MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

TechConnect

Your Law Firm Link to Industry News

SEPTEMBER 2016

Letter from the Editors

Dear Readers,

The world of raising capital for emerging companies has experienced a revolution. Prior to the enactment of the JOBS Act in 2012, raising capital for private companies was limited to offline communications and was dominated by professional venture capitalists; now the capital raising process has been democratized. Capital can be raised online directly by companies or through intermediaries. It can be accomplished by crowd sourcing to “accredited investors” or, in limited amounts, by crowdfunding to everyone. Additionally, companies can raise capital in an “IPO lite” manner by using the new Reg A+.

With all of these changes, we thought it would be useful to create a chart outlining the different ways to raise capital and the applicable regulations so entrepreneurs can make more informed decisions about the capital raising process. Our chart below can be opened in pdf format and printed out for easy offline use.

We would also like to remind our readers that you can always ask us anything at http://mintzedge.com/ask-anything/. We built the MintzEdge website as a resource for entrepreneurs and investors, and hope that all of you take advantage of the site and see how it can help you.

Happy Reading!

Dan + Sam

CONTENTS

EDITORS

- Daniel I. DeWolf
- Samuel Asher Effron

RELATED PRACTICES

- Corporate & Securities
- Intellectual Property
- Privacy & Security
- Private Equity
- Real Estate
- Securities & Capital Markets
- Sports Law
- Technology Transfer
- Venture Capital

RELATED INDUSTRIES

- Arts & Entertainment
- Energy & Clean Technology
- Financial Services
- Life Sciences
- Technology

RELATED WEBSITES

- MintzEdge

Changing World of Raising Capital

BY DANIEL DEWOLF, MEGAN GATES, AND KAORU SUZUKI

The world of raising capital changed over the last several years. Offerings of securities generally used to fall into two main buckets: (i) private placements under the old Rule 506, or (ii) a public offering. With the implementation of various provisions of the JOBS Act now mostly complete, the array of choices has increased exponentially and include crowd funding, crowd sourcing by general solicitation for accredited investors, IPO light under the new Reg A+ rules, and confidentially submitted initial public offerings. No one size fits all and issuers, bankers, and legal counsel should look carefully as to the context of the situation to determine which format makes the most sense for a particular offering. We thought it might be helpful to provide a chart of the various alternatives for offerings now available.

PDF AVAILIABLE AT www.mintz.com/pdf/ComparisonChartVSO.pdf

Comparison Chart of Various Securities Offerings
** This chart is a high-level summary only; one should consult the relevant statutes, regulations, and SEC guidance when engaging in any of the following transactions.*

	Exempt Transactions / Private Offerings					Registered Public Offerings	
	'33 Act, Section 4(a)(2)		'33 Act, Section 4(a)(6)	'33 Act, Section 3(b)(2)			
	Regulation D Rule 506(b)	Regulation D Rule 506(c)	Regulation Crowdfunding	Regulation A+ Tier 1	Regulation A+ Tier 2	Confidentially Submitted Initial Public Offering (Emerging Growth Companies)	Initial Public Offering
Eligible Issuers	Any company, including publicly traded and private issuers.	Any company, including publicly traded and private issuers.	(1) Must be US issuer (2) Must not be a reporting company; an investment company; a shell company; or an issuer that has failed to make any required Form C filing.	(1) Must be US or Canadian issuer (2) Must not be a public company, an investment company, a "blank check" company, a delinquent filer under Reg. A+, a company with a revoked Exchange Act registration, or a "bad actor" (see below).	(1) Must be US or Canadian issuer (2) Must not be a public company, an investment company, a "blank check" company, a delinquent filer under Reg. A+, a company with a revoked Exchange Act registration, or a "bad actor" (see below).	Must qualify as an Emerging Growth Company (EGC). Generally, issuers that have not completed a US IPO before December 8, 2011 and have less than $1 billion in annual gross revenue can qualify as EGCs.	Any company.
Issuer Size Thresholds	No limit.	No limit.	No limit.	No limit.	No limit.	Must qualify as EGC	No limit
Rule 506(d) ("Bad Actor") Disqualification	Yes	Yes	Yes	Yes	Yes	No (although as a practical matter could present challenges)	No (although as a practical matter could present challenges)
SEC Filing Requirement	Form D	Form D	Form C	Forms 1-A	Forms 1-A	S-1	S-1
Maximum Raise	Any amount	Any amount	$1M/12 Months	$20M/12 Months. Issuer raising less than $20M may choose between Tier 1 and Tier 2.	$50M/12 Months. Issuer raising less than $20M may choose between Tier 1 and Tier 2.	Any amount	Any amount
Testing the Waters	n/a	n/a	No	Not Recommended Due to Range of State Laws	Yes	Yes. Only to Qualified Institutional Buyers (QIBs)/Institutional Accredited Investors (IAIs) and only after the registration statement has been submitted confidentially.	Not unless issuer is an EGC
General Solicitation Permitted	No	Yes	Issuers may only issue "tombstone" ads with specific limited information. No limits on communications with potential investors through the intermediary's platform.	Yes. Issuers also permitted to engage in test-the-waters communications before and after the offering statement has been filed.	Yes. Issuers also permitted to engage in test-the-waters communications before and after the offering statement has been filed.	Yes, only after the registration statement has been filed publicly.	Yes, only after the registration statement has been filed publicly.
Investor Restrictions	Unlimited number of Accredited Investors and no more than 35 Non-Accredited Investors, if each such investor is sophisticated	Unlimited number of Accredited Investors.	Per-investor limits in any 12-month period: For investors with annual income or net worth below $100,000, the limit is the greater of (i) $2,000 and (ii) 5% of the lesser of annual income and net worth. For investors with annual income and net worth both above $100,000, the limit is 10% of the lesser of (i) annual income and (ii) net worth, in each case with a $100,000 cap on sales to any individual.	None.	Per-investor investment cap for non-accredited investors (unless the securities are listed on a national exchange). The cap is equal to 10% of the greater of: annual income or net worth (for natural persons), or annual revenue or net assets (for non-natural persons).	None.	None.
Obligation to verify investor status	Reasonable belief must be held that each purchaser is (1) an accredited investor or (2) a non-accredited investor that, alone or together with its purchaser representative, is sophisticated. Purchaser self-certifications are generally used.	"Reasonable steps" must be taken to verify that each purchaser is an accredited investor. May not rely on self-certification alone.	May rely in good faith on a determination by an intermediary that an investor has not exceeded the per-investor investment limit. Intermediaries may rely on an investor's representation that it has not exceeded limits.	None.	Must inform investors of the investment cap for nonaccredited investors, and may rely on an investor's representation that it is in compliance with cap.	None after the registration statement is filed publicly. Before the registration statement is filed publicly, TTW sessions must be held only with QIBs/IAIs.	None after the registration statement has been filed.
Limitation on Resales?	Yes, securities sold under Regulation D are restricted securities.	Yes, securities sold under Regulation D are restricted securities.	Resales prohibited for one year, with limited exceptions (including resales to accredited investors and family members).	None.	None.	None.	None.
Intermediary Requirement	None.	None.	Yes. Each offering must be conducted through a single intermediary that is a registered broker or a registered funding portal.	None.	None.	None.	None.
Disclosure Requirement to Investors?	Yes, but only if sales are made to any non-accredited investors. Disclosure requirements are similar to those for a Securities Act registration statement. In addition, a Form D must be filed with the SEC.	No, but subject to anti-fraud limitations.	Form C must be filed with SEC. Includes two years of financial statements (must be reviewed by an accountant for offerings raising over $100,000 (or first-time offerings over $500,000) and audited for non-first-time offerings over $500,000). Similar to disclosure in a Securities Act registration statement. Form C is not subject to SEC review.	Form 1-A must be filed with SEC, including an offering circular and two years of financial statements, which need not be audited. Similar to disclosure in a Securities Act registration statement. Form 1-A is subject to review and comment by the SEC and by state securities regulators. First-time issuers are eligible for non-public review by the SEC.	Form 1-A must be filed with the SEC, including an offering circular and two years of audited financial statements. Similar to disclosure in a Securities Act registration statement. Form 1-A is subject to review and comment by the SEC. First-time issuers are eligible for non-public review by the SEC.	Yes, all information required in the Form S-1 is required to be disclosed. Includes description of business, risk factors, audited financial statements, MD&A, description of offered securities, etc.	Yes, all information required in the Form S-1 is required to be disclosed. Includes description of business, risk factors, audited financial statements, MD&A, description of offered securities, etc.
Annual Reporting Requirements	None, unless/until the issuer exceeds the threshold for becoming a reporting company under Exchange Act rules.	None, unless/until the issuer exceeds the threshold for becoming a reporting company under Exchange Act rules.	Annual report on Form C-AR, including financial statements satisfying the requirements applicable to its most recent offering statement. Form C-AR requires information similar to the offering statement on Form C.	None, unless/until the issuer exceeds the threshold for becoming a reporting company under Exchange Act rules.	Annual reports on Form 1-K (with audited financial statements), semi-annual reports on Form 1-SA (with unaudited financial statements) and current reports on Form 1-U.	Yes, annual report on Form 10-K and other periodic reporting is required.	Yes, annual report on Form 10-K and other periodic reporting is required.
Blue Sky Requirements Preempted?	Yes.	Yes.	Yes.	No. Issuers must comply with state blue sky registration and qualification requirements where offers and sales are to be made.	Yes.	Yes.	Yes.
Combinations Permitted	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Integration Concerns	Yes, if multiple offerings occur within six months, must ensure that each component satisfies the applicable exemption.	Yes, if multiple offerings occur within six months, must ensure that each component satisfies the applicable exemption.	Limited to $1 million per 12-month period.	Limited to $20 million per 12-month period.	Limited to $50 million per 12-month period.	None.	None.

Industry Update: Entrepreneur Rule

Parole for Entrepreneurs

BY DOUGLAS HAUER AND SAMUEL ASHER EFFRON

At MintzEdge, we are already thinking about how a recent immigration law development may help our clients grow their ventures. The United States Citizenship and Immigration Services (USCIS) recently announced a new rule for entrepreneurs. If the rule becomes law, qualified entrepreneurs would be considered for parole (temporary permission to be in the United States) to jumpstart and build their businesses in the United States. The rule is a path-breaking proposal because it seeks to use and retrofit an existing immigration benefit called "parole" to meet the needs of entrepreneurs, who may otherwise be unable to secure a nonimmigrant visa such as an H-1B or E-2 visa.

While this proposal could be a solution for some entrepreneurs, it contains requirements that are out of step with

the realities of many emerging companies. Note that we may not see a final rule published until next year (if at all), and any final rule would likely have adjustments. The proposed rule is intended to accelerate innovation that will have a broad impact on the United States, but is burdened with job creation and minimum investment requirements that aspiring and potentially IPO-bound entrepreneurs would not be able to satisfy in the initial years of growing a business.

What are the criteria for a two-year grant of parole to an eligible entrepreneur?

Under the proposed rule, the United States Department of Homeland Security (DHS) would be able to parole, on a case-by-case basis, eligible entrepreneurs of startup enterprises for a two-year period to grow their businesses. Qualified entrepreneurs are those who:

- have a significant ownership interest in the startup (at least 15%) and have an active and central role to its operations;
- have formed a startup in the United States within the past three years; and
- can show evidence that their startup has substantial and demonstrated potential for rapid business growth and job creation.

The proposed rule would require an entrepreneur to provide evidence of $345,000 of investment capital from arm's length, qualified United States investors with established records of successful investments. The entrepreneur would not be permitted to calculate any personal investment to their venture in showing a qualifying investment. Also disallowed would be funding from immediate family members.

In the alternative, an entrepreneur seeking parole benefits could show significant awards or grants (at least $100,000) from certain federal, state, or local government entities with expertise in economic development, research, and development, and/or job creation that regularly provide such awards or grants to United States businesses.

The proposed rule would allow partial satisfaction of one or both of these criteria, in addition to other reliable and compelling evidence of the startup entity's substantial potential for providing a significant public benefit. We don't know how the terms "substantial potential" or "significant public benefit" will be defined in a final rule, but we think that entrepreneurs with STEM backgrounds (science, technology, engineering, and mathematics) may have an edge in showing impact to the public.

Who may benefit from this rule if it is finalized?

Entrepreneurs growing technology or R&D startups that can attract experienced venture capital firms, angel investors, or qualifying government grants early in the seed financing stage, and within two years of formation, may be strong candidates for parole. However, no more than three founders or employees of any one entity would be eligible to qualify for parole benefits under the proposed rule. The rule would allow a fixed stay of two years only, after which an extension or transition to another visa status would be necessary to remain in the United States.

What are the requirements for securing a re-authorization of parole for three years?

For eligible entrepreneurs wishing to stay in parole status beyond two years, extending parole or "re-paroling" will be necessary. But the extension provisions proposed by DHS may be unworkable for entrepreneurs of even promising and vibrant emerging ventures.

To "re-parole" for three years, an entrepreneur would be required to provide reliable evidence that the startup continues to have a substantial potential for rapid growth and job creation. DHS proposes that this be satisfied by the entrepreneur showing that the startup has achieved the following in the two-year window preceding the extension: (1) received substantial additional funding of $500,000 or more from qualifying United States investors; (2) generated substantial and rapidly increasing annual revenue of at least $500,000 in the United States over the prior paroled period; and (3) generated 10 full-time, direct jobs for US workers. The entrepreneur must also establish compliance with household income requirements during the prior paroled period.

These metrics will be very tough to meet. Many entrepreneurs will be unable to satisfy the revenue generation

and job creation requirements when it comes time to “re-parole.” In certain industries such as life sciences and clean-tech, an emerging company often needs several years of lead time to navigate complex regulatory requirements before commercializing novel products and becoming revenue generating. The proposed framework would lock out strong ventures that grow on a runway of five to ten years.

It is also impossible to predict that capital investment will be available in a timeframe that lines up with a request by an entrepreneur to “re-parole.” Sourcing capital is not an exact science and can take even successful ventures more time than anticipated. Although the proposed rule permits that the totality of facts will be reviewed in an extension process, the criteria as proposed are not workable for many – if not most – talented entrepreneurs wishing to grow a venture in the United States.

Conclusion

DHS needs to introduce more flexible provisions in the final rule for it to have the intended effect of jumpstarting businesses in the United States. Overly stringent criteria on the amount of a qualifying capital investment, revenue generation, and job creation need to be revised. Many foreign entrepreneurs who have more conventional visa options will likely elect to consider parole as a last resort, if at all, if the criteria are unworkable.

While the proposed solution by DHS is imperfect, it is a positive step in the direction of advancing solutions for attracting and retaining entrepreneurial talent. If the criteria for parole benefits are more accessible, we may have an additional option in our toolkit of solutions for foreign entrepreneurs growing ventures in the United States.

Innovator Profiles

Vidrovr

Joe Ellis and Dan Morozoff have been fascinated with the way people obtain information from videos and how these videos lead to our understanding of the world. The pair met four years ago as doctoral students at Columbia University on a project called News Rover. Along with their advisor, Shih-Fu Chang, the pair and colleagues set out to answer the question of why viewership in television news has drastically declined over the past 10 years, and how they could solve this problem. They decided that the internet has fundamentally changed the way people consume news. In today’s society people only want news they are interested in, on-demand, and from perspectives they trust. This hardly describes the paradigm that currently exists in television news.

To solve this problem, Dan and Joe built a television news processing system called News Rover, that ingested up to 100 hours of raw TV news a day and then organized video clips based on information within them. For example, the system could organize the clips based on what news event was being discussed, who was actually speaking, what they were saying, and what was appearing on screen. News Rover won multiple academic and industry accolades including 1st Place in the ACM Multimedia Conference Grand Challenge in Barcelona. The technology developed was patented by Columbia University, and the team started thinking about possible commercial applications of their academic achievements. Through the News Rover project, the team have published and patented foundational research in machine learning, computer vision, multimodal information processing, and multimedia.

Dan and Joe joined the NYC Media Lab’s Combine Incubator program in January to try and understand whether the News Rover technologies could be transformed into a viable business. They learned that content creators are severely under monetizing this portion of their business, because the internal video content management solutions for searching, recommending, and disseminating their video content are currently inadequate. To address these needs, Dan and Joe have founded Vidrovr to bring the technology they developed to the people who need it most.

Vidrovr can index, search, and recommend video content in a cost-effective, automatic, and accurate manner. Vidrovr addresses three key market needs: 1. Domain and customer-specific automatic metadata generation for videos, 2. Video Content Management solutions that enable automatic placement and recommendation of video clips for across a company's digital products, and 3. Automatically linking and sourcing visual social media content that is relevant to a particular video or online article before it is published. Vidrovr was recently named as one of the winners of the prestigious Publicis90 competition, which entails investment and mentorship from Publicis Groupe.

Featured Article

FinTech Companies Face Big Privacy Challenges in 2016

BY NATALIE PRESCOTT AND CYNTHIA LAROSE

According to the FBI, "there are only two types of companies: those that have been hacked and those that will be." It does not take an actual data breach, however, for a company to be liable for its data security practices. In March 2016, the Consumer Financial Protection Bureau (CFPB) made this clear when it settled its first-ever data security enforcement action against an online payment processing company, Dwolla. The CFPB pursued Dwolla because it found the company's representations to customers about its cybersecurity misleading – disregarding the fact that Dwolla had never, since its inception, experienced even a single reported cybersecurity incident. As a part of the settlement, Dwolla agreed to sign a Consent Order, pay a $100,000 fine, take certain steps to improve its data security for the next five years, and make accurate representations to consumers. The *Dwolla* case offers important guidance to FinTech companies and provides a framework for data protection and preparedness plans.

The Story of Dwolla Illustrates Startup Privacy Pitfalls

A young FinTech company, Dwolla first launched in Iowa with just two employees. Small but persistent, it secured funding and eventually grew to over 650,000 consumers and $5 million in daily payment transfers. Even the US Treasury Department's Bureau of Fiscal Service saw its potential and included Dwolla – alongside with the industry giant, PayPal – in its online payment system in 2015.

But that was not how Dwolla became famous. As the company learned the hard way, today's consumer privacy protection is different from what it was years ago. Where previously FinTech companies caught consumers' attention through fast growth and innovations, they are now capturing the government's attention with their outdated cybersecurity practices. This was the case for Dwolla.

Dwolla's Case Offers a Cautionary and Valuable Lesson

The CFPB investigated and sued Dwolla for its public representations to customers that its transactions were "safe" and "secure," that its information was "securely encrypted," and that it was compliant with up-to-date data security standards. The CFPB is not the first federal or state agency to warn companies that privacy policies must "say what they mean, and mean what they say."

The *Dwolla* case highlights the need to be proactive and to implement proper security protocols, which can avoid the breach altogether or at least negate the risk of penalties. What it leaves unresolved, however, is (1) to which extent FinTech companies may benefit from proactively reporting cybersecurity breaches and concerns, (2) whether various regulators intend to collaborate by way of uniform guidelines and joint enforcement actions, and (3) if the companies may seek advisory opinions from the CFPB on their current practices.

The CFPB Joins Other Regulators in the Privacy Enforcement Arena

While *Dwolla* was the first-ever privacy and security action by the CFPB, other regulators have long ago entered the field. They include the Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), Commodities Futures Trading Commission (CFTC), the National Futures Association (NFA),

the Department of Justice (DOJ), the Federal Trade Commission (FTC), and state Attorneys General.

The *Dwolla* action is most noteworthy, however, because the CFPB did not wait until an actual data breach. In an aggressive move, the CFPB prosecuted Dwolla despite lack of harm. The CFPB used *Dwolla* as a test case, (1) to provide guidelines to other companies on what it believes to be reasonable and appropriate in the arena of privacy protection, and (2) to warn other FinTech companies whose privacy practices may be non-compliant. This action should provide a warning to younger startups, which may not have fully vetted cybersecurity policies in place – if privacy policies have been reviewed at all. And it is a clear sign that the agencies are becoming more proactive with respect to data-privacy regulatory actions.

The CPFB is following the Federal Trade Commission's path in bringing this enforcement action. Its authority under 12 U.S.C. § 5531(a) allows it to regulate "unfair," "deceptive," and "abusive" practices, akin to the powers granted to the FTC under the FTC Act. Under what is known as the Dodd-Frank Wall Street Reform and Consumer Protection Act, the CFPB can take actions against financial companies that misrepresent privacy safeguards. Importantly, the CFPB can also seek fines for non-compliance. The Act further requires all companies that offer financial services to abide by the consumer-financial-protection regulations.

The *Dwolla*-*Wyndham*-*HTC* Decisions Finally Establish Clearer Privacy Guidelines for US Companies

Although most legal commentators focus exclusively on *Dwolla* and the CFPB, the *Dwolla* consent order has a much broader implication. This action was not just about the CFPB or an isolated incident of misstatements about online security. When read together with other key enforcement actions, the *Dwolla*-*Wyndham*-*HTC* trifecta represents the clearest guidelines the financial industry has available to date. In many respects, the *Dwolla* consent order builds on the foundation set forth by the *Wyndham* and *HTC* enforcement actions discussed below and then further expands on it by imposing penalties. And, although the CFPB has not previously issued clear guidance in this arena, the *Dwolla* case now fills that gap.

By way of background, Wyndham Hotels and Resorts experienced three major data breaches in 2008-2009 that compromised consumer information and led to over $10 million in unauthorized credit card charges. The FTC brought an action against Wyndham in federal court, which settled last year. The gist of the lawsuit was the allegation that Wyndham engaged in "unfair and deceptive practices" because it promised customers to follow rigorous security standards while its actual standards were inadequate. The company argued that there were no clear guidelines and no fair notice from the FTC. The court disagreed, noting that the FTC's guidance documents, enforcement actions, and prior settlements provided sufficient notice as to what measures are reasonable. In the end, the FTC required the company (1) to "establish a comprehensive information security program designed to protect cardholder data," (2) to conduct annual information security audits, and (3) to "maintain safeguards in connections to its franchisees' servers." Yet, despite evidence of actual consumer harm, there were no monetary penalties.

Another notable consent order originated in 2013 between the FTC and HTC America Inc. There, again, the FTC claimed that the company engaged in unfair and deceptive business practices, including lack of proper training and data security protocols. The FTC alleged that the company's platform had a number of security deficiencies, while representing to customers that higher-than-actual security standards were in place. In the end, the company stipulated to a 20-year-long consent decree, which required it to address current vulnerabilities and to implement a comprehensive security program.

Read together with *Dwolla*, these decisions provide an unequivocal answer to what the FTC and the CFPB expect from companies that handle consumer data.

To Prevent Data Breaches and Show Good Faith, Companies Must Follow 10 Steps

Dwolla and its progeny established a broader regulatory landscape for financial privacy and provide a practical guide to FinTech companies with respect to privacy practices. Post-*Dwolla*, companies that handle sensitive consumer information must follow these 10 steps to shield themselves from enforcement actions:

1. **Make accurate representations to customers.** Companies must review their online and direct

representations to consumers and verify that their listed privacy policies and statements regarding data security are current and accurate.

2. **Regularly update privacy and data security policies.** Companies must review and routinely update their policies, ensure that they follow the latest protocols, and provide the most advanced protection of consumer data. This includes a policy not to collect data unnecessarily – after all, the more data the company has, the more data it will lose in the event of a breach. Updating policies is not enough, however. Companies must also ensure that the employees actually know about and follow these policies.

3. **Prepare a comprehensive Data Security Plan.** The Plan must include safeguards for preventing a breach, steps necessary to identify a breach, and protocols to follow in the instance of a breach. Additionally, the companies should obtain cybersecurity insurance coverage.

4. **Conduct annual information security audits.** Depending on the size, FinTech companies should either conduct a smaller-scale internal audit or retain an outside auditor. The audit can identify potential weaknesses, analyze whether the current practices are up-to-date, and even uncover a breach that may have occurred and gone unnoticed.

5. **Train employees on data security.** Every employee who handles sensitive data, every manager, and all IT personnel must undergo regular mandatory training. They should know how to handle consumer data, how to spot potential breaches, how to avoid them, and where to report them.

6. **Rely on latest technology.** Companies should utilize data loss protection software, which can detect internal unauthorized data downloads. Additionally, digital rights management software can track where sensitive data is going.

7. **Have an anti-USB policy.** Because many breaches occur from within, companies must ban the use of thumb drives, storage drives, and other removable media by employees. They should also prohibit the storage of personal consumer data on employee laptops.

8. **Always encrypt sensitive data.** Companies should password-protect sensitive documents. Employees should not send or receive identifying personal information via e-mail. Encryption must be used for data in transit. Additionally, companies should consider double encryption, which may soon be the new golden standard for the FinTech industry.

9. **Test your operations and vet your vendors.** The IT department should be responsible for periodic testing of the operations and compliance. This includes phishing-assessment campaigns, internal audits, and analysis of individual employees' practices. Where gaps exist, additional mandatory training is necessary. Furthermore, companies must appropriately vet their vendors – who access customer data – and ensure that the vendors' security practices also meet current standards.

10. **Designate a privacy reporting manager.** Every company should have an employee responsible for privacy compliance and reporting. Employees must know where to turn in the event of a breach or lack of compliance. In larger companies, this role belongs to a Chief Privacy Officer, while in smaller firms, it may fall on the IT or HR manager. Irrespective of the title, privacy officers must have proper training and qualifications.

FinTech Startups Will Continue to Face Big Security Challenges

Cybersecurity compliance is important because data breaches are on the rise in the financial sector. This trend is noted in the Verizon 2016 Data Breach Investigations Report, a comprehensive analysis of cybersecurity threats and breaches. Last year, the Report analyzed over 100,000 security incidents and 2,260 confirmed data breaches across 82 countries. In 2015, the Report notes, the finance sector encountered 1,368 incidents of compromised online security and 795 instances of actual data loss.

The financial industry is at the top for targeted attacks through web applications. It's "where the money is." For financial services, web app attacks are the main vulnerability and account for nearly half of all security breaches.

Typically, the attack exploits code-level vulnerabilities and thwarts authentication mechanisms. Hackers are driven to financial companies for monetary gain, espionage, and information gathering to aid in a different attack. Importantly, it does not take long to infiltrate online security: In 98% of cases, financial factor systems are compromised in a matter of minutes.

Although No Uniform Privacy Laws Yet Exist, the Pressure on FinTechs to Comply is Rising

When a FinTech company becomes a victim of a cybercrime, it faces serious consequences. Data itself is compromised, the system is affected, revenues suffer, and reputational damage follows. Needless to say, for young FinTech companies and established financial institutions alike, reputation is paramount, and the consequences of a data breach can be long-lasting. The risk of consumer class actions and regulatory enforcement actions only complicate things further.

Unfortunately, US Privacy and cybersecurity laws and regulations are anything but clear. They are numerous, they co-exist at the state and federal level, and there is no comprehensive and uniform regulatory system in place. There is also not one official authority in charge. As discussed above, many different agencies seek to regulate privacy laws. But because of the sensitive nature of the information involved, FinTech companies face more pressure when compared to other industries.

FinTech Companies Face Greater Scrutiny Because They Are Intimately Involved in Consumers' Lives

FinTechs face tougher penalties for data breach, in part, because they typically collect and retain the most personal data about a large group of consumers. They are the ones most likely to have custody of particularly sensitive data. For example, companies offering mobile payment solutions may gather names, addresses, dates of birth, telephone numbers, Social Security numbers, bank account and routing numbers, passwords, and PINs.

Consumers and agencies justifiably expect the highest level of protection from the FinTech industry because of the special relationship of trust. As a result, financial companies face more scrutiny in general. In May 2016, the CFPB issued a proposed rule that would restore the customers' rights to sue financial institutions and will no longer allow them to include mandatory arbitration clauses in fine-print contracts. And The New York Department of Financial Services recently announced that it was soliciting input from other regulators on how banks and startups can bolster cybersecurity.

In short, the CFPB and other regulators believe that FinTech's access to sensitive data represents a unique threat to consumers. In a press release, the CFPB's Director Richard Cordray explained, "Consumers entrust digital payment companies with significant amounts of sensitive personal information…. With data breaches becoming commonplace and more consumers using these online payment systems, the risk to consumers is growing. It is crucial that companies put systems in place to protect this information and accurately inform consumers about their data security practices." Lack of notice or certainty in the privacy regulatory arena will not shield the industry from the CFPB, especially since *Dwolla* and other recent enforcement actions now provide in-depth guidance.

The CFPB's Authority to Impose Fines Provides It with Greater Leverage

FinTech companies who closely followed *Dwolla* should not assume that the same lower penalties will be the standard for future actions. The CFPB's fines greatly range in size. This is why the CFPB's actions have more bite to them: In contrast to the FTC, which lacks the authority to impose fines for unfair and deceptive practices in these circumstances, the CFPB can seek monetary penalties and mandate compliance. The CFPB's Civil Penalty Fund is a depository for these collections. Since establishing the fund six years ago, the CFPB has already obtained well over $200 million in fines. This does not include more recent actions and the relatively small – in comparison – sum of $100,000 it received from Dwolla.

The CFPB uses the money to reimburse the victims (including victims of unrelated breaches) and to educate consumers on data privacy and financial literacy. In 2013, a staggering $13.8 million of these funds went towards consumer education. In short, the CFPB's ability to levy monetary sanctions undoubtedly gives it a lot of leverage in cases where there are no actual damages.

* * *

As for Dwolla, it has recently issued a public statement: “It has never been the company’s intent to mislead anyone on critical issues like data security. For any confusion we may have caused, we sincerely apologize.” Reportedly, “Dwolla’s current data security practices [now] meet industry standards.”

Upcoming Events

New York

September 26–27: IAB MIXX

September 29: Convertible Notes for Startups: Lunch & Learn with Mintz Levin at Columbia Tech Ventures

October 7: The New Yorker TechFest

October 10–16: TechWeek

October 28: NVCA SHIFT: Accelerating Corporate and Venture Partnerships

October 30 – November 2: O’Reilly Security Conference

November 1–4: Fast Company Innovation Festival

November 2–3: ad:tech New York

November 3: The Changing World of Raising Capital

November 15–16: New York City Government Technology Forum

November 16: Momentum

Boston

September 29: SIM Boston Technology Leadership Summit

October 6: MITX Disruptive Innovator Series: Making sense of IoT, AI, 3D Printing, and Other Tech

October 13: Disrupt CRE Boston

October 18–20: MIT EmTech

October 20: Influence(her) Mentor Round Robin – During the City of Boston Women Entrepreneur Week

October 20: TUGG 6th Annual Tech Gives Back

November 3: MITX DesignTech Summit

November 8–11: Inbound 2016

November 17: Xconomy Presents: What’s Hot in Boston Healthtech

December 4–9: USENIX LISA ‘16

San Francisco

September 26–27: GMIC SV

September 27–28: SMIC Silicon Valley

September 28–29: RoboBusiness & Chief Robotics Officer Summit

October 4–7: Dreamforce ‘16 Tech Conference

October 10–11: O’Reilly Next:Economy

October 12–13: Corporate Venturing Summit by Innovation Enterprise

October 13: Quartz’s The Next Billion

October 17: SF MusicTech Summit

October 17–21: NewCo Bay Area

October 18–19: FinDEVr Silicon Valley 2016

October 18–20: Vanity Fair New Establishment Summit

October 21: The Information Subscriber Summit

October 26–27: Tech Inclusion 2016

October 30 – November 6: The Lean Startup Conference

November 1–2: CMX Summit

November 8–9: Structure 2016

November 15–16: LAUNCH Scale

November 15–16: Minds + Machines

November 16–17: FutureStack 16

November 29–30: Open Mobile Summit

San Diego

September 30 – October 2: TwitchCon

October 17: 2016 International Conference on Interactive Mobile Communication Technologies/Learning

October 31: Tech.Co Adobe MAX

October 31 – November 4: Adobe MAX

November 1: San Diego Tech Summit

November 7–10: TBM Conference

Washington, DC

September 27: NVCA CFO Boot Camp

October 11–14: AppSec USA

October 21–23: CyCon U.S.

November 4: Ask a VC DC

November 10–11: Open Minds Technology & Informatics Institute Conference

November 10: Diaspora Demo Experience & Startup Showcase

Contacts

CORPORATE

Daniel I. DeWolf *(Editor)*
Member, New York
212.692.6223
DDeWolf@mintz.com

Jeremy D. Glaser
Member, San Diego
858.314.1515
JDGlaser@mintz.com

Sahir Surmeli
Member, Boston
617.348.3013
SSurmeli@mintz.com

Samuel Effron *(Editor)*
Associate, New York

Dean Zioze
Member, Boston

Jay Clare
Associate, New York

212.692.6810
SEffron@mintz.com

617.348.4795
DZioze@mintz.com

212.692.6816
JJClare@mintz.com

Kristin Gerber
Associate, Boston
617.348.3043
KAGerber@mintz.com

Eddie Rodriguez
Member, San Diego
858.314.1527
ERodriguez@mintz.com

Brian Novell
Associate, New York
212.692.6265
BJNovell@mintz.com

Cliff Silverman
Associate, New York
212.692.6723
CMSilverman@mintz.com

Yilei He
Associate, New York
212.692.6232
YHe@mintz.com

Rachel Gholston
Associate, New York
212.692.6244
RAGholston@mintz.com

Talia Primor
Associate, New York
212.692.6740
TSPrimor@mintz.com

Marc D. Mantell
Member, Boston
617.348.3058
MDMantell@mintz.com

PRIVACY & DATA SECURITY

Cynthia J. Larose
Member, Boston
617.348.1732
CJLarose@mintz.com

Julie Korostoff
Member, Boston
617.348.1638
JKorostoff@mintz.com

Julie M. Siripurapu
Member, Boston
617.348.3039
JSiripurapu@mintz.com

TECHNOLOGY TRANSFER

Julie Korostoff
Member, Boston
617.348.1638
JKorostoff@mintz.com

Ran Zioni
International Member, Washington, DC
202.434.7456
RZioni@mintz.com

Julie M. Siripurapu
Member, Boston
617.348.3039
JSiripurapu@mintz.com

INTELLECTUAL PROPERTY

Peter Corless
Member, Boston
617.348.1859
PCorless@mintz.com

Michael D. Van Loy, PhD
Member, San Diego
858.314.1559
MDVanLoy@mintz.com

Peter Snell
Member, New York
212.692.6850
PSnell@mintz.com