

Talking point

The digital credo of traditional banks: Data protection & data security (Fintech #4)

October 19, 2015

Contrary to what some critics say, traditional banks would be well advised to start using digital and algorithm-based data analysis instruments now. In future, this will be the only way they can offer their customers personalised financial services and recommendations and continually optimise their internal processes. Should they hesitate, however, the technology-driven, non-bank market newcomers will continue to extend their information lead and in time begin to offer more financial services (also outside the retail banking segment) that are easy to standardise and automate. The latter would further intensify cut-throat competition in the financial industry and could reduce traditional banks in the case of some financial services to pure-play infrastructure providers with declining customer contact. The introduction of so-called recommendation algorithms should be accompanied by the mandatory consent of the customer and transparent communication on how they function.

As many digital transactions as well as data access in households and companies have increasingly migrated from desktop PCs to the cloud and as powerful mobile devices are increasingly becoming the means of data access, IT security is gaining overriding importance in all spheres of life. No doubt the debate over IT security vulnerabilities following the release of the Snowden documents in June 2013 has been an additional driver of growing uncertainty and the feeling of “no longer being alone” online. This is an important signal for traditional banks, for customers are becoming justifiably worried about the eavesdropping activities and data abuse perpetrated by some technology-driven players – especially in the case of sensitive financial data. This is an area where traditional banks currently (still) hold a valuable trump that they should take with them to the table when negotiating strategic alliances.

Banks need to revisit current ways of handling (client) data within the framework of applicable data protection rules in order to deploy algorithm-based analytical methods that filter additional valuable information out of existing and/or supplementary new data. Indeed, the digital debate in the financial sector often gives short shrift to the aspect that banks possess huge amounts of valuable data with the potential to explore new ways of addressing customers. Banks know their customers' behavioural patterns (in terms of payments, consumption, propensity to save and invest, risk aversion, travel preferences, etc.). Therefore, it makes sense for established banks to apply the same data evaluation strategies as the large internet platforms, so they can also offer their customers convenient, one-stop shopping for as many value-added services relating to their finances as possible. After all, intelligent data analyses are the only way it will be possible in the long term to a) maximise customer utility and b) make internal infrastructures leaner and more efficient.

Consumers have a right to data sovereignty

Besides the not to be underestimated technical challenges facing the banks – the converting of unstructured data into machine-readable data, for instance – customers have a right to sovereignty over their own data. Traditional banks should start using modern analytical techniques now, but with the mandatory consent of the customer and additional transparent communication channels. These measures can boost customer confidence and minimise data protection infringements. Transparency should cover all steps of analysis, meaning from the collection of data and its fusion with other data sets right through to the analysis itself and any subsequent use of the findings. In this process, communication must be simple and understandable so that customers can follow the individual steps and select them at will.

Numerous pages of "General Terms and Conditions" in complex legalese printed in small type are not a good model to fall back on. Customers have a right to know what will happen with all the data collected on them and to decide on their data sovereignty themselves at all times. Therefore, banks should lead the way in allowing customers to indicate their choices on a short, simple (digital) application list stipulating what should happen with their personal data and which algorithms should be used. There has to be a guarantee that any change of

consent indicated by the customer can be granted at any time. One good way to impart information and awareness of these issues is a face-to-face meeting with the customer. Incidentally, such confidence-building measures on the transparency of business terms and contractual agreements should apply outside the banking sector, too.

Naturally, a stringent regulatory regime compels banks to comply with certain data protection aspects ex ante, but here they could assume a pioneering role. Additional self-imposed, i.e. voluntary, measures – such as disclosing how the underlying algorithms work – could enable the banks to make their analytical practices even more transparent, in contrast to many internet platforms. These confidence-building measures enable customers to have informed and self-determined knowledge of what happens when (personal) data is passed on and/or when consenting to an analysis that simplifies their decisions on the choice of financial services. This can also help to overcome the "black box" character of big data.

A level playing field is absolutely essential for all participants

At this juncture one must not forget that for regulatory reasons established banks are not allowed to correlate the personal data of a client between business divisions in order to gain new insights from the acquired data sets. Banks have to observe compliance guidelines which ensure that there can be no exchange of information between individual business divisions managed by different functions, and thus preclude any conflict of interest. Of course, these strict regulatory guidelines also apply to the underlying IT systems and (customer) data sets. For the new competitors from the non-bank sector in particular, however, this aspect plays a minor role. This means that for now digital ecosystems still tend to have an information edge. It follows that for regulatory reasons traditional banks permanently lag one step behind in the catch-up process.

The credo of traditional banks in the digital age

At the end of the day, what is required is a regulatory environment that provides fair rules and a level playing field. This is the only way to guarantee that individual market players are not given preferential treatment to the detriment of traditional banks. To sum up, traditional banks deserve the go-ahead to use modern analytical techniques, as long as they permanently guarantee their customers that they will neither monetarise personal data by selling them to third parties nor misuse them for other non-business projects. This is what needs to be marketed as the new digital credo of traditional banks in the digital age. That is when the modern analytical methods widely described in the big data debate will start to deliver their much vaunted benefits for traditional banks, too.

Further commentaries from the Fintech series may be found here:

[Fintech #3](#)

[Fintech #2](#)

[Fintech #1](#)

Details about the opportunities and risks of "Big Data" can be found here.

[Click here for more background on the Fintech movement.](#)

[Fintech reloaded](#) maps out a strategy showing how traditional banks should become a digital platform.



Author: Thomas-Frank Dapp (+49) 69 910-31752

...more information on **Technology, Innovation, Education**

Talking Point - Archive

© Copyright 2016. Deutsche Bank AG, Deutsche Bank Research, 60262 Frankfurt am Main, Germany. All rights reserved. When quoting please cite "Deutsche Bank Research".

The above information does not constitute the provision of investment, legal or tax advice. Any views expressed reflect the current views of the author, which do not necessarily correspond to the opinions of Deutsche Bank AG or its affiliates. Opinions expressed may change without notice. Opinions expressed may differ from views set out in other documents, including research, published by Deutsche Bank. The above information is provided for informational purposes only and without any obligation, whether contractual or otherwise. No warranty or representation is made as to the correctness, completeness and accuracy of the information given or the assessments made.

In Germany this information is approved and/or communicated by Deutsche Bank AG Frankfurt, licensed to carry on banking business and to provide financial services under the supervision of the European Central Bank (ECB) and the German Federal Financial Supervisory Authority (BaFin). In the United Kingdom this information is approved and/or communicated by Deutsche Bank AG, London Branch, a member of the London Stock Exchange, authorized by UK's Prudential Regulation Authority (PRA) and subject to limited regulation by the UK's Financial Conduct Authority (FCA) (under number 150018) and by the PRA. This information is distributed in Hong Kong by Deutsche Bank AG, Hong Kong Branch, in Korea by Deutsche Securities Korea Co. and in Singapore by Deutsche Bank AG, Singapore Branch. In Japan this information is approved and/or distributed by Deutsche Securities Limited, Tokyo Branch. In Australia, retail clients should obtain a copy of a Product Disclosure Statement (PDS) relating to any financial product referred to in this report and consider the PDS before making any decision about whether to acquire the product.