FRAUD AND PRIVACY VIOLATION RISKS IN THE FINANCIAL AGGREGATION INDUSTRY: THE CASE OF REGULATION

Anastassios Gentzoglanis, PhD
University of Sherbrooke, Canada
Dr. Avner Levin
Associate Professor and Director, Privacy and Cyber Crime Institute
Ryerson University

Abstract

The financial aggregation industry is on the rise again. After having experienced high growth rates during the pre-financial crisis of 2007-2008, the industry has undergone significant changes in terms of structure, behavior and performance. Plagued by lack of trust on behalf of the customers and under the pressure of changing technologies and in the absence of a regulatory framework, new entrants had difficulties in penetrating the market the way have originally anticipated. In the meantime, banks and other financial institutions refined their strategies and consolidated their positions in the new emerging industry. To survive, many early entrants developed new strategies and became suppliers of technology to the banks and other financial institutions. This study uses the SCP paradigm to analyze the emerging financial aggregation industry and the attitudes young customers have toward these services. The results show that customers are seriously concerned with the risks of violation of privacy and fraud associated with aggregation activity online and they are ready to pay a prime to get a more secure service. Nonetheless, regulating of the aggregation industry on the ground of these risks is premature. Yet, the existing regulatory agencies should increase awarness concerning the looming risks and provide incentives to financial aggregators to adopt technologies and operational strategies that minimize the potential for fraudelent behavior online.

Keywords: Financial Aggregation, Disruptive Technologies, Regulation, Fraud, Privacy, Competitive Strategies

Introduction

Financial aggregation is on the rise again. A growing number of new personal finance and non-finance sites combine many new technological features and ingenuity to provide account aggregation services and novel financial management tools to an ever-increasing number of individuals interested in completing their financial transactions and financial planning online.

Financial aggregators are financial service firms – either banks or non-banks, which collect data online, group them together and present them to customers within a single application interface. The financial aggregation industry originated in the US – Mint and Yodlee are the most well-known world-wide – but it has expanded rapidly and conquered foreign markets in Europe (UK, France), Asia (Japan and South Korea) and Canada (ASIC, 2001). The international divisions of financial aggregators are not fully-fledged yet, but they are expanding quickly as a result of increasing competition from traditional financial service firms and newcomers.

The approach to aggregating financial services is rather novel and so much so the issues emerging from this. On the one hand, this innovation is quite interesting and responds to ever-increasing needs of individuals who desire to group their financial and utility accounts. Dealing with all the accounts is not only tedious (remembering and frequently updating user names and passwords, responding to soliciting advertisement and surveys, etc.) but also time consuming. Individuals who monitor multiple accounts waste their time, i.e., they do it at the expense of leisure. Financial aggregation not only does reduce search costs (costs of monitoring and tracking specific accounts) but also frees time of busy individuals who could make better use of it and increase their wellbeing.

On the other hand, financial aggregation may cause some inconveniences and even create serious problems. Security risk and violation of privacy are some of them. For instance, while a user is online on a non-bank personal finance site, his or her personal information is used in order to get access to the service. Usually this information is encrypted and thus protected. But this simple method of authentication, the so-called single-factor authentication (the mere use of a username and password) is notoriously known for its vulnerability to phishing and fraud. *Malware and other intrusive programs are widely used by fraudsters to extract funds or perform other fraudulent activities under a user's name while the latter is using aggregation services online.* Contrary to the nonbank financial aggregators, banks and other heavily regulated financial institutions normally use a technology that requires the use of a multifactor authentication method and aggressive consumer education with respect to security and privacy (Albrechtslund, 2008).

The growth of the financial aggregation industry depends on the success of these and other innovative services offered to consumers. But the questions related to privacy and the issues of identity theft, fraud and misuse may hamper its growth potential. Nowadays, these problems are getting exacerbated by the ever-increasing use of *cloud computing and storage.* For instance, personal data may be stored in the cloud and used by fraudulent individuals around the globe increasing thereby the risks of fraud and violation of privacy. As the industry grows, these risks may increase and this is the reason why many regulatory authorities warn consumers about the potential problems. For instance, the Financial Consumer Agency of Canada (FCAC) has issued a warning as to the possible threats financial aggregation may present to Canadian consumers (FCAC, **2011**).

This research explores the privacy, fraud and potential online financial risks and security issues arising from the increasing use of account aggregation services offered by a growing number of nonbank and bank aggregators. It uses a modified version of the so-called structure-conduct-performance (SCP) paradigm in order to identify the main issues to be investigated and analyze them in detail with the objective to understand thoroughly the structure of this industry, the conduct of financial aggregators and their respective performance. Conduct is crucial because it implies strategies and the latter have a definite impact on industry performance. To use strategies, firms need to understand customers' behavior, particularly those who use the financial aggregation services online.

Section II of the paper presents the analytical framework and justifies its importance to the current work. Section III examines the technologies used by the financial aggregators and the strategies used by them to collect data and understand the behavior of individuals using these services online. It also makes a literature review of the key finding on the subject. Section IV presents the results of the study and compares them to the literature. Lastly Section V concludes and offers policy recommendations.

Methodology

There are various frameworks that can be used to analyze the financial aggregation industry. The most important of them are presented in table 1 below. Porter's five forces

model, Ansoff's matrix, BCG (Boston Consulting Group) growth-share matrix and the SWOT model do recognize the importance of competition *within* and *for* the industry and the development of strategies which would give a competitive edge to incumbents. Each model explores the most appropriate strategies to be developed by incumbents to either penetrate new markets or make the current competitive environment less intense. Despite their similarities, they do have significant differences chiefly with respect to the key elements each model uses to establish relationships and appropriate strategies. For instance, Porter's five forces model emphasizes the importance of recognizing the relative competitive position of each firm in the industry and develop strategies that would maintain each firm's competitive advantage. Ansoff's matrix and the SWOT models are similar too in some respects since both of them are based on the development of corporate growth strategies after making a thorough evaluation of different alternatives in terms of existing and/or new products and markets.

Unfortunately, both models fail to take into account the dynamic interaction of different players within and outside a particular industry and develop strategies in terms of product and technology advancements. Further, key stakeholders who actively intervene in the process of strategy development are ignored such as the government, regulators and competitors from abroad. Bain's SCP paradigm is broader and encompasses all previous models. It also goes a step further by taking into account *potential competition* and the strategies that may be used by entrants and incumbents. Using a game theoretic approach, Bain's model is widely used to explain the dynamics of competition in existing and new or emerging industries. In its modified version, Bain's model takes also into account government policies and the influence regulation has on industry's structure and performance. Given that the financial aggregation industry is currently characterized by intense competition arising from the traditional banking industry and new aggregators, the SCP paradigm is used in this paper to analyze this industry and examine whether regulation is an appropriate policy option.

Table 1Comparison of various analytical frameworks and the modified version of SCP paradigm

Models	Competition in-muro	Competition ex-muro	Static strategies	Dynamic strategies
Porter's model	X	X	X	
Asnoff's matrix	X	X	X	
BCG growth-share matrix	X			
SWOT model	X	X	X	
SCP paradigm	X	X	X	X

Source: Author's conception

The modified version of the SCP paradigm makes the role of each decision maker within the company (operations research, marketing, production and engineering, accounting, market and regulators, etc.) more explicit. It also takes into account the industry's broader business environment (elasticity of demand, unionization, technology, product and customer attributes, etc.) and shows the dynamic interplay among all stakeholders.

Also, the modified version is more appropriate than the traditional SCP paradigm. The latter, in its basic form, establishes a link between structure, conduct and performance. It is based on sound economic theory – the Cournot model – which shows that the more concentrated an industry is the higher the monopoly power of the incumbents and lesser the competition in the industry. Thus, structure (number and size of firms in the industry, economies of scale, etc.) affects the conduct of individual firms (pricing, R&D, M&A, collusion, etc.) and performance measured by profitability, allocative and dynamic efficiencies and price-cost margins. There may be feedback effects among the three basic elements and government policies are driven by performance.

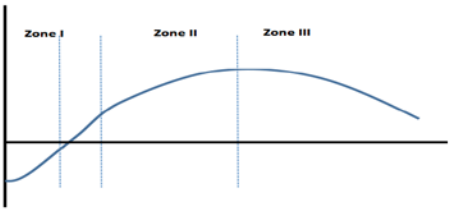
Thus in this study performance is measured by indices constructed using data generated through a questionnaire distributed in Canada. Questions were asked related to fraud, privacy violation, theft identity and the degree of security that prevails in this industry and its dynamics. The results are used to analyze the desirability of government intervention and regulation of this industry.

Technological Changes and Customer Behavior in Financial Aggregation Industry: A Review of the literature

Technological changes dramatically affect the structure of an industry, the behavior of existing firms and potential entrants and the whole performance of an industrial sector. These effects are even starker when technological changes are disruptive and not evolutionary. The latter allow firms to adjust themselves and provide them sufficient time to adopt strategies that would increase their competitiveness. The former are more sweeping and generally not very well understood by incumbents, at least at the initial stages of their appearance. They are normally introduced by start-ups and small-sized firms, capable of creating niche markets and even penetrating the well-established ones dominated by large-sized incumbents. As new entrants enter the industry competition intensifies by the introduction of entirely new and similar services to the ones of incumbent. Normally, new entrants are facing less regulation and other institutional constraints as government and regulatory organizations are slow to react, given their limited technological knowledge. This asymmetry in information and technological competence plays at the benefit of new entrants. The latter have the so-called "first-mover advantage" which may make new entrants major players in the industry.

However, incumbents are not powerless. They would first call for an even-leveled competitive field by asking for a tougher regulation and entry barriers. Unable to react rapidly, given their sheer size and their long-lived experience functioning in a rather stable and well-defined business, incumbents would even raise issues of security and increase users' awareness concerning the dangers that exist in switching providers and in trusting their newly created businesses. This is precisely what happens in the financial aggregation industry. The current technologies used by new entrants to provide aggregation services are indeed disruptive and far-reaching. Incumbents, large banks and other financial institutions launch a far-cry to customers alerting them that they are no longer obligated to offer protection of their accounts should customers give their PINs and other sensitive information to third party providers. Such an attitude is legitimate and by all means justifiable but as long as incumbents do not offer the aggregation service and this is a need not satisfied by incumbents, customers would, nonetheless, use the service offered by new entrants (Edge and Sampaio, 2009). So at the early stages, when technology is mastered by new entrants only and the financial aggregation service is offered exclusively by them, customers with high reservation prices – the ones who value the service most – would be willing to use the service anyway. At the outset, there is an erosion of incumbents' market shares but negligible. As entrants become firmly entrenched and expand the gamut of their services, incumbents' market shares are threatened further and their strategies to thwart entry and expansion of newcomers are intensified. The competition process may continue as long as no new regulation is introduced to stop the growth of new entrants and determine the fair play. This life cycle of competition may be stylized and illustrated by the following familiar graph.

Figure 1Life cycle of competition introduced by technological changes and innovation in the financial aggregation industry



The Canadian financial aggregation industry is neither mature in terms of competition nor fully competitive yet. It is situated in Zone I. From a technological point of view the Canadian industry is, at least with respect to innovation, at its early stages. For instance, mobile banking, the most rapidly developing market segment is still under development. For instance, according to *The Pollara online survey (August 2013),* 70% of those who own a mobile device use mobile applications for completing their financial transactions. (http://newsroom.bmo.com/press-releases/bmo-mobile-banking-survey-70-per-cent-of-canadian-tsx-bmo-201309170898511001). CIBC is the first Canadian bank to adopt the electronic deposit while TD is about to introduce this application soon. This strategy would help the banking industry to diversify itself and diminish the intensity of competition that arises from the arrival of financial aggregators over the internet (Fujii et al., 2012).

Indeed, competition over the internet is now a reality. Financial and non-financial firms use various technologies to collect data and other sensitive information to study their customers' behavior and get a competitive edge over their rivals. Indeed, the Internet has created a paradigm shift in almost any type of businesses and is forcingtraditional financial institutions to transform themselves at a rapid pace and at an unprecedented scale.

In Canada there are seven account aggregators, subsidiaries of foreign aggregators all of them established between 1999 and 2007. Canadian banks do not allow financial aggregators to have access to their customers' accounts and refuse to share their customers' financial information. In case of fraud, Canadians banks are not obliged to refund their customers since the customers are responsible for giving sensitive information to financial aggregators.

Competition is high between these seven account aggregators and well-established Canadian banks, although the services offered are not exactly the same. The Canadian banks offer personal finance, budgeting and banking savings services for the accounts a customer has in a specific bank. By contrast, financial aggregators, like Mint Canada, give customers a total visibility of what is happening in the customers' accounts irrespectively where these accounts reside – in TD, RBC, BMO, HSBC, etc. Customers can see what is happening with their accounts at any moment of the day online or with mobile applications (Mearian, 2001).

The security concerns are very important in this industry. Customers are mainly concerned because financial aggregators may use their personal information for purposes other than the ones for which this information has been initially provided. Further, there are risks for identity theft and malwares from unscrupulous individuals who search the internet to get information and commit frauds. Both types of risks are real and they cannot be eliminated. But the probability of their occurrence may be reduced if financial aggregators invest in advanced technologies and apply a vigorous privacy policy and develop monitoring and internal control mechanisms that safeguard safety.

It is notoriously known that financial aggregators use "cookies" – a text file that resides on a customer's computer while online – to provide financial information online. There are two types of cookies, persistent and per-session cookies. A persistent cookie is used by financial aggregators to provide usage information on specific functions residing in provider's online banking application. Normally, there is no customer related information

associated with this type of cookies. A per-session cookie is stored temporarily in customer's PC temporary memory (RAM) and assigns an ID per session whenever a customer logs on the site. This cookie is important to validate a customer's device (PC, tablet, or smart phone) and allow customers to complete their online transactions. As for the persistent cookies, the per-session cookies do not contain any customer-related information. Cookies are site specific and only a single aggregation provider can access, decode and make use of the information.

Online banking has become widespread and still growing. Pew Research Center, Federal Reserve (2014) defines "online banking or Internet banking or e-banking "the use of a web site that allows" customers of a financial institution to conduct financial transactions on a secured website operated by the institution, which can be a retail bank, virtual bank, credit union or building society". Recent statistics by Pew Research Center, Federal Reserve (2014) indicates that 69 million of Americans transact online while 56% of them pay a bill online. Table 2 gives some key summary statistics about the attitudes Americans have towards mobile banking.

Table 2Online banking statistics and customers' attitudes

Online / Mobile Banking Statistics	**Data**
Percent of those who managed household finances who banked online at least once in the past 12 months	81 %
Percent of people who used mobile phone banking within the past 12 months	19 %
Number of Americans who bank online	69 M
Online banking customer satisfaction	78 %
Percent of consumers who receive electronic checking account statements	42 %
Percent of consumers who paid a bill online through their bank in the past month	56 %
Statistics on Mobile Banking Users	**Percent**
Using your mobile phone, have you done any of the following in the past 12 months?	
Checked an account balance or recent transaction	90 %
Downloaded your bank's mobile banking application	48 %
Transferred money between two accounts	42 %
Received a text message alert from your bank	33 %
Made a bill payment using your bank's website or application	26 %
Located the closest in-network ATM for you bank	21 %
Deposited a check to your account using your phone's camera	11 %
Statistics on Non Mobile Banking Users	**Percent**
What are the main reasons you have decided not to use mobile banking?	
My banking needs are being met without mobile banking	57 %
I'm concerned about the security of mobile banking	48 %
I don't trust the technology to properly process my banking transactions	22 %
The cost of data access on my wireless plan is too high	18 %
It is too difficult to see on my mobile phone's screen	17 %
It's difficult and time consuming to set up mobile banking	10 %

Source: Pew Research Center, Federal Reserve (January 1, 2014) http://www.statisticbrain.com/online-mobile-banking-statistics/

Canadian account aggregators make use of cookies and advanced encryption technologies to provide their financial aggregation services. Less than half of financial aggregators offer services using a better technology than the 128-bit SSL technology. There are therefore risks for fraud and breach of security in the financial sector of Canada (Gross and Acquisti, 2005, Kirkpatrick, 2010, Korff, 2008). Canadian financial aggregators have to adopt stringent encryption technologies to offer their services securely and inspire more confidence to users. Unless such measures become more concrete and visible, customers would not use the financial aggregation services heartedly (Langlois et al. 2009).

Data and Main Findings of the Study

There is no publicly available data for the financial aggregation industry in Canada or elsewhere, particularly with respect to market shares, pricing policies, profit margins,

technologies used to detect malwares, fraud, security threats and violation of privacy. Secondary data were obtained from the internet and the scant literature that exists on the subject (Ontario, 2010). Nonetheless, these data are not enough to examine the behavior and attitudes customers have while making their financial transactions online using financial aggregators like Mint, Savvy Money, PocketSmith, MVelopes, Check.me, iBank, and Yodlee.

For this purpose we have developed a questionnaire which was distributed in both official languages (English and French) in two Canadian provinces, Ontario and Quebec. A number of questions were asked to elicit information with respect to the use and knowledge Canadians have of the financial aggregation industry and their concerns about privacy, fraud and security issues.

The questionnaire was divided into four parts. The first concerned questions related to the use of financial aggregation services and the awareness of users about the existence and the type of aggregation services offered in Canada. The second deals with questions related to how users perceive financial aggregator firms in Canada and what type of platforms or devices they use to access these services. The third part concerned questions related to privacy, identity theft, fraud, and issues of security. Questions concerning their willingness to pay to safeguard the offer of secure services were also included in this part of the questionnaire. Finally, the fourth part concerned questions with respect to their socio-economic and demographic characteristics. In total, we got 255 responses (110 from the province of Quebec and 145 from Ontario). Summary statistics concerning responders' gender, age group, annual income and highest degree are indicated in the table 3 below.

Table 3Responders' Summary Statistics

Responders' gender		
	Quebec (%)	Ontario (%)
Male	63%	37%
Female	37%	63%
Responders' age group		
20-29 years old	80%	22%
30-39 years old	16	21
40-49 years old	3	25
Over 50	1%	32%
Responders' annual income		
<$19,999	72	6
$20,000-$39,999	16	91
$40,000-$59,999	3	19
$60,000-$79,000	6	18
$80,000-$99,999	2	16
$100,000>	0	19
I'd rather not say	0	14
Responders' highest degree		
High school diploma	1	4
College diploma	23	7
University diploma (Undergraduate - Bachelor's degree)	54	35
University diploma (Graduate - Master's degree)	18	37
University diploma (Postgraduate - Doctorate)	3	17

Source: Author's data

A first glance at the summary statistics indicates that there are important differences between responders residing in Quebec and Ontario. The Quebec sample is mostly composed by males while the opposite is true for the responders from Ontario. Quebec responders are mostly young professionals with a bachelor's degree while the Ontarians are mostly middle-aged with a majority of them holding a master's degree. As far as the income is concerned, Quebecers are in the lower income bracket while the responders from Ontario belong to the next upper income bracket. The statistical analysis of these two samples is done in Gentzoglanis and Levin, 2014).

The answers to the questions related to responders' knowledge concerning the existence of the financial aggregation services in Canada show that the majority, more than 37%, had a very good knowledge and uses frequently these services, while more than 28% had some idea about their existence and use them occasionally.

As far as privacy policy and security issues are concerned, 21% of Quebecers answered that they do read the privacy policy of financial aggregators before making any transactions while this percentage is much higher for the responders from Ontario (37% of Ontarians). Thus, 1 out of 5 Quebecers and 2 out of 5 Ontarians do read the financial aggregators' privacy policy. These documents are many pages long and use a jurist language which makes them difficult to understand. The high percentage of users who read an aggregator's privacy policy shows that users of financial aggregation services are seriously concerned about privacy.

This finding is consistent with the answer users give to the questions concerning their level of concern about identity theft and fraud when they make financial transactions on different platforms or devices. The results show that 93 % of Quebecers are concerned and 86% of Ontarians are highly concerned. Given this overwhelming concern of users about privacy and risks of fraud, financial aggregation service companies should be very careful when they use marketing tools to promote their services. Their marketing strategy should emphasize the safety characteristics of their technologies to preserving privacy and thwarting fraud.

These high levels of concern are reflected as well in the answers they gave to the questions concerning their willingness to make transactions with well-established financial aggregators as opposed to the newcomers which in many instances are virtual. Thus 35% of Quebecers and 41% of Ontarians are willing to deal solely with aggregators having a physical presence in the market (as opposed to virtual ones) although both state that they prefer the firms having an explicit privacy policy in addition to having brick and mortar presence. Thus it is important for financial aggregators to have an explicit policy on privacy and a record of integrity should they want to attract new customers. By and large, established financial aggregators and banks with long history of presence in the market have a competitive advantage compared to newcomers less well-established financial aggregators.

As far as the results are concerned with respect of the use of encryption technologies and the level of trust customers have towards these technologies, Quebecers are more trustful than Ontarians (55% versus a meager 14%). It is obvious that financial aggregators must make considerable efforts to increase their reputation and confidence among actual and potential users. The industry's survival and growth depends on its capacity to use the most advanced encryption technologies that inspire confidence to users.

Trust in financial aggregators is an important element for growth in a nascent industry (Boyd and Hargittai, 2010). Quebecers (42% of responders) declare that they trust their financial aggregators because of good reputation (26%) and the absence of any problems associated with security issues, while this percentage is only 26% among Ontarian responders. Nonetheless, 43% of the latter say that they have never had problems with their financial aggregators as far as security, privacy and fraud issues are concerned. Reputation is thus important for Quebecers while the absence of problems is more important for Ontarians. It is possible to surmise that customers trust their financial aggregators using tangible criteria like absence of violation of privacy and security problems. Financial aggregators should build on these findings.

Knowing customers' online behavior, particularly the frequency with which they consult their accounts and make transactions, is important because financial aggregators may target their customers according to the type of transactions, their duration and frequency. Their profitability depends, to a great extent, on knowing well their customers' online

behavior (Steeves et al., 2010). Every financial aggregator uses cookies, persistent and non-persistent for marketing but also for safety purposes. This provides opportunities for increasing market shares and returns on investment. Most of the responders (52% in Quebec and 45% in Ontario) complete their transactions once every two weeks and 24% in Quebec and 34% in Ontario once per day.

Given the changing nature of technology and the fact that mobile banking is increasingly becoming the new standard in this industry, knowing the platforms or devices used by customers to complete their financial aggregation services is becoming important for aggregation providers. The latter must make investments in infrastructure to make their interfaces compatible with the platforms or devices customers use to access the services. It appears that Canadians in Quebec and Ontario use laptops, desktop computers, tablets and smart phones to access the aggregation service providers. Notwithstanding, 63% in Quebec and 39% in Ontario declare that the laptops are the most frequently used platform or devise to make their financial transactions but Ontarians trust more their desktop computer (32% compared to 17% of Quebecers).

As far as the change in attitude is concerned in the use of a particular platform because of privacy or security issues, 72% of Quebecers report that they have not changed attitude at all while this percentage is only 56% for Ontarians. Furthermore, about equal percent of Quebecers and Ontarians (95% and 92% respectively) declare that they have never had to change bank, financial institution or financial aggregators because of their concern about the protection of personal data.

Patronage for financial aggregators with explicit privacy policy is praised by both groups of responders (79% of Ontarians and 49% of Quebecers) even if their services are less attractive than the ones offered by financial aggregators *without* explicit privacy policies. This illustrates that an explicit and well-articulated privacy policy is a requirement for patronage even if most of customers won't read it, as it was indicated above.

Fraud, theft of identity and online security are serious concerns for all customers (Warren and Brandeis, 1980). If the latter wanted to reduce the probabilities of occurrence, they may be willing to pay a fee to aggregation service providers to get the warranty that these risks would be reduced to the minimum. The answers to the question “How much each respondent is willing to pay to have the warranty that the service would be provided almost risk free” vary dramatically between the two groups. A large majority of Quebecers (63%) is willing to pay a “prime” up to $10 per month to be assured that financial services are offered with high security. This percentage drops to only 37% for Ontarians. This difference in behavior may be explained by hypothesizing that Quebecers are either more risk-averse or Ontarians believe that their data are well protected and there is no need to pay an additional fee (insurance) for that.

Table 4Summary of the main findings

	Believes and attitudes online	Groups distinguished by language	
		English	French
Trust in encryption technology	Strongly	77	55
	Fairly	6	7
Read privacy policy	Yes	54	18
	Never	40	78
Level of concern	Very	46	61
	Fairly	45	29
Change in attitudes	Yes	39	25
	No	57	72
Platform choice	Laptop/smart/tablet	36	69
	Desktop	41	17
Virtual vs bricks and mortar	Virtual with privacy	73	49
	Bricks and mortar without privacy	16	36
Willingness to pay	$0	55	25

Source: Author's data

All in all, the financial aggregation industry is growing but there are some stumbling blocks to its growth. Data protection, privacy, security and fraud issues are some serious concerns users have which may inhibit or at least retard future growth (Gentzoglanis, 2010). Financial aggregation service providers should acknowledge customers' concerns and attitudes and adopt new technologies and strategies that would increase safety and establish a good reputation for the industry. This is particularly important at every stage of development of any industry but more important so for the financial aggregation industry which is at its infancy (Sans Institute, 2004). Given the newness of the industry and the low rate of incidences related to privacy violation and fraud, regulation may not be necessary. Regulation as a prevention mechanism would not contribute to making the industry safer and therefore no such mechanism is required at this time. Even if there are some real and potential problems related to privacy and security, nonetheless, the introducing of new regulations before the industry fully develops is premature. Table 3 summarizes the main findings.

Conclusion

In the early 2000s, account aggregation was fast becoming a basic expectation of banking customers, and companies were racing to install the technology that would allow them to reach millions of new customers. Only very few were able to hold their ground against the systems. Unfortunately, these predictions were wrong and in the aftermath of dot com bubble most of them went bankrupt. Once again, the survivors have been harshly hit chiefly because of the recent financial crisis. After these two major shocks, the financial aggregation industry is on the rise again. This time, the technologies are better known and the internet has become more widespread and better understood by service providers and customers alike. The account aggregation industry has started all over again but this time it is based on solid ground.

The analysis of data indicates that Canadians are seriously concerned by the problems of privacy violation and fraud while when they are using aggregation services online. Convenience of service outweighs the inconveniences caused by these threats but the risks remain high and customers are willing to pay a high prime to get a more secure aggregation service. As far as the issue of regulation is concerned, the study concludes that (1) the financial aggregation industry be allowed to exercise its potential free of new regulations and (2) regulators continue to monitor the industry and alert users with respect to the potential problems associated with privacy, theft identity and malware intrusions while completing their transactions online. It is argued that the existing regulatory framework is adequate to exercise some discipline in the market. The current anti-spam legislation (CASL Bill C-28 to be in effect from July 1st 2014) banns unsolicited electronic messages such as emails and texts, and although is meant to crack down on unwanted spam and to protect customers from harassment, identity theft, spyware and fraud, it would also contribute to limiting the use of persistent cookies by financial aggregators for marketing and related purposes not associated with the financial aggregation services – for instance, the use of personal information by other divisions of financial aggregators to sell products like insurance and/or financial products.

Acknowledgement:

This research received funding support through the Office of the Privacy Commissioner of Canada's Contributions Program. The opinions expressed in the paper are those of the author and do not necessarily reflect those of the Office of the Privacy Commissioner of Canada

References:

ASIC, Australian Securities and Investment Commission (2001). Account aggregation in the financial services sector, Consultation Paper 20, May. http://www.asic.gov.au/cp

Albrechtslund, A. (2008). Online Social Networking as Participatory Surveillance. *First Monday*, *13*(3). Retrieved from http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2142/1949

Bigge, R. (2006). The cost of (anti-)social networks: Identity, agency and neo-luddites. *First Monday*, *11*(12). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1421/1339

Boyd, D., and Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, *15*(8). Retrieved from http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589

Edge M. E and P. R. Sampaio (2009).A survey of signature based methods for financial fraud detection, *Computers & Security28(6):381-394 (2009).*

FCAC (The Financial Consumer Agency of Canada), "Financial Aggregation Services: Risk of disclosing online banking information"March 10, 2011**).** http://www.fcac-acfc.gc.ca/eng/about/news/pages/ConsPress-ConsPresse-0.aspx?itemid=32

Fujii, H., T. Okano, S. Madnick and M. Siegel (2012). E-Aggregation: The Present and Future of Online Financial Services in Asia-Pacific, Sloan School of Management, Massachusetts Institute of Technology, Cambridge, MA 02139.

Gentzoglanis, A. (2010). "Risk and Regulatory Reforms in the Securities Industry: A Need for a Paradigm Shift?", in the *International Journal of Financial Markets and Derivatives (IJFMD), Vol. 1, N0 4.*

Gross, R., and Acquisti, A. (2005). *Information Revelation and Privacy in Online Social Networks (The Facebook case)*. Proceedings from ACM Workshop on Privacy and the Electronic Society (WPES), 2005, Alexandria, Virginia.

Kirkpatrick, D. (2010). *The Facebook Effect: The Inside Story of the Company That Is Connecting the World.* New York: Simon & Schuster.

Korff, D. (2008). The difficulties in Meeting the Challenges Posed by Global Social and Technical Developments, London Metropolitan University, European Commission Comparative Study, Working paper, N0. 2.

Pew Research Center, Federal Reserve (January 1, 2014) http://www.statisticbrain.com/online-mobile-banking-statistics/

Langlois, G., Elmer, G., McKelvey, F., and Devereaux, Z. (2009). Networked Publics: The Double Articulation of Code and Politics on Facebook. *Canadian Journal of Communication*, *34*(3). Retrieved from http://www.cjc-online.ca/index.php/journal/article/viewArticle/2114

Mearian, L. (2001), "Banks See Online Account Aggregation as Necessary Evil", http://www.telegraph.co.uk/finance/personalfinance/2732394/Citibank-My-Accounts.html

Ontario, Ministry of Economic Development and Trade, (2010). E-Commerce: Purchasing and Selling Online – What You Need to Consider, Ontario, Queen's Printer for Ontario.

Sans Institute (2004). Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth. Retrieved from https://www.sans.org/reading-room/whitepapers/detection/understanding-ips-ids-ips-ids-defense-in-depth-1381

Steeves, V., Milford, T., and Butts, A. (2010). Summary of Research on Youth Online Privacy. *The Office of the Privacy Commissioner of Canada*.

Warren, S. D., and Brandeis, L. D. (1980). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220. Retrieved from http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html