The European Consumer Organisation

The Consumer Voice in Europe

INNOVATIVE USES OF CONSUMER DATA BY FINANCIAL INSTITUTIONS

BEUC response to EBA consultation

Contact: **Farid Aliyev – financialservices@beuc.eu**

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • consumers@beuc.eu • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2016-091 - 29/09/2016

Why it matters to consumers

Consumers' financial and non-financial data is being increasingly and more intensively used by financial firms for various purposes. It is important to have a clear understanding of the potential benefits and risks of such practices for consumers, in order to prevent the development of harmful practices.

Summary

As the world becomes more digitalised and people increasingly use smartphones and social media, consumers' behaviour is ever more under scrutiny and recorded by service providers and traders. It is increasingly difficult to stay offline and anonymous. Financial and non-financial companies strive to collect more and more consumer data in an attempt to predict, with a higher and higher level of accuracy, their preferences, future behaviour and risk profile. Your banker or car insurance provider, without forgetting all types of providers like private credit registers that collect personal data without your knowing, probably know more about you than you would expect.

The EBA consultation on innovative uses of consumer data by financial institutions covers the area of credit, payment accounts and payment services. While we acknowledge that in some cases the use of consumer data may contribute to improving the quality of services, we also point to undesirable developments and any potential consumer detriment. It is important to have a clear understanding of what benefits and risks there may be in order to prevent the development of harmful practices.

It is worth mentioning that insurance products are not in the scope of the EBA consultation, yet the extensive use of personal and big data in that sector raises a number of fundamental issues which question the very nature of the current insurance model based on risk pooling, a practice that groups large numbers of people together to minimize the cost impact of the highest-risk individuals. Hence, a separate consultation on insurances is more than necessary.

Your banker or car insurance provider, without your knowing, probably knows more about you than you think.

1. Consumer data

Questions:

1. In what capacity (i.e. consumer, financial institution, technology providers, etc.) have you had experience with innovative uses of consumer data?
2. Based on your knowledge, what types of consumer data do financial institutions use most?
3. Based on your knowledge, what sources of consumer data do financial institutions rely on most?
4. Based on your knowledge, for what purposes do financial institutions use consumer data most?
5. How do you picture the evolution of the use of consumer data by financial institutions in the upcoming years? How do you think this will affect the market?

BEUC comments

Question 1: BEUC, the European Consumer Organisation, represents 42 independent national consumer organisations from 31 European countries (EU, EEA and applicant countries). BEUC acts as the umbrella group in Brussels for its members and our main task is to represent them at European level and defend the interests of all Europe's consumers.

The issue of personal data protection, regardless of the sector involved, is one of the top priorities for BEUC and its members. In this perspective, we are actively involved in the current discussions on the digital single market in its different dimensions: from connected products to collaborative economy, from smart appliances to demand-response energy schemes.

Question 2: Data is considered to be the new gold. Digital giants like Google, Facebook, Apple, Amazon, as well as other service providers are leading the gold rush. Consumers' online behaviour is continuously tracked and recorded. It is becoming increasingly difficult to stay offline and anonymous. With the explosion of digital technologies and connectivity, financial and non-financial institutions strive to collect more and more consumer data in an attempt to predict with a high level of accuracy their preferences, future behaviour and risk profile. Your banker or car insurance provider, without forgetting all types of service providers like private credit registers that collect personal data without your knowing, probably know more about you than you would expect. Financial institutions use consumer data of both non-financial and financial nature.

At the same time, it is difficult to know exactly what consumer data financial institutions are already using, which is part of the problem itself.

Test-Achats, our Belgian member, has been contacted by several consumers who were surprised by their bank's requests that want to access data stored on their mobile phone to install a mobile-banking app. One may wonder, for example, whether access to contacts or pictures is relevant.

A Which? magazine investigation in 2011 found that personal details such as name and email address were being sold for as little as £0.06 but if additional information, such as your occupation, what car you drive and where you live is added, the value of this information rockets. Personal details could be worth thousands of pounds if sold to numerous other companies. One UK car insurer was found to make 5% of its profits from selling on the details of customers who had been involved in accidents.

> If data is the new gold, then digital giants like Google, Facebook, Apple and Amazon are leading the gold rush.

Question 3: Both internal and external sources of consumer data are used by financial institutions. With the new developments, there seems to be a trend towards using more external sources.

Financial institutions are also obtaining more consumer data by expanding their interaction with consumers, for instance thanks to additional services like budgeting programmes or via social media.

When commenting on potential benefits and risks to consumers, we set out BEUC's views about the objectivity and validity of data used by financial institutions.

Question 4: Financial institutions use consumer data for various purposes, including:

- To make credit risk assessments;
- To select profitable customers and exclude those who are financially not interesting;
- To segment offers made to targeted customers based on their profile;
- To send personalised offers of investment products to consumers who have large amounts of deposits;
- To sell data to data brokers for use by other industrial sectors based on the customer's financial profile.

Question 5: One of the major risks/challenges in the coming periods is that banks, payment service providers, and other financial firms may be tempted to sell their customers personal data to third parties, e.g. what ING bank already envisaged in the Netherlands few years ago[1].

In Belgium, BNP Paribas Fortis has revised its terms and conditions governing relations with its customers.[2] Several articles referring to the use and transmission of customer personal data have been modified in such a way that the biggest bank operating in Belgium may transmit personal data of its customers to business partners, including for direct marketing operations.

[1] http://www.bloomberg.com/news/articles/2014-03-10/ing-plan-to-share-customer-payment-data-spurs-privacy-concerns
http://www.lalibre.be/actu/belgique/bnp-paribas-fortis-s-autorise-a-transmettre-les-donnees-des-clients-5327da5835707711f4a7de2d

The national data protection authority has opened a file on the matter and, after a first analysis, requested explanations to the bank. Test-Achats said in a press release that *"if it is not illegal to sell customer data, it shall be done in accordance with the law under which the client must give special permission to the bank to his data being transmitted to a trading partner. BNP Paribas Fortis must specify this in its general terms and conditions so that the customer knows how his data are used. Furthermore, the consumer should at any time have the right to cancel this authorisation*."

The number of financial institutions creating mega databases about their customers will make the data held by these companies more attractive to third-party companies.

Another major risk is the increase of financial exclusion, as product provision becomes something that is less mutualized and more individually risk-based.

That could also lead to price personalisation which is a form of price discrimination. For instance, an online shop which had access to your financial information could try to set the price as high as it can, based on the information it has on you.

2. Potential benefits

Questions:

6. Do you consider the potential benefits described in this chapter to be complete and accurate? If not, what other benefits do you consider should be included?
7. Are you aware of any barriers that prevent financial institutions from using consumer data in a beneficial way? If so, what are these barriers?

EBA statement: Consumers benefit from financial institutions' improved cost effectiveness

Using consumer data could enhance the cost effectiveness of marketing activities of financial institutions, allowing them to save money in advertising, for instance, and increase their sales and their reactiveness to any developments in the market. This increased cost- effectiveness may be passed on to consumers in terms of lower prices.

BEUC comment

While the use of data seems to benefit financial institutions like banks, insurance companies and others, the benefits to consumers are not necessarily there. It is likely that financial institutions cut their costs through using more consumer data. Yet, the passing on of their cost savings to consumers is not proven. Or at least there is no such evidence so far.

EBA statement: Consumers save money because they are offered targeted discounts by their financial institutions

Financial institutions may use consumer personal and financial data to understand their preferences and payment habits and offer consumers targeted products and services with specific trading partners (e.g. automatic discounts at restaurants or shops that are frequently visited by a specific consumer). This may enable consumers to save money whenever they purchase products or services included in the offers, either because products and services are cheaper or because they are tailored to consumers' needs and thus there is no need to complement the purchase with other products or services.
Consumers are seen as being interested in receiving points, rewards, and suggestions of purchases when they purchase a given product or service. Some consumers would

apparently be willing to reveal a wider range of their personal data if this meant better service from banks.

BEUC comment

In an attempt to boost their income, banks and other financial firms try to find other revenue streams. One such new development is the use of banking channels to promote non-financial goods and services. Banks partner with retailers and marketing companies to market their goods to bank customers based on their past spending behaviour. This practice is widespread on the other side of the Atlantic, and is apparently emerging in the UK[3]. For example, if the consumer has bought a new pair of shoes, he could find an ad from a rival company offering a coupon or gift card in his online account statement. Or after having bought a smart TV, your bank may suggest a high speed internet offer. In the US, bank customers are usually automatically enrolled into such schemes, without any explicit consent from the consumer.

As the world becomes more digitalised, and the use of smartphones and social media increases, consumers' online behaviour is being continuously observed by all kind of traders. Consumers are flooded with both general and targeted advertising, which is mostly considered as spam. Do consumers need to be exposed to such levels of spam when they log in to their online banking? Is that a service expected from financial institutions? Do consumers want a third party to spy and scan all their payment transactions and advise on their next purchase[4]?

We strongly disagree with the claim that targeted ads from banks' trading partners constitute a benefit to consumers. Such developments would certainly not be desirable in the EU. First, unsolicited spam should be banned. Second, the practice would raise privacy and security concerns: third parties have full access to the consumer's payment transactions and shape his future spending behaviour. Even though the industry pioneers claim that the data is anonymised and the consumer's identity is not revealed to third parties, the fact is that a person can be relatively easily identified by putting together data elements from different sources.[5] In this context it is important to stress that consumers should always have the freedom to fully protect their privacy.[6]

And most importantly, consumers' expectations from financial institutions are different: they want simple and transparent financial products, unbiased sales practices and fair treatment with regard to their finances.[7]

Comparability of products with so many additional offers attached is very questionable, mobility might also decrease because getting out of a part of a package might worsen the conditions of the remaining parts of the package.

---

3 http://www.thisismoney.co.uk/money/saving/article-2266542/Banks-spy-customers-sell-targeted-online-advertising.html

4 https://consumerist.com/2012/01/20/i-dont-want-ads-in-my-online-bank-statement/

5 This is also about people's freedom and fundamental rights! See Charter of Fundamental Rights Article 7 (right to private life) and Article 8 (right to data protection).

6 Why digital can't replace cash, BEUC blog, June 2016: http://www.beuc.eu/blog/

7 See BEUC response to the EC call for evidence on regulatory framework for retail financial services; BEUC response to the EC consultation on the Green Paper on retail financial services: http://www.beuc.eu/financial-services

We strongly disagree with the claim that targeted ads from banks' trading partners constitute a benefit to consumers.

EBA statement: Consumers pay less as a result of more accurate creditworthiness assessment

Financial institutions may use consumer data in order to better perform creditworthiness assessments before providing credit to consumers. This can be done by combining data they were given by consumers with other sources of data (e.g. social media) in order to increase credit score accuracy for improved risk control and offer more competitive pricing to consumers.

By applying more accurate credit scoring methodologies, based on more sophisticated analysis of consumer data, financial institutions may be able to increase the accuracy of risk profile and hence pricing of a specific risk. For instance, financial institutions may be able to offer lower interest rates on mortgages to consumers with a lower risk profile than less accurate traditional credit scoring models are able to produce.

BEUC comment

The use of consumer data in lending is not new. Lenders need sufficient information to conduct an accurate creditworthiness assessment i.e. to check whether the potential borrower can afford to repay the loan.

BEUC strongly supports the principle of responsible lending that is in the Mortgage Credit Directive, and advocates for the same principle to apply to personal loans.[8] A key question is the following: what information is needed to assess the borrower's creditworthiness?

Banks, credit unions and other traditional lenders conduct such assessments based on information and documents directly provided by the borrower, plus data registered by third parties (public credit registers, private credit bureaus). More recently, some lenders, especially online providers such as peer-to-peer lending platforms, have been using alternative information sources (web and social media profiles). Recently Facebook patented a technology that could be used by lenders to determine whether the borrower is a good credit risk, based on the credit scores of his/her Facebook friends[9]. Though later on, the social network giant opted to limit the amount of information available to third-party services, perhaps following the hint by the US Federal Trade Commission that the company could be regulated as a consumer-reporting agency which was not yet the case.[10]

Depending on the EU country, consumer credit data is collected and registered by public credit registers or private credit bureaus. The sector is strongly regulated in some Member States, where only public registers exist and collect minimum data related to consumers' pending and/or delayed credit commitments (positive and negative data). For

8 See BEUC response to the Commission's Call for Evidence on the EU regulatory framework for financial services, February 2016, p. 16: http://www.beuc.eu/publications/beuc-x-2016-010_call_for_evidence_fs_regulatory_framework_beuc_response.pdf

9 http://money.cnn.com/2015/08/04/technology/facebook-loan-patent/

10 http://fortune.com/2016/02/24/facebook-credit-score/

example, Belgian, French and Slovenian registers are managed by these countries' central banks and aim to fight against over-indebtedness. The French register contains only defaults of payment. There was a legislative attempt to expand the register to all loans being held by consumers (our French members were against that proposal), but the Constitutional Court opposed it.

Private credit bureaus like Experian, Equifax, and Creditinfo are present in many EU countries and collect extensive information on consumers' financial and non-financial commitments that they sell to lenders and non-financial service providers.

The Belgian register records all loans held by a consumer. Lenders are pushing for the credit register to contain other data related to consumer contracts. Our Belgian member, Test-Achats, is totally opposed to this possibility.

On the other side, private credit bureaus (also called credit reference agencies) like Experian, Equifax, and Creditinfo are present in many EU countries and collect extensive information on consumers' financial and non-financial commitments that they sell to lenders and non-financial service providers. Furthermore, in many countries several credit bureaus compete with each other.

<u>Link between the amount of data and responsible lending</u>: Credit bureaus claim that collecting more data on individual consumers contributes to a more accurate creditworthiness assessment by lenders. Yet, the reality seems to be different. FSUG (the Financial Services User Committee of the European Commission) recently conducted an investigation to assess the role of credit bureaus in responsible lending and prevention of over-indebtedness. One of the key findings was that *"… no clear link exists between the frequency of arrears in the different EU countries and the extent of credit data used. France, Spain, Finland Portugal, Belgium and Austria have similar frequency of arrear levels with a limited use of credit data. The United Kingdom, the Netherlands and Germany also have comparable frequency of arrear levels with a very high use of different credit data. On the other hand, countries such as Poland have very high arrear levels while the use of credit data is high; Cyprus has a very high arrear levels while the use of credit data is relatively low."* The FSUG concludes that the levels of arrears is much more dependent on other variables such as employment, income, social policies than the depth and breadth of credit data used[11].

<u>Link between the amount of data and lower interest rates</u>: the claim that increased and 'innovative' use of data for creditworthiness purposes improves access to more affordable credit for consumers is also questionable. For example, a US study carried out by the National Consumer Law Center (NCLC) assessed, inter alia, whether the use of big data actually improves the choice consumers face in the area of credit. The authors tested a number of claims made by big data proponents, such as: multiplying the number of variables will expand access to borrowers with thin credit files; by using a constellation of factors to price credit, the cost of credit will be reduced for low-income borrowers, thus

[11] Assessing the impact of credit data on preventing over-indebtedness, contributing to prudential regulation and facilitating access to affordable and quality credit, FSUG, December 2015: http://ec.europa.eu/finance/finservices-retail/docs/fsug/papers/1512-credit-data_en.pdf

enabling lenders to provide lower-cost small loans as alternative to payday loans. The study concluded that big data is a big disappointment and does not live up to its big promises. The use of big data in the lending area does not appear to result in more affordable products for low-income consumers. While some loans are marginally better, for the most part, credit products using alternate data are just as expensive as payday loans.[12]

Some scoring assumptions, although statistically relevant, can also be detrimental for consumers who act responsibly. For example, it is unfair to give lower scores to consumers without a credit history or for consumers who have an overdraft facility and credit card only in case of emergency but don't use these for their daily purchase. Such detriment increases as more assumptions are made during a credit worthiness assessment.

Consumers not in control of their data: there are also issues around how credit registers handle and process consumer data. Frequent problems experienced by consumers include: inaccurate data that adversely affects the consumer's credit application, difficulty for consumers to access and correct inaccurate data about themselves, opaque credit scoring mechanisms, and an automated process without human intervention. In addition, in some countries consumers are incentivised to borrow more to improve their credit score i.e. potential borrowers are judged on their capacity to borrow and refund, rather than on their capacity to save money. A recent awareness campaign by our UK member Which? informed consumers about various aspects and their rights related to credit scores.[13]

German consumers complain about opaque scoring mechanisms applied by credit bureaux, as well as the difficulty to understand assessments. According to BEUC's German member vzbv, consumers' ability to repay a loan must be evaluated based on valid criteria, and should never depending on whom they are friends with on social networks, what they like to shop for or what apps they install. Wrong assessments must be corrected.[14]

BEUC considers that policymakers should take action. We believe it is the right time to conduct an in depth analysis covering the following questions:

- What data is necessary and sufficient to assess the borrower's ability to repay a loan[15]?
- What is the role of credit bureaus and do they perform their role appropriately?
- Is it appropriate that consumers' credit data is controlled and traded by third-party commercial entities?

BEUC's suggestion: In our view, all the information (income and expenses) necessary for a creditworthiness assessment can be found on the consumer's bank/payment account statement. This information is objective and should allow the lender to conclude whether the borrower has a sufficient and stable income, whether the level of the loan-to-income ratio is appropriate, whether the consumer already has other pending mortgage credit or personal loans, including payment arrears, what are other financial and non-financial commitments (rent, utility bills, insurances, etc.). We see no reason to add other data, which is likely to be subjective and increase the risk of an incorrect assessment of the

[12] Big data : A big disappointment for scoring consumer credit risk, NCLC, March 2014: https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf

[13] http://www.which.co.uk/money/credit-cards-and-loans/guides/your-credit-report-explained/credit-report-myths-busted/

[14] http://www.vzbv.de/pressemitteilung/schufa-und-co-kredit-scoring-verfahren-undurchsichtig

[15] When considering the question of necessary and sufficient data, 'data minimisation' principle under data protection law should be taken into account and respected: Article 5.1 b of the GDPR 'Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'

consumer's financial situation. The information derived from the account statement (covering a sufficiently long period of time, e.g. one year) can be provided directly and quickly by the consumer to the lender, including new types of lenders such as peer-to-peer platforms, in a friendly format – digitalisation and new technologies should help with that. Data belongs to the consumer; it should not be collected, controlled and traded by private credit bureaus, which result in substantial consumer detriment.

Data belongs to the consumer; it should not be collected, controlled and traded by private credit bureaus, which result in substantial consumer detriment.

EBA statement: consumers are offered products and services that are personalised and adapted to their needs

More sophisticated analysis of consumer data can enable financial institutions to have real- time insight into consumer behaviour and anticipate consumers' needs or interests by offering products that are more adapted to them. For example, products could be adapted such that they allow insights in consumers' lifestyles, life-events, behaviours, or preferences (e.g. a financial institution proactively sending an email advertising a children's savings account to a recent parent).

BEUC comment

Financial products better adapted to each consumer's needs are welcome. Regrettably, recent financial scandals in different EU countries show that consumers are often tricked by financial firms into buying unsuitable or toxic products (see for instance the foreign currency loans crisis in Eastern, Central and Southern Europe, the PPI mis-selling in the UK, advice that does not fit the retail investor's profile, etc.). So far the financial sector has not proved that selling products tailored to customer needs is a priority. Quite the contrary. Technology advances have usually not led to a better focus on consumer needs, nor do these advances provide the consumers with more control over the products they use (e.g. blocked cards, forced NFC, rigid bank account or credit packages).

In that context, BEUC calls on regulators to tackle the market failures that cause most financial consumer detriment. Sales incentives in retail investments must be banned, otherwise investment distributors will never put the consumer's interest first.

As regards the use of data, we believe that a more intelligent analysis of consumer data by providers may help them adapt financial products to each consumer's specific needs. This is still a new trend, which implies that more time is needed to assess potential benefits and detriments, if any.

Midata scheme in the UK looks promising in that respect. The tool jointly launched by several banks helps consumers to choose a current account better adapted to their needs. To use the service, the consumer needs to download his data from his online banking in a specific format, and then upload the data on the dedicated website. The site then produces an account comparison based on the consumer's personal data and displays the amount he could earn - or lose - if he switched to any of the accounts on the market[16]. This type of tool could also potentially be used to help consumers choose other

16 http://www.which.co.uk/money/bank-accounts/guides/switching-your-bank-account/what-is-midata/

financial services.

EBA statement: consumers receive better advice based on analysis of their data

More extensive analysis of consumer data (e.g. payment data) can enable financial institutions to gain better knowledge of consumers' overall financial situation, needs and objectives and, thus, to provide better advice to consumers, tailored to their specific needs.

BEUC comment

Before talking about 'better advice', it should be mentioned that most of consumers have never received any financial advice from their financial institutions and are only in contact with pure salespeople. The number of cases of mis-selling and misleading that led many consumers to severe financial detriment is huge all over the EU. This explains why financial services have the lowest rating in the EU consumer scoreboard year after year.

For the time being, we do not have sufficient evidence suggesting that a more extensive analysis of consumer data (e.g. payment data) by financial institutions could enable financial institutions to provide better advice to consumers tailored to their specific needs. This must be monitored in the long run. Financial institutions should first change their model, i.e. putting their customers' interests at the center of their business first, which is far from the case today.

Today, consumers in the EU are not getting the advice they really need when looking for mortgages, insurance or seeking to better invest their savings, and they are too often recommended products they do not need (e.g. a far too sophisticated bank account or bundled products). Especially in the retail investment area, the low quality of advice has been documented widely, both by our members and by public authorities. Third-party commissions or in-house sales incentives tend to steer consumers towards overly complex and expensive retail investment products, often not suitable for their risk profile.

The number of cases of mis-selling and misleading that led many consumers to severe financial detriment is huge all over the EU.

BEUC is in favour of introducing measures to develop independent and unbiased financial advice outside of the financial sector.

BEUC considers that getting advice in financial services, in all its different forms, will be one of the areas where consumers may potentially benefit a lot from smart technology, if designed well.

A BEUC response to a recent EBA consultation on automated advice set out our views regarding potential benefits and challenges to consumers. For example, one of the key factors determining market outcomes will be the quality of the algorithm guiding consumers through the advice process.

Regulatory oversight of the software involved is therefore crucial, as all the features of unsuitable 'human' advice e.g. a product bias toward unsuitable products because of commissions can easily be mimicked by an algorithm[17] that may hide the interests of the financial institutions. It should be noted that the quality of the algorithm will become increasingly important in retail finance and influence the consumer experience in general, as traditional providers and fintechs invest heavily into such tools and rely on them to process and interpret massive volumes of data.

BEUC is in favour of introducing measures to develop independent and unbiased financial advice outside of the financial sector.

More generally, potential benefit as described above by EBA is very similar to their statement on page 9, thus requires more time to assess the impact on consumers.

EBA statement: consumers gain better insight into, and control over, their financial situation

Analysis of consumer data may enable financial institutions to provide services that give consumers better insight into their financial situation and spending behaviour, should they possess the desire to want to take control of their financial situation. Such services could help consumers to save money, budget their expenses and control their borrowing level.

BEUC comment

The same technology that warns someone not to overspend in a nearby store can also be used to encourage them to spend as much as possible.

Budgeting tools that give consumers better insight into their financial situation can be beneficial. Many tools of this kind are already present on the market in different EU countries, the so called 'account information services' regulated by the revised Payment Services Directive.

We doubt whether banks are the most appropriate suppliers for these services. For example, BEUC's Spanish member OCU developed an app called Mooverang that helps consumers to better manage their money. Mooverang analyses the data on the consumer's bank account(s) in order to improve their financial situation through matching user's consumption data with OCU's market data and sends unbiased recommendations to the user. The app detects the potential savings in the main spending categories (utilities, financial products, petrol station, etc.) and automatically informs the user.[18]

At the same time, one should be cautious here. The same technology that warns someone not to overspend in a nearby store can also be used to encourage them to spend as much as possible.

---

[17] BEUC response to EBA consultation on automation in financial advice, March 2016: http://www.beuc.eu/publications/beuc-x-2016-025_gve_automation_in_financial_advice.pdf

[18] http://www.mooverang.es/

EBA statement: consumers are better protected against fraud

Increased use of consumer data could help financial institutions to improve their fraud detection so that fraud is detected more often and/or earlier. For instance, if financial institutions know where a specific consumer lives and works, where he/she normally makes his/her payments, and the amounts that he/she usually spends, they will be more likely to be able to spot an unusual transaction because of where it is initiated, the product/service that is purchased, or the price that is paid. This could protect consumers against financial losses and the inconvenience and practical problems that are associated with incidents of fraud.

Many consumers complain that their credit card gets blocked by the issuer when making payments outside the EU, sometimes without any prior notice. Getting the card unblocked is usually a huge inconvenience and has a cost for the consumer.

BEUC comment

Security of payments is very important for consumers and payment service providers alike. We agree that the use of consumer' transactional and behavioural data by financial institutions can contribute to detecting unusual transactions and preventing fraud from happening. Behaviour-based fraud prevention is already being performed by payment service providers such as card schemes.[19] Those techniques may be efficient to block potentially fraudulent transactions, for example, where the transaction is initiated from an unusual place, country or IP.[20]

On the other hand, users are sometimes unfairly penalised due to automated behaviour-based techniques. For example, many consumers complain that their credit card gets blocked by the issuer when making payments outside the EU, sometimes without any prior notice. Getting the card unblocked is usually a huge inconvenience and has a cost for the consumer, not to mention the fact that the consumer may run out of money and his holiday or business trip may be at risk.[21] It can lead to major consumer detriment. Therefore, we believe that fraud prevention should in any case involve human intervention on behalf of the financial institution. Whenever the financial institution considers blocking a payment instrument upon suspicion of a fraudulent transaction:

- It should immediately contact the consumer to check whether the transaction had been authorised or not;
- The responsibility on reaching the customer should lie with the financial institution;
- The procedure for unblocking the payment instrument should be available 24/7 and easy to reach from anywhere around the world;
- The procedure for unblocking the payment instrument should be based on advanced identification and security check, which should be easy to fulfil on the one hand from abroad but enough to ensure authenticity on the other.

19 https://www.visaeurope.com/media/images/sca%20position%20paper-73-31002.pdf

20 See BEUC response to EBA consultation on strong customer authentication and secure communication, February 2016: http://www.beuc.eu/publications/beuc-x-2016-012_eba_consultation_strong_authentication_in_payments.pdf

21 https://communaute.ingdirect.fr/t5/Moyens-de-Paiement/carte-bloqu%C3%A9e-%C3%A0-l-%C3%A9tranger/td-p/13247

Which? found that 62% of consumers say they have been targeted by online fraudsters in the past 12 months

UK member Which? recently launched a Safeguard Us from Scams campaign. The campaign calls on the UK government to put more pressure on companies to protect their customers from the increasingly sophisticated tactics of fraudsters, and not leave the onus solely on consumers to protect themselves. An overwhelming majority of people (85%) think companies must take an equal or greater responsibility in protecting us from online scams.

Which? found that 62% of consumers say they have been targeted by online fraudsters in the past 12 months, with the most common types of scam and fraud being:

- Phishing emails - emails purporting to be from a bank or payment service;
- Phishing messages that seek money for services/help, e.g. a friend stuck abroad and;
- Bogus computer support.

We believe companies need to do far more to protect consumers from scams and should bear the cost where their weaknesses have left customers' money vulnerable.

German member vzbv indicated that insecure procedures to use data may weaken security precautions by behavioural-based fraud prevention if fraudsters get access to this data. For example, options to pay by using the online-banking PIN-code may invite consumers to use this credential more openly. Scams may then cause consumers to enter this highly sensitive code on a fraudulent website. While no payments may be enacted by a PIN code only, the data provided on the account will become accessible and may be stored and abused later to mimic, for instance, normal payment behavior by that user with a lost or stolen payment instrument. Apart from the breach of privacy this may cause further security leaks and cases of identity theft by allowing fraudsters to open up new accounts on behalf of the rightful account holder: a number of services still send tiny payments with a code to check whether a new customer has actually access to a certain payment account and may thus be authenticated by it.

3. Risks

Questions:

8. Do you consider the potential risks described in this chapter to be complete and accurate? If not, what other risks do you consider should be included?
9. Have you observed any of these risks materialising? If so, please provide examples.

EBA statement: consumers experience detriment if they are unaware of the way financial institutions make use of their personal data

Consumers may not always be properly informed of the usage of their personal data. This may be the case when, for instance, the use of their data is not properly described or updated in contractual documentation provided to them by financial institutions.

On the other hand, consumers may not understand information that is provided to them regarding the use of their data. For example, very comprehensive information may be made available in the contracts between consumers and financial institutions, but it tends to be too complex and/or too detailed for consumers to understand.

Unlike financial institutions, consumers may not always have an in-depth knowledge about the legal framework applicable to the usage of their personal and financial data. This information asymmetry may be especially relevant in cross-border transactions, where the applicability of legal requirements is not always clear.

BEUC comment

We fully agree with the risks described above.

If a financial institution is using data or intends to use data that has not been provided directly by the consumer or that does not come from its direct relationship with the consumer, this needs to be made clear to the consumer.

Financial and non-financial service providers must respect EU data protection law, in particular the rules on 'purpose limitation' (data must not be used for purposes which are incompatible with the original purpose that justified the initial data collection) and 'data minimisation' (service providers should not ask for more data than is necessary for the provision of the service). Consumers also need to be well informed and receive transparent information on how their data is used and processed.

If a financial institution is using data or intends to use data that has not been provided directly by the consumer or that does not come from its direct relationship with the consumer, this needs to be made clear to the consumer. There needs to be balance between the legitimate interest of the financial institution to use external sources of data and the impact on the consumer rights and freedoms.

***EBA statement**: Additionally, financial institutions may have in place automatic rules based on the information given by consumers that result in the usage of consumer data in a way that may be non-transparent and somewhat arbitrary, notably because consumers may not be aware of the factors that led to the decision (e.g. non-approval of credit application because of automatic credit scoring based on consumer data).*

As a result of the above, consumers may experience detriment in the form of breaches to their privacy.

BEUC comment

As automatic credit scoring is not a new development, there is evidence of related consumer detriment. See our comment on page 6.

EBA statement: consumers are "locked-in" by their current provider because their data is not assessable to other financial institutions

Financial institutions may collect and process a significant amount of data throughout the contractual relationship with consumers, which means that they may be able to offer to consumers products and services that cannot be matched by other financial institutions (that do not have access to the same types of data). If financial institutions do not allow for the portability of consumer data, consumers may be hindered from choosing a different provider for the provision of financial services.

BEUC comment

The new EU data protection law provides the consumer with the right to receive his personal data from his financial service provider, as well as to request the provider to transmit the data directly to another provider, where technically feasible[22]. This will allow the consumer to e.g. receive customized current account offers from other banks, based on his real situation, spending/saving patterns and future needs, and compare products across the market. As already mentioned above, solutions similar to Midata in the UK can benefit consumers and competition, as they may facilitate product comparability and switching.

EBA statement: consumers experience detriment if financial institutions misuse their personal data

Consumer personal and financial data may be used by a financial institution for purposes that were not in any way disclosed to consumers. The misuse of consumer data may be a result of deliberate or accidental actions by the financial institution or an individual employee.

Also, financial institutions may interpret legal requirements for data collection, for anti-money-laundering purposes for instance, such that they collect more data than is legally required and then reuse it for other purposes.

The misuse of data can manifest itself in consumer data being sold by financial institutions to third parties (such as marketing companies) without the consumers' consent. Financial institutions may also be processing consumer data without explicit authorization from the consumer. This may result in detriment for consumers, through financial institutions being remunerated for selling consumer data and consumers not benefiting from this; consumers being targeted by third parties with whom they never have, and do not wish to be, commercially engaged; or various types of identity fraud.

Finally, the misuse of consumer data can also result in detrimental marketing approaches by financial institutions, in the form of spamming of electronic or conventional mail. This is more relevant in the context of the increasing digitalization of communications between financial institutions and consumers, where the costs of communicating via email are low.

BEUC comment

The above risks are accurately described, though the risk of misuse of data is not new and not necessarily related to innovative uses of consumer data by financial institutions.

Consumer trust in financial service providers is crucial, and is difficult to restore once broken. As already stated above, service providers must respect EU data protection law.

As regards the EU anti-money laundering rules, BEUC is in favour of harmonising the provisions of the Anti-Money Laundering Directive (AMLD) to achieve its coherent application across Member States and better protect consumer personal data and privacy. The available evidence suggests that some financial service providers collect information from consumers for commercial purposes, using the AMLD requirements as an argument.[23] We hope this issue will be addressed by policymakers as a follow-up to the Green Paper on retail financial services.

---

[22] Art 20 of General Data Protection Regulation (GDPR) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

[23] See BEUC position, May 2013: http://www.beuc.eu/publications/2013-00398-01-e.pdf

EBA statement: consumers experience detriment as a result of wrong decisions by financial institutions on the basis of wrong information

Financial institutions may use consumer personal and financial data, irrespective of where such data was obtained, to make decisions that may result in detrimental treatment of consumers. This unfair treatment can manifest itself in the following ways:

a. *consumers are turned away by financial institutions, for example, as a result of a financial institution rejecting a consumer based on a profile that categorises the consumer as being prone to credit default because of outdated or inaccurate information;*

b. *consumers are declined from purchasing certain products or services, for example, because of a consumer not being offered a mortgage because the specific personal data from social networks incorrectly led the financial institution to believe that the consumer was less creditworthy a borrower;*

c. *consumers are offered or declined certain contractual conditions when asking for a specific product or service, for example a consumer not being granted a long-term loan because the financial institution has wrongfully concluded from external data that the consumer may be a gambler.*

BEUC comment

We fully concur with the above descriptions. With regard to the use of consumer data in the area of credit, see our comments on page 6.

In addition, a consumer's right to not be subject to a decision based solely on automated processing of personal data must be respected.[24]

EBA statement: *this risk is more likely to arise if the provider establishes discriminating criteria based on sensitive consumer data, such as those related to health. When consumers are profiled through the use of personal information they might be targeted for specific products and/or services that are not in their best interest (e.g. unsuitable insurances for risk-averse consumers); or they may be excluded from the offer of services that would be interesting to them, because financial institutions see them as uninteresting or too risky.*

BEUC comment

The growing use of personal data and big data carries also the risk of unjustified discrimination and the financial exclusion of consumers. The greater the types of data gathered, the higher the likelihood there is irrelevant data, an incorrect interpretation or an adverse effect on the consumer.

As already stressed earlier, only objective and valid data, i.e. data originated from reliable sources, and only those necessary for the service provided, should be used by financial institutions in their activity. The question of the quality of algorithms and competences of data analysts who control them remain. Nowadays, data analyst jobs are extremely common, and companies in different sectors actively implement algorithms for automated data processing. These are subjective elements in the equation, i.e. if an algorithm is wrongly configured, it could leave to discrimination of certain consumer groups.[25]

[24] Article 22 of the GDPR: Under certain circumstances, individuals have the right not to be subject to a decision based solely on automated processing of personal data which produces legal effects or significantly affects him/ her.

[25] http://theconversation.com/its-not-big-data-that-discriminates-its-the-people-that-use-it-55591

Personal data and big data must be used ethically. In that respect, the General Data Protection Regulation (GDPR) forbids the processing of particularly sensitive personal data, unless certain strict conditions are met. The prohibition applies to, inter alia, personal data revealing racial or ethnic origin, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health.[26]

Insurance products are outside the scope of this consultation, yet the extensive use of personal and big data in that sector raises a number of fundamental issues which question the very nature of the current insurance model based on risk pooling. Hence, a separate consultation on insurances is essential.

Overall, a more intensive use of personal data and big data by financial institutions in their risk assessment models aims to maximize their profits and minimize risks. The industry aims at 'zero risk taking', while the entire risk is being shifted to consumers. As a result vulnerable consumers may become financially and socially excluded as they are considered too risky by financial institutions. This is one of the key challenges for the coming years that needs to be anticipated and prevented by competent authorities.

EBA statement: consumers have restricted or no access to financial products or services because they do not allow for their information to be used by financial institutions

If consumers do not wish to disclose their data for purposes different than those required by law and do not allow their financial institutions to use it for any kind of commercial purposes, they might be excluded from relevant offers.

This risk is more relevant if the use of consumer data becomes the main marketing tool of financial institutions. Consumers that do not allow their data to be used for commercial purposes would then have restricted access or even be excluded from some financial services.

Also, there may be the case that consumers will be perceived as having a higher risk, thus paying more for the same services when compared to other comparable consumers, because they refuse to disclose any data with which financial institutions would be able accurately to profile them.

BEUC comment

The above-described risk of exclusion/discrimination of privacy-minded consumers appears to be imminent. For example, recently an insurance executive said it could be impossible to get a life insurance without a wearable device in the next five to ten years.[27] Such a scenario could also happen with respect to other financial services, like credit: for example the consumer is required by the lender to allow access to his social media accounts before the decision to grant the loan is taken.
Digitalisation and the increasing use of personal and big data may also penalise offline consumers e.g. those who do not have a broadband internet connection, those who lack the access or the knowledge to navigate easily on line, elderly people, and some people with disabilities (the visually impaired).

Policymakers should track such dangerous developments and prevent them.

There is evidence that fear of scams is starting to affect consumer behaviour, as half of people (48%) say they do not use certain online products, services or apps for fear of

---

[26] Art 9 of GDPR
[27] http://www.swissinfo.ch/eng/no-wearable--no-policy-_insurers-grapple-with-wearable-big-data--revolution-/41381560

being targeted by scammers[28].

EBA statement: consumers suffer detriment if consumer data stored by financial institutions is obtained fraudulently by third parties

Consumer data stored by financial institutions may be accessed by third parties in an illegitimate way if, for instance, such data is hacked (e.g. credit card details stolen and subsequently used by third payments to purchase goods/services in the name of the consumer). There may also be the case that financial institutions have anonymized consumer data, but third parties with fraudulent intents are able to reconstitute such data and misuse them to the detriment of consumers. This risk is more likely to occur when financial institutions have weak IT-security measures in place.

BEUC comment

In 2014, eBay asked users to change their passwords after hackers stole encrypted passwords and other personal information, including names, e-mail addresses, physical addresses, phone numbers and dates of birth.

With digitalisation, the Internet of Things and a data-driven economy, more personal information is collected up by powerful computers and data centers containing large volumes of data are being targeted by fraudsters.

Cyber-security is a growing concern. In the last few years, there were several high profile cases of hacking and data theft including the Target case where millions of consumers' credit card details were stolen. Earlier this year, the US Financial Consumer Protection Bureau (CFPB) alleged that a payment processor made public statements regarding the efficacy of its data security system and failed to fulfill those promises[29]. In 2014, eBay asked users to change their passwords after hackers stole encrypted passwords and other personal information, including names, e-mail addresses, physical addresses, phone numbers and dates of birth[30]. Following a very recent hack into Linkedin's system, about 100 million accounts might have been affected.[31]

Worryingly, a UK Government survey found that over six in 10 large firms detected a cybersecurity breach or attack in the past year, but only 5% of firms invest in ongoing monitoring of breaches on their systems.

[28] https://press.which.co.uk/whichpressreleases/government-taskforce-must-not-let-businesses-off-the-hook-on-scams/

[29] http://www.srz.com/CFPB_Targets_Online_Payment_Platform_in_First_Enforcement_Action_on_Cybersecurity/

[30] https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach/

[31] http://time.com/4340172/linkedin-hack-2012-passwords/

Cyber-security is a horizontal topic and has a much wider scope than financial services. In the area of financial services, some initiatives have been undertaken to improve the security of payment services at the EU level. In 2013, the SecuRe Pay Forum's Recommendations addressed to payment service providers looked at issues related to the PSPs internal governance, risk identification and assessment, monitoring and reporting, risk control and mitigation issues as well as traceability.[32] Payment service providers put in place solutions like end-to-end-encryption and tokenization[33] in order to reduce the risk of data theft and payment fraud[34].

Consumers have growing concerns about being exposed to scams and the harm they could cause. Worryingly, the UK Government's Cyber Security Breaches 2016 Survey found that over six in 10 large firms detected a cyber-security breach or attack in the past year, but only 5% of firms invest in ongoing monitoring of breaches on their systems. And when individuals have fallen victim, Which? found that banks were inconsistent when dealing with fraud. The Financial Ombudsman Service stated that in many cases banks have based their decisions 'on a hunch', without conducting a full investigation and potentially leaving victims out of pocket and feeling like suspects for crimes they didn't commit.

EBA statement: Integrity of the financial sector is undermined if trust in financial institutions decreases because of lack of data security

In the event that consumer data is stolen, hacked and/or leaked, trust in financial institutions may be undermined, with spill-over effects to the financial sector overall, in respect of the sector's ability to securely store and process data. This distrust may even spread to other services offered to consumers and result in reduced market confidence.

BEUC comment

Companies need to do far more to protect consumers from scams and should bear the cost where their weaknesses have left customers' money vulnerable. Scams have the power to undermine public confidence to engage with genuine companies – how do we know what's real and what's not? Both consumers and business will suffer as a result.

END

---

32 https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf

33 Tokenization is the process of replacing sensitive data with unique identification symbols that retain all the essential information about the data without compromising its security.

34 http://www.bankinfosecurity.com/tokenization-vs-end-to-end-encryption-experts-weigh-in-a-1869