The Journal of Business Inquiry 2016, 15, Issue 1, 17-32
http:www.uvu.edu/woodbury/articles
ISSN 2155-4072

The Evolving Financial Services Industry: The Financial Advisory Role Today and in the Future

By AARON JACKSON, DRAKE P. SAFFELL, AND BRIAN D. FITZPATRICK*

Cyber security is emerging as a leading corporate and government issue, and it will be the topic at the forefront of the financial services industry's list of concerns in the years to come. Data management and solutions companies stand poised to take advantage of these changes within the industry. The authors will develop a new consumer model which we believe will be adopted in the financial service industry by the year 2020. The impact these changes will have on the financial advisor/client relationship remains to be seen.

Keywords: Data Management, Financial Services Industry, Consumer Model

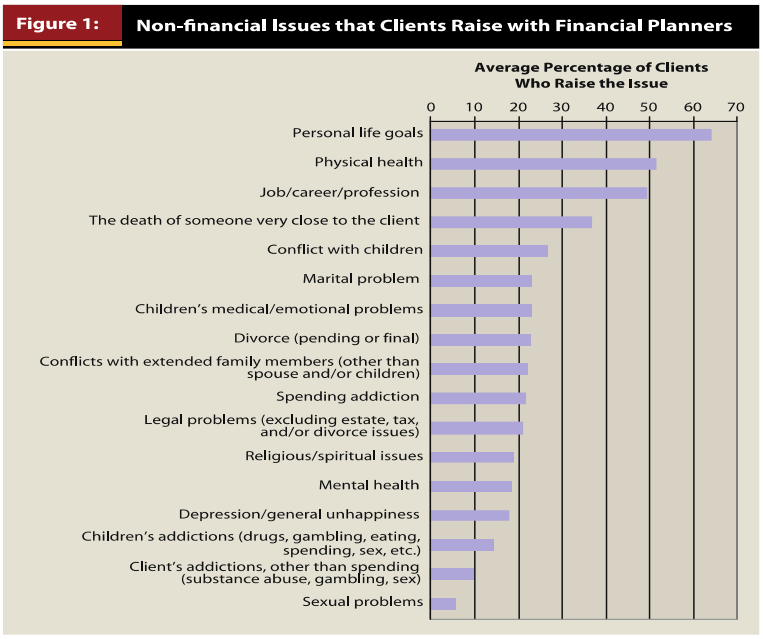
JEL Classification: G

I. Introduction

Financial advising has traditionally been thought of as a career dealing strictly with investment strategies and financial figures. In recent years this career has added yet another role, that of life coach. Dealing with an individual's or family's financial situation involves very personal issues, which has led clients to share more information about their private lives. In a study performed by Dubofsky and Sussman (2009), one response to a general comment section of a questionnaire stated: "When someone trusts you enough to open up about finances, usually they will open up about other more personal issues." From the results of their study it was found that out of the 1,374 financial advisors surveyed, over 74 percent have seen an increase in dealing with non-financial issues with over 25 percent of their time on an average day being spent on non-financial issues (Dubofksy and Sussman, 2009). The non-financial issues of clients that financial advisors have been facing are diverse, ranging from personal health to religious or spiritual issues. The chart below illustrates how financial advisors are expanding their role further than ever before, raising ethical questions on whether financial advisors are qualified to handle such personal life issues.

*Aaron Jackson, Student, Business Apprentice, Cerner Corporation. Phone: (816) 797-5448. Email: aaron.jackson@cerner.com. Drake P. Saffell, Student. Phone: (316) 737-4295. Email: saffelld@hawks.rockhurst.edu. Brian D. Fitzpatrick, Professor of Finance, Rockhurst University, Helzberg School of Management, 1100 Rockhurst Road, Kansas City, MO 64110. Phone: (816) 501-4577. Email: Brian.Fitzpatrick@rockhurst.edu.

Figure 1: Non-Financial Issues that Clients Raise with Financial Planners



Source: Dubofsky and Sussman (2009).

The financial advisor's role as a life coach will continue to develop as more aspects of their clients' lives become a part of their financial plan. Multiple clients looking for financial assistance with regard to their personal lives are seeking saving strategies for their children's education and for supplemental income for lifestyle expenditures. We believe that the financial advising role will continue to develop along the life-coach path for another four to five years before technology once again will change the sector as we know it. For the next four to five years, the financial advising sector will still need to answer the question of whether it is ethical for finance professionals to be handling matters involving life issues. To address this challenge, it will be essential for advisors to enroll in life-coaching classes that cover the aspects of self-awareness, social awareness, self-management, and relationship management. According to Dubofsky and Sussman's study (2009), only 40 percent of financial advisors surveyed had taken any courses covering the previously listed issues necessary to conduct their role in a professional manner. With more and more individuals searching for financial advice, it will become imperative that advisors be equipped with the necessary means to handle personal situations as well.

Clients are faced with personal situations that require the use of advisors throughout their lives, and as the financial world becomes more complex in the future, they will turn to advisors more frequently. Advisors will have to prepare for the changing needs of their clients and be able to meet these needs. Further improving the emotional awareness of financial advisors will enable them to meet the needs of their clients, which would in turn increase customer satisfaction. According to the study performed by Dubofsky and Sussman (2009), financial advisors saw increased business because of their non-financial activities in 40 percent of cases.

The proactive approach financial advisors would take – completing classes to improve their non-financial counseling – will meet their clients' needs for the time being. As technology continues to advance the clients' requests will continue to advance as well. By the year 2020 and beyond, we believe that there will be a substantial change within technology that will make

financial decisions and information even more accessible, giving clients more transparency when dealing with personal life issues.

II. Future Trends in Financial Services

The digital revolution has brought about unprecedented changes to every sector of the U.S. economy, and the financial services industry has been impacted more than just about any other sector of the economy by this development. Advanced information systems have been adopted by transfer agencies and payment processing centers. Mobile and electronic banking is becoming vastly more prominent than banks' physical branches. Fund management and even financial advising are becoming more software and algorithm driven. Trading has been overtaken by high-frequency traders and their high-powered computing capabilities. The present state of the world is undeniably reliant upon computers, software, and advanced networks that help to keep them closely interconnected, and the financial sector is inseparable from this state of affairs. These technological developments have been largely beneficial and progressive, but they do not come without challenges. The rise of digital based alternatives to traditional financial services activities has brought about a new environment within which finance companies must compete.

Within the last couple of decades, the financial landscape has been completely altered. Not long ago, online banking and trading platforms were huge innovations. Now, it is all but commonplace for banking, trading, and account management to appear right at an individual's fingertips on mobile devices. Physical offices and branches are seen as less necessary as well as costly; their growth has slowed as the need for them diminishes (KAW, 2014). The human element is becoming less and less prevalent while the technological element grows exponentially. From the consumer perspective, this is no great loss. As millennials make up a larger portion of the U.S. consumer base and workforce, cultural desires and needs will shift dramatically (Lynch, 2013). These consumers are focused on three trends: (1) efficiency and speed, (2) transparency and fewer layers of bureaucracy, and (3) lower fees and fewer unnecessary expenses (Booz Allen Hamilton, 2014).

The world is becoming more digitized as individuals expect activities to become quicker, easier, and more streamlined. After all, the whole point of technological innovation is to decrease human inputs while simultaneously increasing outputs. The new generation, in particular, has little patience for the inter-workings of large corporations. Requests should be processed immediately, accounts should be opened instantaneously, and payments should clear promptly. These expectations are the curse of being brought up in a world where technological innovations have occurred more rapidly than at any other time throughout human history; the present status quo is never enough. These expectations have formed a new paradigm within which financial services companies and indeed all companies must do business.

Efficient in the consumer's eye means whatever is convenient at the time, and to be convenient at all times, finance companies must offer their services across all platforms. That must include developing products for the platforms of the future, be it the Apple Watch, Google Glass or something yet to be created. Each new addition to the arsenal of consumer tech brings about a change to consumers' lifestyles and ways of performing everyday activities (KAW, 2014). It is difficult for a finance company to call itself efficient and up to date if it doesn't have an app on the latest digital platform.

A desire to increase speed necessitates that transactions, processing procedures, and even fundamental financial functions such as clearing checks or crediting accounts be completely

reevaluated. Processes can only be refined up to a point, and when that point is reached, a new process must be developed if further progress is to be made. The fact of the matter is, new entrants into the financial world will find a way to perfect systems and refine current best practices. As these newly created methods become the norm, the old and snail's pace forms of conducting commerce will fall by the wayside, as will the companies that fail to change with the times. Upon evaluation of current procedures, it becomes evident that the future will entail more programs, more algorithms, more artificial intelligence, and fewer human beings. Compared to a properly coded and run program, humans make substantially more errors and take much longer. Technology's purpose is speed and efficiency, and these objectives will be accomplished through its continued implementation.

Computers will continue to replace humans in positions involving data entry and financial transfers; the issue of too many bureaucratic layers should correct itself. As fewer individuals are needed to touch papers and view electronic documents, the time it takes to complete client requests and routine tasks will be dramatically reduced. However, the resolution of one headache may lead to another. The consumer desire to deal with fewer people may create a situation in which their other desire for transparency becomes more difficult to achieve. As computers pick up more and more of the workload, there will be less explanation and clarity as to what is taking place.

Unless there is adequate human oversight, there may actually be less transparency than before. The need for transparency all ties back to the great mistrust the general populace has for the financial industry. According to the Harris Reputation Quotient1[1], only tobacco and government rank lower than financial services (Lynch, 2013). Especially during a time when the industry is rapidly changing due to technological innovation and new product development, the morality and integrity of companies going forward will be pivotal to their success. Unfortunately, there may be less of a reassuring human element at the exact time it is needed most. This is just one example of the difficulties companies face in appeasing consumers and their contradictory desires.

Part of the reason the younger generation is so focused on transparency is that they want to know exactly what they are paying for and why. Any random or conspicuous fee sets off warning sirens, and the impacts are powerful enough to turn customers away. As the financial industry becomes more democratized and commoditized, consumers are establishing low costs as their top priority (Booz Allen Hamilton, 2014). If two funds look similar, if two online trading platforms look similar, if two IRA custodians look similar, the one with the lowest fees will generally win.

It would appear that the elimination of human labor and the implementation of software would drive down costs and allow financial institutions to drop fees, but this may be an erroneous conclusion. The development, attainment, and maintenance of software, as well as advanced information systems, are very expensive. In many cases, small to medium institutions may postpone implementation because of the large costs (New York State Department of Financial Services, 2014). The revenues that banks use to fund these costs are generated from the fees they charge their customers, and financial services and solutions companies generate similar fees from their clients. The combination of downward fee pressure from consumers and upward cost pressure from technology-driven R&D makes for a volatile mix in the midst of threats from new entrants.

According to Berman (2015), Northwestern Mutual already has a personal finance site called the Mint GRAD, which is targeting college students and recent college graduates. This site features millennials who possess experience managing their student loans or addressing their undesirable credit card debt. Emily Halbrook, who is director of the young personal market for Northwestern

[1] http://www.harrisinteractive.com/Products/RepurtationQuotient.aspx.

Mutual, says that "peer-to-peer contact and investment content are really important." These posts can assist young adults and potentially capture clients for life insurance, a core product, by stressing how it can benefit millennials today and not just in 50 years in the future (Berman, 2015).

A robo-savings tool labeled DIGIT nudges users, who are an average age of 27, to think more about saving and investing money. Ethan Block, who is the 30-year old CEO of DIGIT, says the inspiration for this product came from his observing his friends working diligently at decent paying jobs, but struggling to relieve themselves of student loans or credit card loan debt. DIGIT links to users' bank accounts and periodically puts away small sums of savings. Berman (2015) believes this robo account is one of many to come to the market in the future.

In a *Wall Street Journal* article, Tergesen (2015) talks about the growing future trend for robo investment advice to join an industrywide trend toward lowering investment minimums, in an effort to attract more millennials as investors.

Personal Capital, a San Francisco firm that manages approximately $1.8 billion, recently reduced the minimum required to open an account to $25,000 from $100,000. Tergesen (2015) states that Personal Capital's average client is 42 years old, and the firm desires to lower their average client's age in the future. CEO Bill Harris believes that these young people are in the earliest stages of their careers and lives, but they are on the road to build significant financial futures for themselves. Tergesen sees many attempts by robo advisors, a broad category that would include companies that offer fully automated services and financial advice, as well as "hybrid" advisors such as Personal Capital that combine computerized services with hand-holding from human advisors.

Currently, Fidelity Investments has commenced testing its own robo product called Fidelity Go, utilizing a small group of company employees. Personal Capital is following the trend to lower minimum fees – lower than the Vanguard Group's hybrid Vanguard Personal Advisor Service, which recently reduced its minimum from $100,000 in the pilot program to $50,000 now. Personal Capital's minimum has been lowered to below the Vanguard Group's minimum. The Vanguard program boasts $26 billion in assets, by far the highest in the industry. The importance of capturing the millennials' investing business is apparently not a flash-in-the-pan commitment. We should all expect more competition and lower fees in the future. In fact, Wealthfront Inc., with approximately $3 billion under management, recently reduced its required minimum investment to just $500, while Bettermint LLC, which manages a similar amount of money, has no minimum required to open an investment account, but does require a $100 automatic monthly deposit for accounts below $10,000 in order to eliminate a $3 monthly fee. The trends are obviously showing lower minimums and fewer fees – exactly what the millennials are looking for. The robo accounts can help attract funds while keeping costs lower – they are building scale (Tergesen, 2015).

Irvin Wladawsky-Berger, who worked for IBM for 37 years and who is affiliated with MIT, NYU, and Imperial College, believes that beyond technology, the evolution of financial services will be influenced by various social, political, and economic factors in the future. He lists four possible future scenarios predicated on different combinations of two vital factors: the rate of technological innovation and the number of financial suppliers. The four possible future scenarios are as follows: rapid change/many suppliers, rapid change/fewer suppliers, slow change/many suppliers, and slow change/few suppliers (Wladawsky-Berger, 2015).

The rapid change/many suppliers scenario shows many existing financial services providers going out of business, with those companies being replaced by new digital entrants. Under this scenario, the new demand, along with uncertainty about the future, will predominate – this sounds familiar. The rapid change/few suppliers system leads to a few major information and

communication technologies (ICT) – e.g., Amazon, Apple, and Google – while traditional financial institutions unable to compete will simply fade away. The customers under this system operate as passive consumers. The slow change/many suppliers paradigm shows that periods of rapid ICT and financial services innovation are followed by long periods of stability and consolidation, where privacy and security will become key competitive advantages. The new suppliers will eventually replace present players who try to reinvent themselves as niche providers or owners of declining profitable asset bases. There is no one supplier who will achieve market dominance. The slow change/few suppliers environment is basically where we are today. Technologies are advancing rapidly, but social factors and privacy issues are constraining the speed of growth. There are a few firms that will emerge in technology ecosystems and financial services. Until the trust issue is satisfactorily addressed, progress will be slower than desired. When trusted relationships are established, then the ecosystems will develop their own long-term savings and investment policies. The transactional payments will be performed usually by new entrants who will exploit existing schemes to maximize data value. The future most likely will not look like any one of these scenarios according to Wladawsky-Berger (2015), but will be an amalgam of all four scenarios. He concludes that the future will change the very nature of money, payments, and identity. The trust relationship will undergo changes never seen before. The future of financial services in the decades ahead will be a challenging journey – changing future generations' demands for these products.

III. Wall Street vs. Fintech

Venture capitalists and Silicon Valley are becoming ever more involved in the evolving field of finance. There is no shortage of start-ups looking to revolutionize the way commerce is conducted and money is handled, and such enterprises are expected to only grow in number. These operations have been dubbed "Fintech," and Fintech is the David hoping to fell the Goliath that is Wall Street (Roose, 2014). Challenging the financial sector head on has never been advisable, for these institutions have massive amounts of capital as well as political clout that they can use to help shape their own destinies.

However, the new technological environment driven by consumer desires is setting up the perfect scenario for an innovative and creative player to take a bite out of the market. People rely on and supposedly like the current systems for automobiles and hotels, yet Uber and Airbnb have made waves within their respective industries (Roose, 2014).

The strongest card that Fintech companies possess may be nothing more than a reiteration of the past. Wall Street, despite being an integral and ingrained part of our society, has a black cloud hanging over its head. It is viewed as an industry full of unchanging, hidebound, rigid companies perceived as fee-hungry giant corporations. Emerging technology companies entering the field of finance have little to overcome from a perception standpoint; they are perceived as sleeker, more efficient, and actually more trustworthy compared to the large players (Lynch, 2013).

According to Rajesh Jayaraman, a Fintech entrepreneur, all financial institutions need to do is move bits around (Roose, 2014). There is rarely any physical product, and as banking progresses, these firms are going to look more and more like software companies. Despite this trend, most traditional financial institutions utilize the same outdated infrastructure – paper checks, debit cards that require punched-in pins, and wire transfers that take days to clear. Meanwhile, venture capitalists are eager to throw their money at banking and financial alternative companies; U.S.-based Fintech start-ups raised an estimated $1.3 billion in just the first quarter of 2014 (Roose,

2014). The huge financial support these companies are seeing represents just how badly the current system needs change, and it is only a matter of time before someone lands a critical blow to the $1.2 trillion financial services industry (Roose, 2014).

It will be difficult and largely unprecedented for financial companies to slim down, streamline operations, and completely change focus to becoming software services providers. Such an endeavor actually looks quite hopeless in the face of such determined new entrants, but the fact of the matter is that this industry is still dominated by a few large players. The resources, politically established entry barriers, and capital access these large institutions possess are forces to be reckoned with. Their current course of action is to follow the greater corporate trend of buying up innovative start-up companies. By purchasing start-ups and Fintech companies, these financial institutions accomplish the dual mission of reducing competition while purchasing valuable patents and human capital that can be utilized to further their own innovation and development efforts.

Wall Street and its ancillary industries have rarely been in the forefront of innovation and change. If something works, they will sail the ship until it runs aground. Such a tactic is hardly optimal for the attainment of new clients and the retention of current ones. In an environment where consumers expect new products, new ways to access these products, and less unnecessary communication – all while paying less money – it simply does not pay off to be a laggard or even a fast follower. These emerging trends represent colliding and conflicting needs, and they do not get resolved by doing business as usual. The nature of the industry has progressed rapidly of late, and it is not going to slow anytime soon. In the midst of this whirlwind, the large financial institutions will be required to act more nimbly than they traditionally have.

The current and future developments in the financial services industry will help to bring about more efficient processes, more accessible information, and continued commoditization. These trends all converge to create a continuum spanning the gap between finance and technology, two essential facets of the modern world. The financial world will become a more technologically competent and consumer-conscious place, but with change comes challenge. As data continue to proliferate, transparency and security will clash; each step towards accessibility and convenience also brings the world closer to vulnerability. Corporations, particularly financial companies, are becoming the target of a new type of attack. These attacks will be waged in bits and over networks, and as technology becomes cheaper and more accessible, the potential number of combatants only increases. The warfare of the 21st century is cyber warfare, and it will be waged on the corporate battleground.

In December 2013, Target, Inc. announced that 40 million customers' credit and debit card information had been stolen. It would later be revealed that 70 million more had their personal information stolen (Walters, 2014). Recently Su Bin, a 49-year-old Chinese national, was indicted for the hacking of government defense contractors. Between 2009 and 2013, Bin's group attempted to steal manufacturing plans from companies such as Boeing and for defense programs such as the F-35 fighter jet (Walters, 2014). In June, personal information for over 80 million individuals and businesses was stolen from J.P. Morgan Chase. The hackers are believed to have originated in Russia and may have ties to the Russian government. In late November, Sony Pictures was hacked, and the fallout included the release of internal communications and sensitive company financial information (Walters, 2014).

Whether originating from foreign governments, competing corporations, or small groups of activists, cyber attacks are becoming both more common and more militaristic. The number of attacks will do nothing but increase from this point onward; this is merely the beginning of a hard-fought campaign.

Another disturbing realization is that financial companies will be nearly always involved, regardless of who the attacks take place against. It is becoming commonplace for Americans to receive letters in the mail from their banks stating that their card has been cancelled or their account has been frozen due to a compromise at some company or vendor. Banks and other financial institutions do not only have their own security concerns to worry about, but they also have to deal with the impacts of hacks on other businesses where their services or cards have been used. Moreover, financial companies are the most prominent direct target for a number of reasons.

Firstly, there is always the possibility that the worst case scenario will take place and actual funds are stolen by way of account takeovers or manipulation (Millman, 2014). It is likely that more activists likening themselves to modern bank robbers will appear in the near future. The proliferation of software managed accounts and data driven decision making will make such efforts all the more streamlined for would-be hackers.

Secondly, there is the crippling effect on capital markets that political opponents may wish to inflict upon certain institutions or even entire countries. If the services of a large financial institution are taken down for even a few hours, the implications become huge, from both an economic and psychological standpoint. There will be observable financial impacts due to a lack of access to funds, and perhaps more importantly, consumers will begin to lose faith in the abilities of companies to keep their money safe. A worst-case scenario would see a run on the banks while the banks have no access to the very funds their clients want.

This could be extended to an attack on established capital markets, including the stock market and all of the related investment banking and asset management activities. The implications of such an event would be catastrophic, seeing as markets react wildly to even minor glitches on exchanges or flash crashes driven by automated trading.

Another reason banks and finance companies are such prime targets is the breadth and depth of the information they possess. Information such as social security numbers, addresses, account numbers, PINs, dates of birth, and much more is necessarily kept on hand because of reporting requirements under the Patriot Act and related regulations. All this information is held in mainframes, databases, or in the cloud, and hackers will persistently try to access it.

If an activist group or foreign entity can successfully compromise companies or functions involved in the U.S. financial markets, then the geopolitical implications are enormous. Warfare is becoming ever more digitized, and this warfare spares nobody. Foreign governments will not just attack the U.S. government; indeed they may find it more effective to attack companies and leverage the damage they can cause to force the hand of the government (Camhi, 2014).

IV. Implications and Actions

It is unlikely that financial companies alone will be able to reshape themselves into organizations up to the task of combating cyber security threats. Fintech companies offer new possibilities, yet they are not established and face difficulties in overcoming the systemic advantages that large institutions possess (Roose, 2014). The future of the industry will not see the elimination of traditional Wall Street or finance, but these companies will, out of necessity, undergo developmental change and progression.

Small and large firms alike will require new services and solutions for handling challenges, and data and information processing companies stand poised to take advantage of these circumstances.

Despite changes they will undertake, banks and asset managers will survive out of necessity. Data management and financial transaction processing companies have the most to either gain or lose going forward. Their businesses consist of services and products involving mutual fund transaction processing, check handling, mail organizing, fund sub-accounting, and general data storage and management. Investment managers and banks will need to be reassured that these existing products are safe and that information is secure. If breaches occur on the back end, the fund company is the one that receives the flak from customers and the media, and in the investing field, perception and brand name are everything. Financial companies will become ever more cognizant of the way third parties process and organize information, and internal oversight will be increasing for both regulatory and competitive reasons (Camhi, 2014). While presenting new challenges, these changes provide an opportunity for third-party processors to prove why their services are necessary. This can be effectively accomplished by way of offering a four-pronged approach to cyber security: (1) reinforcement of current products, (2) development of specialized security products, (3) formation of security consulting teams, and (4) formation of cyber first-responders.

Besides the outsourcing services typically provided, products are commonly offered to companies that wish to perform activities in-house. Examples of such products are DST's TRAC for managing business retirement plans, TA2000 for individual account management and recordkeeping, and AWD for efficiently organizing communications as well as systems, together with the individuals that utilize them (DST, 2014). Investment managers and banks will need to be reassured these existing products are safe and their information is secure. The fund company is the one that will suffer the greatest loss of business and revenue because of a breach.

As new products and services are developed, financial solutions companies will need to place a greater emphasis on the security of their offerings. Totally new products should be developed specifically with the intention of being marketed to financial companies as cyber security products. The unique capabilities of companies such as DST allow them to adapt technologically in ways the firms they serve cannot, while doing so in a more formal and impactful way than Fintech start-ups. This ideal positioning will allow established and trusted brands to enter into this new field of required products and services. DST operational products should be backed up by DST security products.

Selling products to companies is not going to wholly stop sophisticated hackers. Cyber warfare is constantly evolving and dynamic, and its landscape shifts with every technological breakthrough. According to the New York State Department of Financial Services report (2014), emerging technologies and increasing sophistication of threats are by far the top reasons that firms are facing difficulties in implementing cyber security measures. These finance companies have never had to be this dynamic, and it shows. They need more than to be sold a product; they need to be taken step by step through the overwhelming intricacies of cyber security (Booz Allen Hamilton, 2014). Services companies that have established themselves as trusted technology players within the industry are strategically positioned to offer advice and consulting to these firms. Cyber security specialists should work with finance companies to set up sound internal networks and advanced detection mechanisms, while teaching internal oversight of the warning signals they should be looking for.

No amount of preparation or security will completely isolate companies from having their systems and information compromised. An area of great opportunity for data solutions firms will be in the creation of fail safes and teams that respond to successful hacks. There needs to be a plan for the worst-case scenario, and this task is simply too big for most companies to handle; they just

pretend it cannot happen. Sitting by idly in the current state of affairs is tantamount to inviting a hack, and companies must take action (Booz Allen Hamilton, 2014). Again, nobody is positioned better to offer such capabilities than the very companies that currently provide the entire internal infrastructure for transaction processing and data collection. Fail safes should be developed and offered to companies as a way for them to mitigate the negative impacts of hacks, and a swift response is essential for this. Services involving reaction to network compromises will be invaluable to companies as they seek a way to improve their processes for detection, isolation, and mitigation.

Any company seeking to provide cyber security solutions will be undertaking a great and difficult task. It can be likened to preparing for war, for the opponents are militaristic and the implications of defeat are enormous. The financial backbone of our country is under threat, and the companies that come to the rescue will be tremendously respected and admired. Furthermore, they stand to achieve great financial gain. If done properly, the risk of such a business venture failing is slim. Firms will become aware sooner or later of the need to increase their digital security, and if they do not, the government will assuredly implement laws and requirements intended to protect shareholder and customer information. Governments at all levels have made it a priority to evaluate and assess the escalating cyber threats the U.S. is facing, not only for the sake of the companies in their jurisdiction, but for their own sake as well (Camhi, 2014).

The potential market for cyber security solutions is increasing daily. Eventually, every business, organization, and government agency that can afford it will be seeking outside assistance in the face of cyber threats (Millman, 2014). Financial services companies have a unique place amidst all of this because of their integral role in society, the fact that they hold funds, and their possession of sensitive information on millions of citizens. For the immediate future, the focus will be on securing the networks and IT structures of the financial companies, but the business opportunities will expand far beyond.

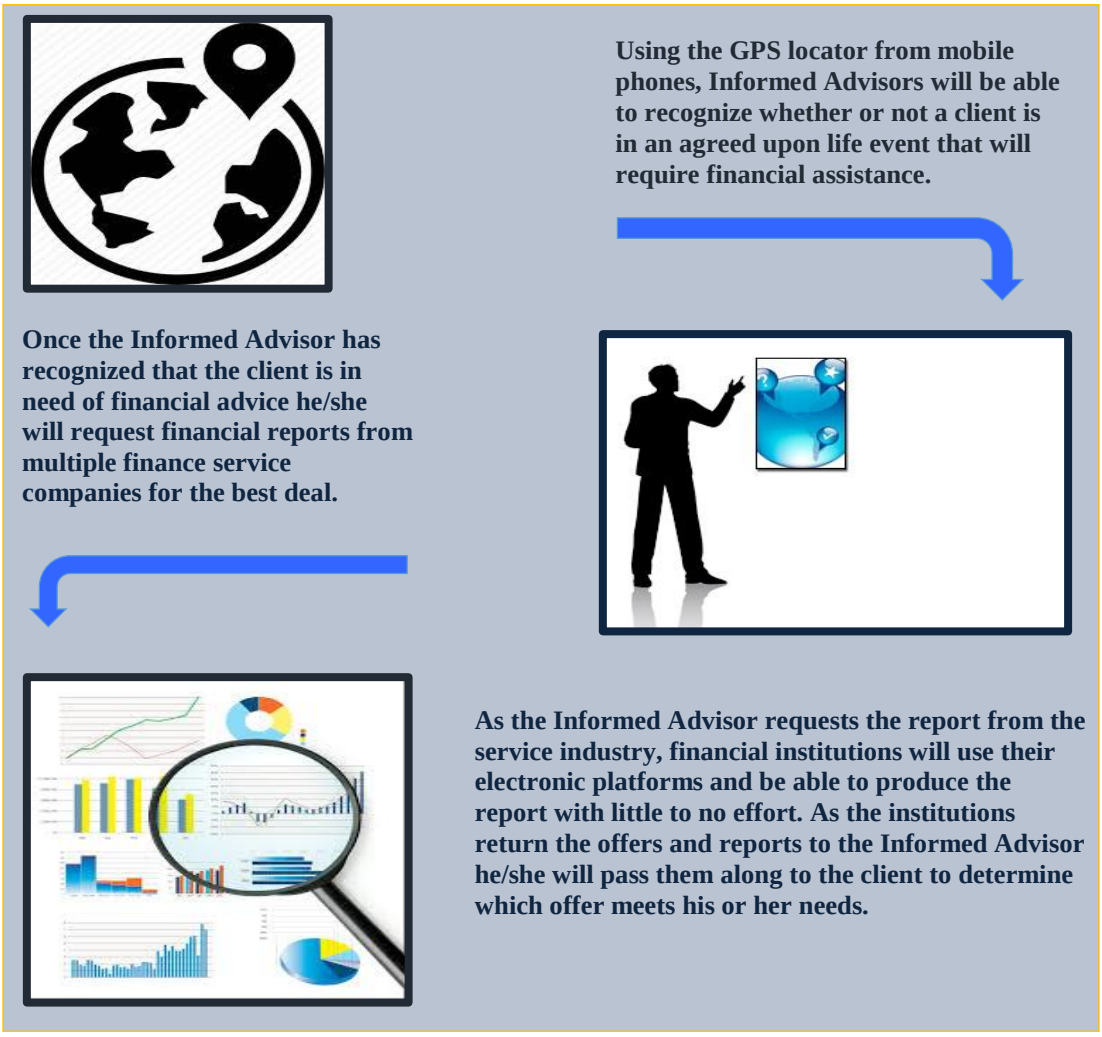
V. The Financial Service Industry in 2020

So far we have discussed the development of financial advisors' roles from a financial professional perspective, and concluded that future roles will always be evolving. As we advance to the year 2020, we believe we will see an integrated model pertaining to financial services. We expect we will transition the role of a financial advisor to what we will call an Informed Advisor. The Informed Advisor will have access to personal information and will be able to provide clients with data reports and advice without their even asking for it. The financial service industry will be alerted by the Informed electronic platform, and will be able to provide a detailed financial report, breaking down the information provided by personal data as well as big data.

The Informed Advisor, having already advanced her/his role as life-coach counselor, will be able to meet with the client on a regular basis highlighting key life events that may need financial attention in the future. As these life events take place in real time, we project that Informed Advisors will not need to be asked by the client for information. When the client and Informed Advisor agree on life events that will need financial attention, the Informed Advisor will be able to put this information into a database. This database will have the capabilities of notifying the Informed Advisor every time the client has entered a business, house, or other commitment that may potentially require financial assistance. We saw earlier that the increase of internet and mobile phone penetration within the world is growing exponentially and the technology to be able to locate a phone using Global Positioning Services is already readily available. Further, the electronic

platform will have the ability to locate the client through GPS giving the Informed Advisor the go-ahead on requesting financial information. Questions might include: Can I afford this? Will I be able to attain a loan? Or is this the right time to purchase the item? Figure 2 illustrates the step-by step process of attaining this information for the client, along with the roles of the financial services industry and the client.

Figure 2: Globe and GPS Locator



Note: Created for the use of this essay; Api, Financial Report, Poster of Globe and GPS Navigation Element.

The time required to attain loans for life events will be cut in half, increasing productivity in the financial services industry. An Informed Advisor will act as a personal assistant to the client assuring that no matter what comes up, there will be a solution to the problem. As this new technology takes over the financial services industry, regulations will be put in place to assure market equality among competitors. There will also need to be regulations formulated regarding the use of GPS among clients and using it to locate them. This new financial service industry procedure will make attaining loans more efficient for customers and even make it faster to gather financial information on companies. The efficiency that the finance sector gains will allow institutions to maximize their technology and continue to advance with the rest of the technological

world. This will free up advisors to give personal time to investors so they can discuss non-financial concerns as well. This will ultimately build rapport and likely strengthen the long-term relationship.

VI. Privacy Concerns

Data breaches have appeared to be ubiquitous of late – from credit card companies to the financial debacle at Target, Inc. Financial services firms can be particularly vulnerable, especially when millennials want instant access, and want it on their time frame. Solutions are varied, but one controversial but popular future move is to implement some type of facial recognition technology. Companies are currently using this information for predominately-marketing purposes, but government uses the technology to help combat terrorism.

The report, *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law,* was given to the Subcommittee on Privacy, Technology and the Law General Accountability Office (GAO) in July 2015. There are various laws now on the books, but many of these laws appear to be outdated. Many privacy advocates want more protection, but as recent breaches have proven, laws do not usually stop criminals from action. The Gramm-Leach-Bliley Act (GLBA-1999) was designed to restrict the disclosure of public information. The Fair Credit Reporting Act (1970) supposedly protects the security and confidentiality of personal information. Companies, as well as consumers, want more surveillance of criminals. Will the future allow technology to block criminals, or will privacy concerns rule the day?

The GAO report issued in the summer of 2015 considers facial recognition technology (FRT) to block unwarranted users from accessing financial services products. Although millennials may want to divulge personal information on Facebook, they have no desire to have their financial information or their money stolen. Most financial experts believe that in the future – and not that far away – it will be feasible to readily and accurately identify by name practically any individual in the world by implanting FRT. The National Telecommunications and Information Administration (NTIA), a Department of Commerce agency, is currently addressing privacy issues associated with this technology. The NTIA is including convening stakeholders to try to develop a voluntary and enforceable code of conduct for industry participants. The GAO report issued in the summer of 2015 reviews privacy issues involving FRT. This report analyzed four areas of concern: the use of FRT, privacy issues concerning commercial uses of FRT, the proposed best practices and industry privacy policies for FRT, and any privacy protections under federal law that apply to FRT. Privacy concerns are relevant, but the major recent breaches of security, including the Target, Inc. fiasco, could have been averted with the use of FRT (GAO Report, 2015).

FRT is one of many biometric technologies – eye scanning being even more effective – that identify individuals by measuring and analyzing not only physiological characteristics but also behavioral tendencies. These biometric technologies have been created to help identify people analyzing their faces, hands, eye retinas and irises, fingerprints, voice, gait, etc. Conventional identification methods, such as usernames, passwords, or special cards for entry can dupe old security systems, but various biometric technologies measure distinctions that are unique to each individual and cannot be changed easily (GAO Report, 2015).

The GAO Report lists four basic components to an effective facial recognition technology system: a camera, an algorithm to create a face print (called a facial template), databases to store images, and an algorithm to compare the image to the databases of images or a singular image in the main database. This technology is already here, but the public's concern is more with

corporations using the information, as opposed to the government implementing the technology. The Homeland Security Department of the U.S. government already requires fingerprints to procure TSA early boarding numbers for airline transportation use. When people, especially the millennials, desire safety over privacy, then this technology of the future will be implemented across the board. We personally believe that Facial Recognition Technologies, along with other biometric technologies, are here to stay, and concerns should be more about companies sharing private data. Consumers can still opt out of allowing corporations permission to share personal information. Biometric technologies are future resources, which probably will not ultimately be blocked by free but secure governments. The safety concerns in industries such as transportation and financial services are just too great (GAO Report, 2015).

VII. Conclusion

The future will see an increase in efficiency, not only with the use of technology, but also in the roles played by financial professionals. Technology will continue to adapt throughout the coming years, until we see electronic platforms and data integrated to reach maximum efficiency. This will also allow the current financial advisor's role to develop into a life-coach counseling function. Advisors will be able to meet the demand for changing client needs. Once maximum efficiency is reached in the electronic platforms and the life-coach consulting roles, the finance professional will be able to offer a more efficient and effective combination of service excellence and customer satisfaction.

The utilization of this combination will only prove sufficient for the finance industry for a finite period. As data utilization and analytics continue to evolve into a new realm, the financial industry will once again be faced with deficiencies in addressing evolving client needs. At that point, yet another solution will be necessary to continue adapting to changing technology. There is only one certainty within the technology world: it will never stop developing. Looking back at how far technology has come in the past two decades, one can only imagine where the technology world will take the financial industry, and society as a whole, in the upcoming decades.

The most difficult challenge faced in improving the cyber security of the U.S. financial industry might just be the financial industry itself. Wall Street is fond of squeezing every last ounce of usefulness out of something before discarding it and seeking an alternative. All too often, this change is ultimately forced by some type of catastrophe or crisis. In this case, it would indeed be a crisis if disaster were brought on by cyber attacks. The era of cyber warfare is about to give rise to an industry of advanced cyber security, and regardless of whether financial companies realize the seriousness of their situation before or after a calamity, someone will stand to profit greatly from it. As the venerable Sun Tzu said, "The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable."

References

Api, K. 2014. Direction, Globe, Earth. Digital image. *Icon Finder*.

Berman, Jillian. 2015. "Where Millennials Go For Financial Advice." Journal Report Wealth Management, R8. *Wall Street Journal*. http://www.wsj.com/articles/where-millennials-go-for-financial-advice-1450062181 (accessed December 14).

Booz Allen Hamilton. 2014. "Booz Allen Releases Annual Financial Services Cyber Trends For 2015." http://www.boozallen.com/media-center/press-releases/2014/11/booz-allen-releases-annual-financial-services-cyber-trends-for-2 (accessed November 19).

Camhi, Jonathan. 2014. "State Governments & the Future of Cyber Security Regulation." *Information Week, Bank Systems & Technology*. http://www.banktech.com/compliance/state-governments-and-the-future-of-cyber-security-regulation/d/d-id/1279216 (accessed July 9).

DST. 2014. "Home - DST Systems. DST Products and Services." http://www.dstsystems.com/ (accessed January 1).

Dubofsky, David, and Lyle Sussman. 2009. "The Changing Role of the Financial Planner Part 1: From Financial Analytics to Coaching and Life Planning." *Journal of Financial Planning*. 48-57. https://www.kinderinstitute.com/newsarchive-pdfs/FPA_Journal-August_2009-The_1.pdf (accessed August) and "The Changing Role of the Financial Planner Part 2: Prescriptions for Coaching and Life Planning." *Journal of Financial Planning*. 50-6. https://www.kinderinstitute.com/newsarchive-pdfs/FPA_Journal-September_2009-The_2-Prescriptions%20for_Coaching_and_Life_Plan.pdf (accessed November 4, 2014).

Government Accountability Office. 2015. *Facial Recognition Technology: Commercial Uses, Privacy Issues and Applicable Federal Law*. Report to the Ranking Member, Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, U.S. Senate GAO-15-621. Washington, DC. http://www.gao.gov/products/GAO-15-621 (accessed July).

Independent Community Bankers of America Report. 2014. www.icba.org (accessed June 6).

KAW. 2014. "A New Era in Banking: The Future of Financial Services." *Knowledge @Wharton Where the Financial Services Industry Goes from Here Comments*. Wharton University (accessed September 5).

Lynch, Matt. 2013. "The Financial Services Industry in 2030." *Wealth Management*. http://wealthmanagement.com/viewpoints/financial-services-industry-2030 (accessed October 21).

Millman, Gregory. 2014. "Venture Capitalist Ted Schlein on the Future of Cybersecurity." *Risk and Compliance Journal, Wall Street Journal* (accessed November 14).

New York State Department of Financial Services. 2014. "Report on Cyber Security in the Banking Sector." http://www.dfs.ny.gov/about/press2014/pr140505_cyber_security.pdf (accessed May).

Norse. 2015. IPViking live updates. http://map.ipviking.com/ (accessed June).

Poster of Globe and GPS Navigation Element. 2014. Digital image. *FotoSearch*. Publitek Inc. (accessed December 10).

Roose, Kevin. 2014. "Is Silicon Valley the Future of Finance?" *New York News and Politics. Daily Intelligencer* (accessed November 20).

Sun, Tzu. 2010. *The Art of War.* Lightning Source Inc.

Tergesen, Anne. 2015. "Automated 'Robo' Adviser Lowers Investing Minimum." *Wall Street Journal*. http://www.wsj.com/articles/automated-robo-adviser-lowers-its-investment-minimum-1447855380 (accessed November 21).

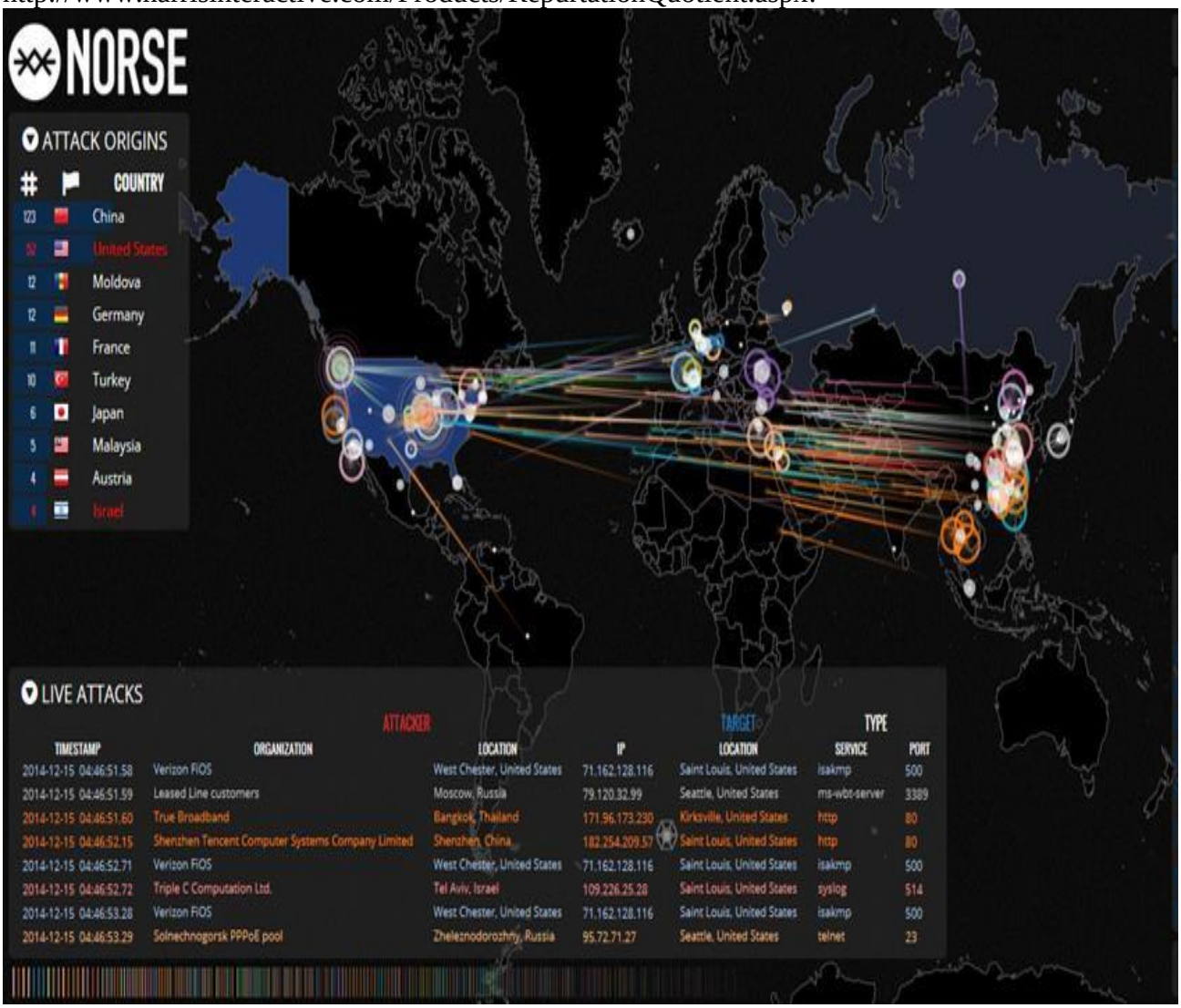
U.S. Bureau of Labor Statistics. (accessed October 21, 2014).

Walters, Riley. 2014. "Cyber Attacks on U.S. Companies in 2014." The Heritage Foundation (accessed October 27).

Wladawsky-Berger, Irving. 2015. "Measuring Technology's Impact on the Evolution of Financial Services." CIO Journal-The DIO Report, *Wall Street Journal Blogs*. http://blogs.wsj.com/cio/2015/06/26/measuring-technologys-impact-on-the-evolution-of-financial-services/ (accessed June 26).

Appendix A

The Harris Poll Reputation Quotient® (RQ®)
Harris partners with clients to provide insight into their public reputation, brand perception and consumer image. For more information visit:
http://www.harrisinteractive.com/Products/RepurtationQuotient.aspx.



Norse – IPViking conducts a global network of millions of sensors that are specifically built for being attacked. When sensors are hacked, those threats are followed back to the source, and the information is displayed in real time. This snapshot of a mere second gives some insight into the mass scale on which cyber-attacks take place. For live updates visit: http://map.ipviding.com/.