https://doi.org/10.48009/3_iis_2018_220-225
Issues in Information Systems
Volume 19, Issue 3, pp. 220-225, 2018

FINTECH, REGTECH AND THE IMPORTANCE OF CYBERSECURITY

Jennifer Callen-Naviglia, PNC Bank, dr.callennaviglia@gmail.com
Jason James, Sullivan University, jejames@sullivan.edu

ABSTRACT

As consumer demand grows for remote banking services, faster turn around times and e-commerce convenience, financial institutions are forced to advance technologically or risk loss of market share. In keeping up with the times, the financial sector has given rise to FinTech. Regulators' attempts to police FinTech products and services, in turn, has given rise to RegTech. As in all advancing technology, the threat of hackers, security breaches, and theft become a daily concern. Cybersecurity, therefore, plays an essential role in the success and continuing advancement of FinTech and RegTech. The following questions emerge: 1. Does advancing FinTech hinder the role of regulators; 2. Will RegTech be able to adequately keep up with the growing demands of FinTech; and 3. Is cybersecurity advancing in a manner to provide proper protection against financial threats. This paper explores, through a literature review, the role of FinTech, RegTech and the reliance on effective cybersecurity.

Keywords: FinTech, RegTech, Cybersecurity

INTRODUCTION

FinTech, RegTech and Cybersecurity go hand in hand within the financial sector realm. Advancing technology continues to evolve the United States financial industry through FinTech products and services. This evolution is creating a paradigm shift within financial regulatory bodies. This paper examines the literature to provide a synopsis of the relationships between FinTech, RegTech, and Cybersecurity. This paper includes five sections: (1.) What is FinTech (2.) The evolution of FinTech (3.) What is RegTech (4.) Role of RegTech (5.) Cybersecurity

What Is FinTech

The term FinTech has gained eminence within the past 3 to 4 years and refers to emerging technology within the financial sector either by way of newly developed products, evolving services (Ng and Kwok, 2017; Skan, Dickerson, and Masood, 2015; et.al.) or internal technological advancements. Examples, of newly developed products and evolving services, range from credit card services to online banking to digital currencies (FinTech Futures, 2018). Internal technological advancements refer, but is not limited, to a financial institution's adaptation of legacy systems or the internal implementation of cloud based system. The implementation of FinTech enables consumers, investors, and businesses the ability to keep up with trends, expand market share, and provide services with minimal to no fees (Sanicola, 2017).

According to Forbes (2018) the following are the most anticipated FinTech trends for 2018:

- Automated financial decisions and actions (i.e. autopay, financial apps)
- FinTech acquisitions by big banks
- Advanced identity validation within financial services
- Fraud and risk automation
- FinTech growth within B2B lending
- Advancing KYC (know your customer) products

The Evolution of FinTech

Despite the increased acknowledgement of FinTech within the last 3 to 4 years, technology and the financial sector have a long standing relationship within the U.S. Monetary System (Callen-Naviglia, 2017; Arner, et.al, 2017). Figure 1 depicts the evolution and growth of FinTech within the U.S. Monetary System.

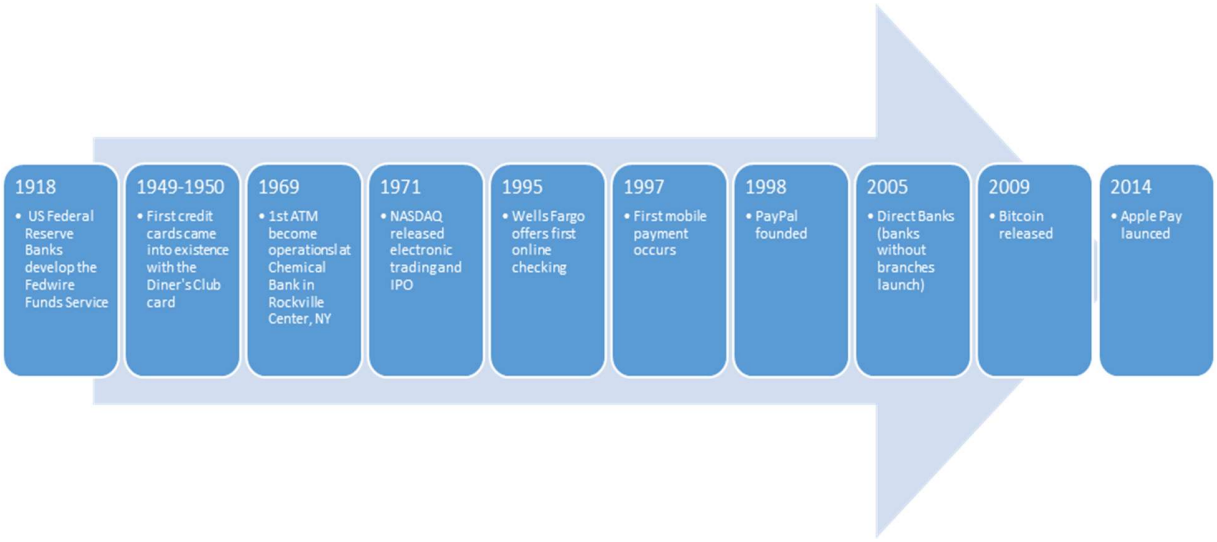

Figure 1. The evolution and growth of FinTech within the U.S. Monetary System (banktech.com, 2017 and Callen-Naviglia, 2017)

Investment in FinTech has grown rapidly since the financial crisis of 2008 (Skan, Dickerson, and Masood, 2015; Ng and Kwok, 2017; and Arner et.al., 2017) which did not solely affect the United States but reached into the European and Asian markets. Financial institutions strive to reinvent or develop new products and services to remain relevant within the industry and meet consumer product and service demand (Ng & Kwok, 2017). Narrowing the scope and focusing solely within the United States, U.S. financial institutions' technological advancements created a need for development within the regulatory and compliance spectrum (Arner, et. al, 2017). The evolution of FinTech introduced technological advancements into an industry engulfed in compliance and regulatory oversight. For example, the growing popularity of digital currencies have drawn attention to the questionable effectiveness of current regulations and compliance requirements. Per Kirby (2104), the current regulatory framework is sufficient to monitor and regulate digital currencies. However, in 2015, the State of New York implemented a new regulatory framework, BitLicense, in attempts to regulate digital currencies. New York's BitLicense is ground breaking regulatory legislation. The success or failure of BitLicense could make way for similar attempts at regulating FinTech products and services (Callen-Naviglia, 2017; Hughes, 2014).

The technological transformation of the finance industry coupled with the growing reliance of digitized financial products and services have increased the financial sector's risk portfolio and vulnerability to outside attacks by cybercriminals. Per Pascu (2017), data breaches have increased from 19% to 24% during 2016-2017. This increase contributed to the fact that "…78 percent of organizations in the financial sector have increased IT security budgets, up from 58 percent in 2016" (paragraph 4). The need for cybersecurity runs congruent with the advancement of FinTech.

The outstanding question is, does the advancement of FinTech hinder the role of regulators? Kidd (2018) argues, FinTech advancements will supersede regulators' compatibilities to effectively regulate within the financial industry as workloads are expected to increase as innovation speeds up "…requiring them (regulators) to do their job more rapidly but, ideally, without any loss of accuracy and efficacy" (pg. 1). Kidd notes that FinTech onlookers maintain "…technological innovation is likely to increase beyond the capacity of regulation to keep pace" (pg. 1). Based on the FinTech observers' argument, Kidd (2018) contends that highly regulated industries, such as the financial sector, will begin "…using regulation as a way of crowding out competition in order to protect profit margins and market share" (pg. 1). The counter to this questionable regulatory oversight for advancing FinTech is RegTech. The questions now become what is RegTech and what role will RegTech play within the regulatory spectrum. This paradigm shift within the financial regulatory sector questions regulators' abilities to maintain accuracy, consistency and effectiveness.

What is RegTech

Magnuson (2018) contends, regulators overlook advancements in financial technology resulting in the need for "…wide-ranging reconceptualization of financial regulation in an era of technology-enabled finance" (pg. 1). Regulating advancing financial technology and transforming the regulation of the financial sector requires the use and implementation of RegTech (Arner, et.al. 2017). As defined by Arner, Barberis and Buckley (2017), RegTech is "…the use of technology, particularly information technology, in the context of regulatory monitoring, reporting, and compliance…" (pg. 371). The evolution of RegTech continues to evolve as new multifaceted regulatory compliance demands are implemented in attempts to keep up with the advancement of FinTech.

Role of RegTech

Regulatory requirements have increased since the 2008 financial crisis and with that regulatory costs (Arner, et.al, 2017; Ng and Kwok, 2017). To this point, Deloitte predicts, in its 2018 banking regulatory outlook, there will be "…no wholesale rolling back of the post-crisis regulatory framework… (pg. 2). Therefore, the lingering issue of how to maintain compliance and uphold risk management within the growing FinTech sector continues. As mentioned previously, financial institutions continue to utilize legacy systems not equipped to handle the now automated and digitized financial requirements. As costs increase to meet regulatory requirements, financial institutions begin to shift to RegTech solutions to meet regulatory obligations while continuing to meet client demands. Figure 2 identifies short-term and long-term benefits of RegTech.

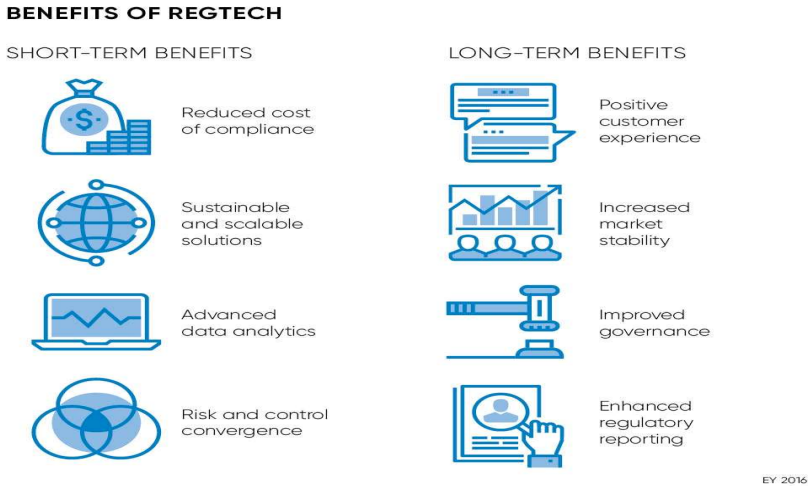

Figure 2. Short-term and long-term benefits of RegTech (Winder, 2017)

This paradigm shift into financial regulations in an era of technology-enabled finance draws into question how secure is the financial sector and FinTech products and services. The role of cybersecurity and its significance within the U.S. marketplace continues to gain in momentum. The *Importance of Cybersecurity* section details the necessity and challenges of cybersecurity's role within the U.S. marketplace.

Importance of Cybersecurity

The Internet and information technology has transformed the world and has created new opportunities for the global economy and humanity at the globe. Civilization reliance on the Internet and information technology, however, has also exposed new vulnerabilities and a multitude of cyber activities by a diversity of hackers, criminals, terrorists, state and non-state actors (Spidalieri & Kern, 2014).

Public and private companies, as well as government agencies, have been victims of cyber-attacks. The United States critical infrastructure, including air traffic control systems, electric power grid, telecommunication networks, and financial systems, are susceptible to cyber-attacks and as the reliance on information technology continues to increase exponentially around the world, the cyber attacker motivations continue to rise (Spidalieri & Kern, 2014).

Since the tragedy of 9/11 and the Enron and WorldCom scandals that resulted in passage of the Sarbanes-Oxley Act, there has been an unprecedented increase in the nature and severity of threats to information systems as well as increased regulations, state and federal, relating to information privacy and security (Swart, 2007).

As a result, cybersecurity, or the practice of protecting electronic data from unlawful or unplanned use, access, modification, or destruction, is more critical today in 2017 and beyond, than it ever has been. In addition, with the number of data networks, digital applications, and mobile users increasing at an alarming rate, compounded with an increase in the number of cyber-attacks—companies must have ongoing awareness to protect private and proprietary information (University of Phoenix and the ISC2 Foundation, 2014).

As companies and government agencies continue to increase their reliability on information technology and information systems to collect, process, store, and transmit data, the knowledge and expertise of cybersecurity professionals has become more important than ever to protect online activities of individuals and companies. If security is not sufficient, companies will experience more data breaches ranging from minor inconveniences to devastating consequences for individuals and organizations (University of Phoenix and the ISC2 Foundation, 2014).

Since no company is immune to cybersecurity threats, company executives are gradually making cybersecurity a top priority. In fact, company leaders have agreed increasing cybersecurity measures is a critical investment (University of Phoenix and the ISC2 Foundation, 2014) ever since the well-known cyber-attacks in 2014 that included:

- Target (hackers had stolen personal information from an estimated 110 million accounts),
- Home Depot (payment system was breached compromising an estimated 56 million accounts) (Tobias, 2014),
- Neiman Marcus (hackers invaded its systems for several months in a breach that involved 1.1 million credit and debit cards) (Harris, Perlroth, & Popper, 2014)
- JPMorgan Chase (hackers accessed approximately 83 million J.P. Morgan Chase accounts) (Tobias, 2014), and
- Office of Personal Management (OPM) (computer systems were compromised that included sensitive personal information, including Social Security numbers, of roughly 21.5 million people from both inside and outside the government) (Sciutto, 2015).

Cybersecurity is critical in all industries and even more so in the financial world due to regulatory development. With the digital transformation of finance due to FinTech and RegTech, the financial world is more vulnerable to attack by hackers. Since digital data continues to evolve in the financial world, cybercriminal activity will continue to increase the risk of attack from hackers.

Not surprisingly, this is an area of focus for regulators and one increasingly at the center of international attention from organizations such as the FSB and Basel Committee.(The Board of the International, 2016) This is in addition to the very natural attention placed on the issue by financial institutions themselves: cybersecurity is one of the most significant risks faced by the financial industry, particularly as the digitization and centralization of processes continues (Dahlgren, 2015). Likewise, for new FinTech start-ups, cybersecurity should be a key concern as these data intensive companies often have a limited comprehension or perceived need of security as they live in a digital world with an abundance of data. Whilst money has scarcity, which drove the development of secure vaults and payment systems, data abundance may not create the right incentive for firms (beyond reputation risks) and can clearly harm consumers. Cybersecurity is thus the clearest example of how FinTech demands RegTech. (Arner, et al, 2016)

CONCLUSION

In conclusion, consumer demand for advancing and convenient financial products and services will continue to evolve the FinTech sector. Regulators must strive to actively maintain oversight equipped to protect consumers and the U.S. economy against technological attacks. RegTech and cybersecurity continue to be at the forefront of tools implemented in maintaining a safe and productive FinTech industry. To continue providing financial stability and consumer safety, RegTech and cybersecurity must advance along with FinTech products and service. Any lag within

either RegTech or cybersecurity within the U.S. financial sector may create vulnerability which may lead to detrimental incidents within the U.S. economy.

REFERENCES

Arner, D., Barberis, J., Buckley, R. (2016). *FinTech, RegTech and the Reconceptualization of Financial Regulation.* Northwestern Journal of International Law and Business.

Avery, C. & Fanger, G. (2014, Nov/Dec). Cybersecurity: The human factor. *FinTech Law Report, 17*(6), 1-14.

Dahlgren, S. (2015). *The importance of addressing cybersecurity risks in the financial sector*, Speech at the OpRisk North America Annual Conference, New York City.

Dattani, I. (2016, June). *Financial Serivces and Fintech- A review of the cyber security threats and implications.* Retrieved April 5, 2018, from https://www.researchgate.net/publication/304023925_Financial_Services_and_Fintech_-_A_review_of_the_Cyber_Security_threats_and_implications

FinTech Futures. (2018, March 5). *Infographic: the incredible growth of fintech.* Retrieved April 5, 2018, from https://www.bankingtech.com/2018/03/infographic-the-incredible-growth-of-fintech/

Grant, G.H. & Grant, C.T. (2014, May). SEC cybersecurity disclosure guidance is quickly becoming a requirement. *The CPA Journal,* 69-71.

Kidd, J. (2018). Fintech: Antidoteto rent-seeking? *Chicago-Kent Law Review, 93(*165).

Magnuson, W. (2018, May). Regulating Fintech. *Vanderbilt Law Review, 71*(1167).

Ng, A.W. & Kwok, B.K.B. (2017). Emergence of Fintech and cybersecurity in a global financial centre. *Journal of Financial Regulation and Compliance, 25*(4), 422-434.

Pascu, L. (2017, December 22). *Financial services industry among top targets of cyberattacks*. Retrieved April 6, 2018, from https://securityboulevard.com/2017/12/financial-services-industry-among-top-targets-of-cyberattacks/

Quora. (2018, January 22). *What will be the most exciting Fintech trends in 2018?*, from Forbes.com: https://www.forbes.com/sites/quora/2018/01/22/what-will-be-the-most-exciting-fintech-trends-in-2018

Sanicola, L. (2017, February, 13). *What is FinTech?* From Huffpost.com: https://www.huffingtonpost.com/entry/what-is-fintech_us_

Sciutto, J. (2015, July 10). *OPM government data breach impacted 21.5 million.* Retrieved December 3, 2015, from CNN.com: http://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/

Shackelford, S. J. & Bohm, Z. (2016). Securing critical North American infrastructure: A comparative case study in cybersecurity regulation. *Canada-United States Law Journal, 40*(1), 61-70.

Skan, J., Dickerson, J. & Masood, S. (2015). *The future of fintech and banking: Digitally disrupted or reimagined?* from Accenture.com: https://www.accenture.com/us-en/insight-future-fintech-banking

Spidalieri, F., & Kern, S. (2014). *Professionalizing cybersecurity: A path to universal standards and status.* Retrieved November 21, 2015, from Salve Regina University: http://www.salve.edu/sites/default/files/filesfield/documents/Professionalizing-Cybersecurity.pdf

Swart, R. S. (2007). *A framework for the integration of information security and assurance within information systems curricula.* Retrieved October 1, 2015, from ProQuest Dissertations & Theses Global: https://reddog.rmu.edu/login?url=http://search.proquest.com/docview/304805660?accountid=28365 (Ascension #304805660)

The board of the international organization of securities commissions, cyber security in securities markets –an international perspective (2016)

University of Phoenix and the ISC2 Foundation. (2014). *Cybersecurity workforce competencies: Preparing tomorrow's risk-ready professionals.* Retrieved September 28, 2015, from International Information System Security Certification Consortium (ISC2): https://www.isc2cares.org/IndustryResearch/

University of Phoenix and the ISC2 Foundation. (2014). *Cybersecurity workforce competencies: Preparing tomorrow's risk-ready professionals.* Retrieved September 28, 2015, from International Information System Security Certification Consortium (ISC2): https://www.isc2cares.org/IndustryResearch/