The Risk to Client's Financial Data:

TURNING RISK INTO OPPORTUNITY

AUTHORS:
Brian O'Donnell, Chief Data Officer, IISAAC Inc.
Richard Nesbitt, CEO, Global Risk Institute

If you watched the recent US Senate hearings attended by Facebook CEO Mark Zuckerberg, you may have noted this response by Senator Tester to the assertion that Facebook clients owned the data provided by its subscribers.

> *"You said multiple times during this hearing that I own the data. … That sounds good, but in practice you're making $40 billion a year. I'm not making money on it. It feels like you own the data."* [1]

So, who does own the data? Is it the client who provides the data in the ordinary use of the service or does it become owned by the service firm once you have agreed to their terms of use? Over the past few years terms like Fintech, Big Data, Artificial Intelligence and Machine Learning have received significant attention. The primary focus of that attention has been on how Financial Institutions, and all industries really, can understand their clients better and drive increasing sales and client satisfaction by gathering and analyzing customer data. Financial Institutions have embraced digitized, omni-channel client strategies, developing the technology to allow clients to bank and transact anywhere and any time they choose.

The Global Risk Institute and others have also devoted significant attention to digital innovation and the increasing volume and sophistication of the accompanying cyber risks. The financial service industry in general, and indeed Canada as a whole, needs to better manage this ever-increasing opportunity and risk.

But Facebook's Cambridge Analytica scandal opens a new window on the issues of data ownership, data privacy and the potential abuses of an individual's data. Out of this scandal we believe a new opportunity presents itself for the financial industry in general, and banks in particular. We believe banks could become instrumental in helping their clients collect, protect and monetize a "personal data account". The client's data repository would allow clients to assert their ownership rights over their data, including allowing clients to monetize their data (for themselves, as opposed to the social media industry).

> *"We are all digital labourers, helping make possible the fortunes generated by firms like Google and Facebook…. If the economy is to function properly in the future—and if a crisis of technological unemployment is to be avoided—we must take account of this and change the relationship between big internet companies and their users."* [2]

We believe there is significant value individuals could realize (some estimate $500 - $1,000 per year) by taking control of their data, while also significantly enhancing their personal cyber security. Financial Institutions ("F.I.") who help their clients assert this data ownership and realize the benefits will drive a new and valuable relationship with these clients.

In a recent GRI published article on Open Banking, the authors cited the natural advantages that banks possess in their current relationship with their customers:

1 *Sen. Jon Tester to Mark Zuckerberg, CNN, April 10, 2018*

2 *The Digital Proletariat: "Should internet firms pay for the data users currently give away?", The Economist (Jan 11, 2018)*

"Banks have certain competitive advantages over their competitors within and outsidethe financial services sector. Firstly, regulatory compliance (such as regulatory reporting, anti-money laundering, and "know-your-customer", etc.) is often a complex and difficult task that banks know how to do well, and other firms are not likely to want to compete on. This is mostly because it would be expensive to build the infrastructure (e.g. establish processes, develop systems, cultivate relationships with regulators, etc.) and run such services for a small portion of financial products.

An additional advantage of banks over other platforms and Fintech's is the trust that the customers have in them in handling money securely. An industry analyst describes this advantage as one that "banks are seen still as the safest and most trusted place for people's money to be". In this context, he adds, "getting a third party established to take some of that market away, will be difficult."[3]

The existence of trust between the F.I. and the customer is the foundation of the relationship. The trusted relationship extends directly into the data held on the customers behalf. The concept of selling this data has not traditionally been a consideration for financial services. However today non-traditional suppliers routinely make this data available to others for a fee or other benefit.

"When a consumer can simply sell their data, there is no doubt about which bytes belong to whom, and the resulting picture can be incredibly rich: not a website visits tentatively paired with a Facebook like, but an actual, "completely deterministic" web of purchases, browsing patterns and social media activity"[4]

The proliferation of social media apps has come with a number of risks and drawbacks for all users, including a bank's retail customers. Chief amongst these risks are data breaches and identity theft. While banks have spent decades hardening their networks, enhancing personal protocols and widening the encryption of client data, many industries have lagged these advances. The social media industry takes the issue one step further and proactively sells and monetizes user data as a key component of their business model.

"Access to and control of user data could make [firms like Google's parent Alphabet, Amazon, Apple, Facebook and Microsoft] unassailable… they can easily drive out competition by combining their scale with innovative use of data to anticipate and meet evolving customer needs at a lower price, and sometimes for free"[5]

Data is either sold into the data broker market (a $200bn a year industry), or monetized through analysis to drive marketing insights such as:

- What do clients like?
- What will they want to buy next?
- How do they like to buy things? How price sensitive are they?
- How susceptible to network impacts are they (i.e. do their family and friends significantly impact their shopping behaviours)?

3 *Zachariadis, M and Ozcan, P, "The API Economy and Digital Transformation in Financial Services: The Case for Open Banking", Global Risk Institute and Swift Institute, (April 2018) p. 17*

4 *David Floyd, "Blockchain Could Make You – Not Equifax – the Owner of Your Data", Investopedia (Feb 2018)*

5 *Barrie McKenna, "Bank of Canada warns of threat from Big Data", The Globe and Mail (Feb 2018)*

While members of the Global Risk Institute identify cyber risk as one of their top risk concerns for their business, we believe this risk permeates its way all the way down into the daily lives of their clients. With that in mind, it is important to think about and provide solutions for cyber security also from their client's perspective. Many clients are only partially aware of their own cyber risks, and the required steps to protect themselves. While we all may have vague notions of the perils of virus' and malware, our busy lives leave us little time to research these risks and the various anti-malware and anti-virus packages to manage them. Fewer still take the time to think through what they would do in the event their identity was stolen, and the necessary legal steps required to remedy the damages and get your identity back. While banking practice generally has been to step up and absorb losses when credit cards are compromised, it is unclear what will happen as hacks become more sophisticated and losses become more material. In a recent case, a Canadian woman from Mississauga had been involved in an identity theft case since 2012, when someone fraudulently took out a $640,000 mortgage in her name.

> *"Like all data-driven businesses, fintech firms are vulnerable to hacks and data breaches. As we have learned from recent high-profile examples like Target and Equifax,12 the stakes are especially high when it comes to detailed personal and financial data. Unlike these large established companies with multi-million dollar cyber security budgets, fintech firms, particularly those in the start-up phase, have far fewer resources to allocate to cyber issues, which may make them more vulnerable to data breaches. Customers should keep this in mind if they chose to do business with these firms."*

> *"Perhaps the most significant risk brought on by the fintech paradigm, however, is cyber risk. As financial institutions, fintech firms, and their customers become more interconnected, the number of entry points that hackers can target grows dramatically, increasing the likelihood that sensitive financial data will be compromised. The development of new tools like open APIs and cloud computing further increases the number of vulnerabilities. With new technologies emerging daily and hackers becoming ever more adept, institutions must allocate adequate resources to ensure that their firms remain secure and are capable of mitigating new threats."*[6]

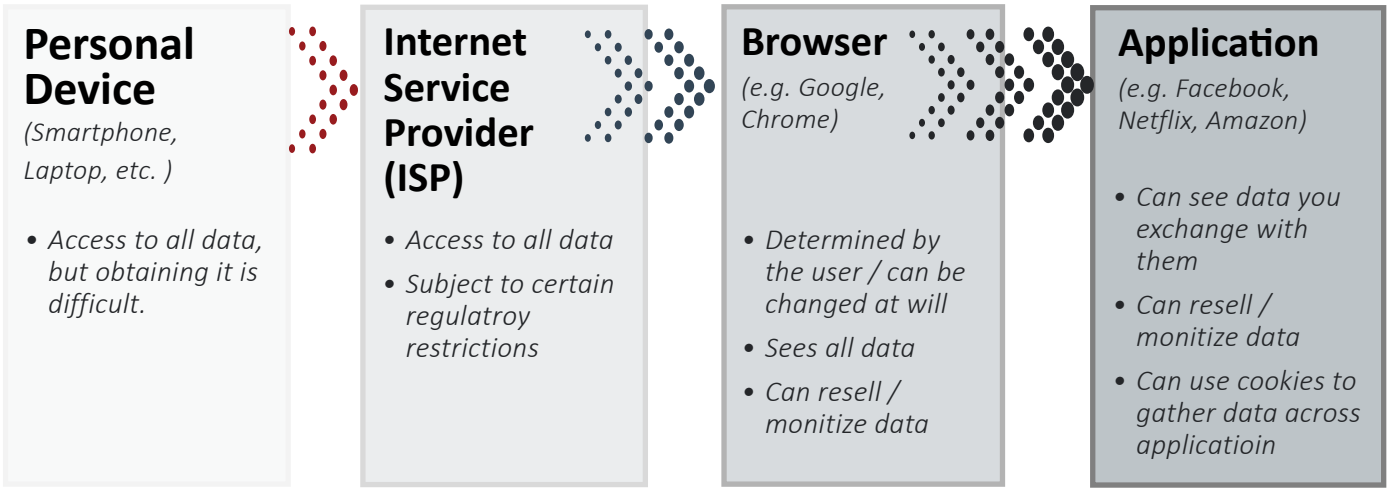
And while personal identification insurance is increasingly available, it generally covers legal costs, provision of an identity recovery case worker, and the cost of lost time at work to deal with the breach (usually up to a specific limit); but what about larger financial losses (such as mortgage fraud)? These are much harder to find coverage for, and the complex language required for such policies lead to ambiguity and uncertainty as to the extent of the coverage. At the same time, the social media industry has a $2 trillion market capitalization based on the usage and dissemination of user's data.

In financial terms, we describe the current situation as a reverse arbitrage for clients and banks. Social media firms take all the upside and leave clients with all the risk and then banks generally absorb the fraud loss when accounts are hacked.

We think there are better alternatives.

6 LaPlante,A. and Watson,C., "The Great Fintech Debate: Risks and Rewards of Financial Innovation", Global Risk Institute, (May 2018) p. 5 and 7

PERSONAL DATA ECOSYSTEM



What is Personal Data Advocacy?

This all leads to the question, in the wild west that is today's social media and data brokerage industry, who is looking out for the individual? We believe the world is ready for what we call Personal Data Advocacy, where an institution helps their individual clients gather, protect and monetize their personal data. We think that once an individual can gather a comprehensive collection of their data, then they will be able to exercise some degree of ownership control over it. With ownership of our data, each individual can then decide how they want their data used. Do they:

- want to lock it down?
- want to sell their data?
- want to donate it to a charity or research organization?

There are a myriad of possibilities. But also, once an individual has gathered their relevant data in one (secure) place, the data can be used to create their penultimate cyber profile; a profile based on their spending data, search data, social media data - basically all online and offline data. Such a profile will be a better cyber representation of them than any profile being created today, as it will have a complete data set and can be directly verified by the client or their agent.

And, not only will that data be valuable, should clients choose to monetize it, it can also enable more advanced cybersecurity practices and even enhanced personal identification theft insurance. The individual therefore becomes much better off as they have a trusted firm providing this type of Personal Data Advocacy for them. We think the financial services industry in general, and banks in particular, are well suited to help bring this type of service to clients.

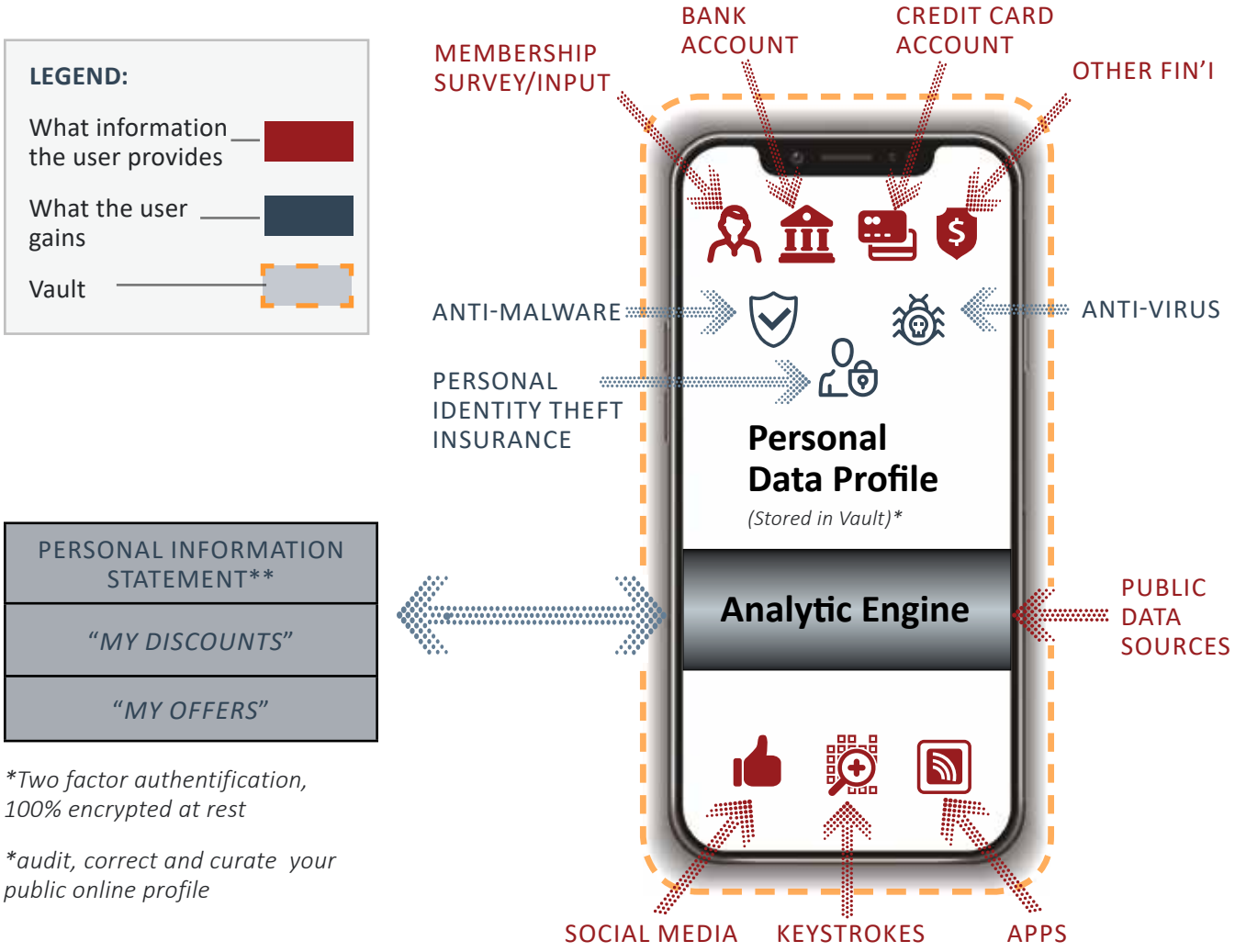
Why are major Financial Institutions well suited to support this type of service?

The components of each client's personal data can be put into three categories. The first and most valuable is your offline private data, including one's static personal data (name, birthdate, address etc.) and personal financial data, including transaction data (basically chequing account and credit card transaction activity) in particular. Banks and credit unions have all this transaction data already, and so they are a natural candidate to offer a personal data advisory service. The second category is your on-line private data (everything from google

searches to device clicks and websites/apps visited). The third component of personal data is on-line public data, primarily social media profiles and certain public government records. While a client's search engine provider and social media companies (which they participate in) currently gather their data and sell it to advertisers (for personalized ads; think in terms of those annoying pop up ads that start showing up based on your most recent searches), they are based only on narrow slices of one's data. Even when data brokers try to aggregate data from various app providers, they are often estimating matches for significant slices of data.

F.I.'s already has our transaction data (which is both the most valuable and most sensitive), and could offer applications (likely via a partnership with an existing technology or telco company) that combine this with online data, and then store a complete data set in one "lock box" or data vault for each customer . If F.I.'s was willing to do that for their clients, clients would suddenly have the most complete and valuable instance of their own data. Such data could then be sold, if the client chose, or could be analyzed for valuable insights (i.e. purchases, discounts and personal security insights), or could simply be locked down. Additionally, the personal data service provider could then help anonymise the client online, significantly reducing personal cyber risks.

What could a Personal Data Advocacy Service look like?



*Two factor authentification, 100% encrypted at rest

*audit, correct and curate your public online profile

Why should banks want to offer such a service?

While it is clear clients could benefit from a personal data advocacy service, why would an F.I. want to get directly involved in helping to provide it? We think there are several reasons.

1. First, banks have always played the role of trusted fiduciary for financial assets such as current or investment accounts. The concept of providing a data fiduciary service is not that far afield. It is becoming a generally accepted principle that data is an asset owned by individuals that produce it, similar to money.

2. Secondly, providing such an incremental value-added service to clients would almost certainly strengthen their propensity to remain a loyal customer to the bank going forward (as we all know, customer churn is a major cost for banks).

3. And third, at a time when margins are constantly getting squeezed, such ancillary services would be a new revenue source for banks, as they would earn a "data brokerage fee" when clients decide they want to monetize their data.

4. Finally, while chip technologies have had a major impact on reducing fraud losses in the past, helping individuals secure and protect themselves on line could well be the next major initiative in reducing a bank's fraud losses. As hackers become more brazen and sophisticated (major hacks and data breaches now number in the tens of millions each year), fraud losses can be expected to continue to grow. And the nature of fraud losses is migrating from smaller dollar credit card fraud type losses to higher dollar, personal identification theft and, for instance, the fraudulent mortgaging and remortgaging of properties; such loss are proving much more complex and costly to resolve.

Financial Institutions will need to consider the risks and policy implications of introducing a personal data advocacy service. The big risk is the assembling of such a significant compilation of a person's data in one (no matter how secure) place. Clients will be very reluctant to agree to such aggregation, as any breach of that environment would be much more significant than the (much narrower) data breaches to date. In fact, clients would require a significant cyber security bundle (including anti-virus, anti-malware, and personal identification theft insurance (both damages and remediation services)). Additionally, as government policy continues to evolve around personal data and cyber security, the personal data advocacy service provider will need to evolve and maybe help shape future policies.

Furthermore it is in the F.I.'s interest that its customers and their data is protected and used in an appropriate way. We mentioned earlier that if it can be the F.I. that pays at least a portion of the cost of a hacking incident if it leads to theft or fraud on an account. From a risk management perspective, helping customers protect themselves also protects the institution.

It has been said that data is the new oil, and if that is the case, your clients could be sitting on a significant unclaimed reservoir. Helping clients claim their rightful ownership of data assets could enable them to both harvest value and enhance their cyber security. We believe the time is right for financial institutions to take the lead and help clients manage the newest form of financial asset.