unregistered services that allow secondary trading of digital tokens like PlexCoin. Its complaint notes that PlexCoin "currently trades under the symbol PXN," although doesn't name any digital token exchange in particular. "I think the next shoe to drop will be what does the SEC do when it comes to exchanges," Morgan says.

The Cyber Unit was set up by the commission last September, with a heavy focus on blockchain distributed ledger technology and ICOs, the spread of false information online, hacking and

threats to trading platforms. The unit is headed by Cohen and Valerie Szczepanik, who leads the SEC's roughly 75-member distributed ledger working group.

The complaint by the SEC alleges that the tokens the Lacroix offered investors were, in fact, unregistered securities and that numerous claims about their potential value were based on false statements. It says that he and Paradis-Royer have obtained some $15 million from thousands of investors since launching the ICO in August.

The coin offering claimed to offer investors "tokenized currency" that would appreciate in value, with early investors reaping "outlandish rewards of 1,354% in 29 days or less," the complaint says. The SEC also alleges that Lacroix sought to hide his involvement in the project because he was "a known securities law violator in Canada."

The case is the latest example of the SEC making clear that blockchain-enabled token offerings are not outside the scope of its regulatory power. Last July, it issued a report following an investigation of an organization called The DAO concluding some digital token offerings are securities under applicable law. It also issued an "Investor Alert" in August warning retail investors about ICOs, stressing that fraudsters "often try to use the lure of new and emerging technologies to convince potential victims to invest their money in scams."

*****

Ben Hancock is a reporter for *The Recorder*, the San Francisco-based ALM affiliate publication of *Cybersecurity Law & Strategy*. He can be reached at bhancock@alm.com. On Twitter @benghancock.

To order this newsletter, call:
800-756-8993

On the Web at:
http://www.lawjournalnewsletters.com/cybersecurity-law-and-strategy

Editorial email: ssalkin@alm.com
Circulation email: mailto:customer care@alm.com
Reprints: www.almreprints.com

Published Monthly By:
Law Journal Newsletters
1617 JFK Blvd, Suite 1750, Philadelphia, PA 19103